

Immobilized or petrified?

Explaining privacy concerns and the (de)mobilization against mass online surveillance in 21st-century advanced democracies

Isadora Borges Monroy

Political Science, McGill University, Montreal

Submitted to committee May 11, 2023

Defended to committee July 12, 2023

Submitted to Graduate and Postdoctoral Studies July 27, 2023

A thesis submitted to McGill University in partial fulfillment of the
requirements of the degree of Ph.D. in Political Science

© Isadora Borges Monroy 2023

Contents

List of Figures.....	4
List of Tables.....	5
Abstract.....	6
Résumé.....	7
Contribution of authors.....	9
Acknowledgements.....	10
Immobilized or petrified? Explaining privacy concerns and the (de)mobilization against mass online surveillance in 21st-century advanced democracies.....	14
Dissertation overview.....	27
Bibliography.....	38
Chapter 1 Deputation in the surveillance complex.....	44
Abstract.....	44
Introduction.....	44
Historical roots of deputation.....	51
Seventy years of deputized national security, praxis, and ideology.....	51
Twenty years of the surveillance complex.....	60
By hook or by crook: degrees of collaboration.....	68
Carrots.....	74
Sticks.....	82
Backends.....	87
Conclusion.....	89
Bibliography.....	96
Chapter 2 Measuring Privacy Concerns under the Surveillance Complex.....	111
Abstract.....	111
Introduction.....	111
Theory.....	117
No one or everyone? Agentless and deputized surveillance concerns.....	133
Methods and Data.....	134
Design and Question wording.....	136
Results.....	138
Univariate distributions.....	139
Dimensions.....	142
Discussion and Conclusion.....	149
Bibliography.....	150

Appendix.....	158
Chapter 3 Who is mass online surveillance for?.....	168
Abstract.....	168
Introduction.....	168
Theory.....	171
Design.....	177
Data	181
Vignette experiment design	181
Hypotheses	187
Outcome variables measurement.....	188
Confounder variables.....	188
Results.....	190
Overview: Group-based surveillance	191
Overview: Soft or hard surveillance policy	194
Regression analysis.....	196
OLS regression results	197
Conclusion	201
Bibliography.....	205
Appendix.....	208
Steadfast respondents	213
Logit and Multinomial results on steadfast respondents.....	215
Chapter 4 European attitudes towards privacy and security as a policy tradeoff.....	218
Abstract.....	218
Introduction.....	218
European surveillance regulation.....	225
Theory.....	230
Cleavages.....	230
Postmaterialism.....	231
Party vote choice and ideology.....	232
Institutions: trust, approval, political interest	233
Emerging cleavages: the European Union and Transnationalism.....	234
Controls	235
Hypotheses for preferences prioritizing privacy or security.....	236
Refusal to tradeoff versus trading one for the other as a secondary outcome.....	238
Data and methodology	241

Outcome measures: Privacy-security tradeoff interval and binary refusal/tradeoff	242
Independent variable measures	243
Cleavages	243
Postmaterialism	243
Vote choice and ideology	245
Institutions	246
EU transnationalism	247
Control variable measures	247
Results	248
Descriptives for country-level surveillance	251
Privacy-security tradeoff as an interval scale	253
Examining the refusal to trade off privacy and security	260
Conclusion	262
Bibliography	265
Appendix	270
Dissertation Conclusion	277
Technical chapter: Sampling and Survey Wording	293
Sampling	293
The external validity of samples and selection bias of people in online surveys	294
Missingness overview	298
Reading the survey codebook	300
Questionnaire wording and response distributions	301

List of Figures

Chapter 1

<i>Figure 1 Snowden slides from PRISM/US-984XN NSA Overview.</i>	46
<i>Figure 2 First Twitter government transparency report, 2016</i>	71
<i>Figure 3 Apple's privacy billboard marketing</i>	72
<i>Figure 4 Dempsey presentation slides on Cybersecurity non-enforcement and non-regulation</i>	79

Chapter 2

<i>Figure 5 Average concern level per dimension</i>	139
<i>Figure 6 Responses of deputized policies</i>	141
<i>Figure 7 Pairwise subsetted correlational heatmap</i>	148
<i>Figure 8 Binary calculation of support for statements</i>	159
<i>Figure 9 PCA Scree plot</i>	159
<i>Figure 10 Correlation heatmap</i>	165
<i>Figure 11 Network plot of dyad correlations</i>	166

Chapter 3

<i>Figure 12 Average response to group</i>	192

Figure 13 Average change in response given group sequence-----	194
Figure 14 Average response to policy -----	195
Figure 15 Visual representation of coefficient estimate effects per model -----	200
Figure 16 Full sample and treated sample average change in opinion -----	211
Figure 17 Size of opinion change (absolute values) -----	211
Figure 18 Change in opinions from deputized battery to vignette experiments-----	214
Figure 19 Selected predicted probabilities from the logit model-----	215
Figure 20 Selected predicted probabilities from multinomial model -----	216
Chapter 4	
Figure 21 Country-level average preference distribution -----	251
Figure 22 2SD-transformed country-year averages-----	253
Figure 23 Country-level change of average (/ 2SD) between surveys -----	253
Figure 24 Tradeoff regression model dot-plot-----	255
Figure 25 2021 distribution of American data (n=1493)-----	273
Figure 26 Vote preference National and EU party families -----	273
Figure 27 US Securities and Exchange Commission Facebook filings on average revenue per user by region -----	276
Technical Chapter	
Figure 28 Response missingness, questions in order of appearance -----	299
Figure 29 Response missingness, ordered by percent NA's-----	300

List of Tables

Chapter 2	
Table 1 18-item Principal Components Analysis-----	144
Table 2 Sociodemographic survey distributions-----	158
Table 3 18-item 3D Principal Components Analysis -----	160
Table 4 19-item Market location Principal Components Analysis -----	161
Table 5 19-item Government location Principal Components Analysis -----	162
Table 6 18-item 5 dimension PCA -----	164
Table 7 Correlation matrix estimates -----	164
Chapter 3	
Table 8 Group distribution-----	190
Table 9 vignette 1, 2 and change score OLS results-----	197
Table 10 Change score combinations, coding, and frequencies -----	210
Table 11 Full sample vignette 2 OLS results -----	212
Table 12 Pre-treatment variable models, robustness check-----	213
Chapter 4	
Table 13 Proportion and difference of outcome responses by year-----	248
Table 14 Logit model's statistically significant exponentiated estimates.-----	261
Table 15 Variable distributions-----	271
Table 16 Country year sample distributions -----	272
Table 17 Tradeoff OLS regression estimates -----	275
Table 18 Logit's Average Predicted Effects Estimates -----	275
Technical Chapter	
Table 19 Socio-demographic distributions -----	294

Abstract

The dissertation studies attitudes toward privacy and surveillance in advanced democracies, particularly the United States and European Union members. I propose the concept of “the surveillance complex” to capture the interplay of governments and markets’ producing and deploying mass surveillance. I describe how democratic governments, usually forbidden from conducting mass surveillance directly, have deputized corporations, who already monitor their users. This provides governments with incentives to keep political and economic costs of surveillance low, by attempting to avoid interbranch and voter political scrutiny. People shape their public opinions on surveillance in generally low-information environments, punctured by whistleblowers, journalists, and data leaks which provoke securitized reactions from the government in the media re-focusing attention on how surveillance can subsequently be used on some law-breaking groups. My dissertation contributes to Political Science’s comparative public opinion and also puts it in dialogue with other disciplines involved in surveillance studies.

I measure American and European’s attitudes toward components of the surveillance complex in three chapters. Using an original, nationally representative survey of Americans ($n = 1,493$). In a descriptive chapter, I analyze whether privacy concerns for deputized surveillance empirically differ from other forms of surveillance. I find attitudes towards surveillance are multi-dimensional and that deputized surveillance is distinct from policies where the source and use of data are unambiguous (government or corporations). In the following chapter, I apply an experiment on the surveyed population to gain insight into two proposed influences on public opinion of deputized surveillance. I hypothesize and test whether intergroup relations, particularly out-group bias, play an important part in people’s willingness to accept two mass policies of deputized online surveillance. I find evidence supporting my hypothesis. Favoritism toward a liked group can influence levels of rejection

(moderately). However, out-group bias exemplified by the disliked group has a stronger influence on surveillance acceptance, sometimes even overriding previous misgivings.

These chapters help explain why two decades after 9/11 people are still willing to continue mass surveillance programs. In the US, the use of rhetoric alluding to criminal behavior can increase demand for policies, by de-emphasizing mass data collection for subsequent data use in law enforcement. Finally, I study European attitudes between a direct security and privacy tradeoff. The European Voter Study data measures attitudes before and after the passing of the General Data Protection Regulation (GDPR), in 2014 and 2019. The chapter tests voting behavior theories, comparing their explanatory power against tradeoff preferences. I highlight their explanatory limits since intergroup attitudes similar to the American study cannot be replicated with the secondary data. While a large proportion of respondents refuse to trade one for the other, I find evidence that after the change in legal regime attitudes crystallized toward more privacy in 2019 compared to 2014, suggesting a modest supply-side effect on attitudes.

The first chapter historicizes and provides a political economy perspective of how the phenomenon of the surveillance complex developed in advanced democracies, spearheaded by the US. The three public opinion chapters analyze attitudes towards different components of the surveillance complex. The dissertation lay the groundwork for future work on how normalizing (e.g., in the US) or critiquing (e.g., in the EU) the supply of some types of surveillance contextualizes how people's demand for surveillance policies takes shape. A technical chapter describes the American survey questions and response distributions.

Résumé

La thèse étudie les attitudes envers la vie privée et la surveillance dans les démocraties avancées, en particulier les États-Unis et les membres de l'Union européenne. Je propose le concept de « complexe de surveillance » pour saisir l'interaction des gouvernements et des marchés produisant et déployant

une surveillance de masse. Je décris comment les gouvernements démocratiques, généralement dans l'interdits de mener directement une surveillance de masse, ont suppléé les entreprises, qui surveillent déjà leurs utilisateurs. Cela incite les gouvernements à maintenir les coûts politiques et économiques de la surveillance à un faible niveau, en tentant d'éviter le contrôle politique interprofessionnel et électoral. L'opinion publique de la population concernant la surveillance est façonnée dans des environnements généralement peu informatifs, ponctués de lanceurs d'alerte, de journalistes et de fuites de données qui provoquent des réactions sécurisées du gouvernement dans les médias, recentrant l'attention sur la manière dont la surveillance peut ensuite être utilisée sur certains groupes qui enfreignent la loi. Ma thèse contribue à l'opinion publique comparée de la science politique et la met également en dialogue avec d'autres disciplines impliquées dans les études de surveillance.

Je mesure les attitudes des Américains et des Européens envers les composants du complexe de surveillance en trois chapitres. À l'aide d'une enquête originale et nationalement représentative des Américains ($n = 1\,493$). Dans un chapitre descriptif, j'analyse si les préoccupations de confidentialité pour la surveillance déléguée diffèrent empiriquement des autres formes de surveillance. Je trouve que les attitudes envers la surveillance sont multidimensionnelles et que la surveillance déléguée est distincte des politiques où la source et l'utilisation des données sont sans ambiguïté (gouvernement ou entreprises). Dans le chapitre suivant, j'applique une expérience sur la population sondée pour mieux comprendre deux influences proposées sur l'opinion publique de la surveillance déléguée. J'émet des hypothèses et teste si les relations intergroupes, en particulier les préjugés hors groupe, jouent un rôle important dans la volonté des gens d'accepter deux politiques de masse de surveillance en ligne déléguée. Je trouve des preuves à l'appui de mon hypothèse. Le favoritisme envers un groupe aimé peut influencer les niveaux de rejet (modérément). Cependant, le biais hors groupe illustré par le groupe mal aimé a une plus grande influence sur l'acceptation de la surveillance, dépassant parfois même les appréhensions antérieures.

Ces chapitres aident à expliquer pourquoi deux décennies après le 11 septembre, les gens sont toujours prêts à poursuivre les programmes de surveillance de masse. Aux États-Unis, l'utilisation de la rhétorique faisant allusion au comportement criminel peut augmenter la demande de politiques, en mettant moins l'accent sur la collecte massive de données pour une utilisation ultérieure des données dans l'application de la loi. Enfin, j'étudie les attitudes européennes entre un compromis direct entre la sécurité et la vie privée. Les données de l'étude européenne sur les électeurs mesurent les attitudes avant et après l'adoption du Règlement Général sur la Protection des Données (RGPD), en 2014 et 2019. Le chapitre teste les théories du comportement électoral, en comparant leur pouvoir explicatif aux préférences de compromis. Je souligne leurs limites explicatives puisque des attitudes intergroupes similaires à l'étude américaine ne peuvent être répliquées avec les données secondaires. Alors qu'une grande proportion de répondants refusent d'échanger l'un contre l'autre, je trouve des preuves qu'après le changement de régime juridique, les attitudes se sont cristallisées vers plus de confidentialité en 2019 par rapport à 2014, suggérant un effet modeste du côté de l'offre sur les attitudes.

Le premier chapitre établit l'historique et fournit une perspective d'économie politique de la façon dont le phénomène du complexe de surveillance s'est développé dans les démocraties avancées, menées par les États-Unis. Les trois chapitres sur l'opinion publique analysent les attitudes envers les différentes composantes du complexe de surveillance. La thèse jette les bases de travaux futurs sur la façon dont la normalisation (par exemple, aux États-Unis) ou la critique (par exemple, dans l'UE) de l'offre de certains types de surveillance contextualise la façon dont la demande des gens pour les politiques de surveillance prend forme. Un chapitre technique décrit les questions de l'enquête américaine et la distribution des réponses.

Contribution of authors

All chapters have been written by Isadora Borges Monroy.

Acknowledgements

Thinking academically about internet governance and technology policy has occupied half of my life. The internet has gone from an increasingly available technology to an inescapable feature of modern life. Around the early 2010s, I was authoring my first dissertation on the subject (an international political economy of the Web 2.0 paradigm). Pirate parties started in Sweden in 2006 were anti-copyright left-wing political organizations that seemed the epitome of hopeful digital politics. These organizations aspired to represent a ‘creative class’ (Florida, 2012) whose labor produced ideas, not things. Their politicians promised to change the power balance of productive relations from within advanced democracies’ parliaments.

I hoped this would come to be. It is said that ‘history may not repeat itself. But it rhymes’. I wondered, if the creative class was growing in size, and traditional parties were unwilling or unable to pivot to accommodate a rising social and economic class, would these parties become the (intellectual) labor parties of the 21st century?

At the same time, I struggled with technodeterministic optimism. I had already started reading disclosures about Facebook’s cross-tracking cookies, thanks to the Electronic Frontier Foundation. I was irked by their dismissive view of privacy and their underhanded ways of getting and profiting from personal data. I closed my account, started taking steps toward blocking cookies and ads, and I told anyone who would listen—starting with my parents, sister, and friends.

From my research, I became attuned to a meta-narrative. The Web 2.0 paradigm seemed to me a rosy PR way spinning the fact that we were all unpaid producers —of knowledge, of data, of labor, and the media we consumed, or *prosumers* (Toffler, 1980; Ritzer, Dean, & Jurgenson, 2012). At the time, I wondered whether this would change our relationship with the state, and, would change the state’s view of us. After graduating, I made a turn toward the state and the market. In my Masters, I analyzed the political process that produced the Digital Millennium Copyright Act in the United

States. I researched the shifts in lobbying power at the end of the 1990s, and the rise in Google's technological, political, and economic power. By trying to avoid gridlock and embarrassment in the courts, the US government had given the company inordinate gatekeeping powers to manage internet information. As the company grew to an international behemoth, American copyright was internationalized sidestepping diplomatic negotiations, WTO battles, or public deliberation.

To me, this seemed like an alarming gap in our understanding of how American soft power institutionalized the internet's way of operating. During my Masters, Edward Snowden's revelations rocked the Obama presidency. The man who had been awarded a Nobel Peace Prize before his presidency had started had been accused of waging a covert extrajudicial assassination program through drone strikes in the Middle East. In retaliation for disclosures of the War on Terror, his administration had prosecuted journalists and whistleblowers, downplaying events and highlighting his persona as a thoughtful man who could be trusted, especially when these programs replaced the ugliness of American boots on the ground. Disillusioned with his U-turn on "hope and change", Snowden took massive amounts of evidence with him and put a mirror up to the administration's reliance on mass online surveillance to run their War on Terror with fewer boots on the ground, the deputized companies' complicity, and the Judicial and Legislative's pusillanimous deference to intelligence gathering claims and justifications, if they were (exceptionally) proffered.

At the University of Chicago, I witnessed firsthand the President's alma mater accommodating the institutional status quo. One of the school's law professors, Geoffrey R. Stone, a First Amendment champion¹ former dean of the Law School, and previous critic of the "trust us" record of the administration (Stone, 2011), was recruited to an advisory panel. The five-panel members, intelligence and legal experts, were given classified access and heard from senior

¹ An advisor for the American Civil Liberties Union, author of a 2004 book on wartime free speech, he has also been criticized by his students for using the n-word in class to incite a discussion of the fighting words doctrine.

administration officials. They were thanked for their recommendations and the exercise in deliberation ended there. Professor Stone then went on a small tour around campus and outside discussing the process. I witnessed two similar speeches justifying the President's use of secrecy and the surveillance programs, while he penned letters reflecting the administration's position that Snowden had carried out illegal dissemination of state secrets—even if the policies were worth criticizing.

The whole series of events struck me as kabuki theater. The experience of being so close to the institutional mobilization of justifications was sobering. The fact that the recommendations were not binding and were quickly laid aside was edifying. A law professor whose reputation on wartime dissent was willing to judge a whistleblower guilty without trial, knowing that the espionage charges leveraged against him excludes a public interest defense. The recommendations in the report validated concerns about lack of oversight, but his public discussion echoed Obama's own pleas to "trust us".

This experience happened the summer before I started my Ph.D. with Dietlind Stolle. The Ph.D. proposal, at first a study of voter support for Pirate Parties, quickly became a pursuit to understand a bigger question: who cares about privacy in democracies? While the focus of the project has sharpened with time, I have been, stubbornly perhaps, steadfast in my desire to drag Political Science into a debate about something conspicuously absent in the literature: countries that are supposed to be democratic engage in mass online surveillance. Do they do this because they have the support of many, despite popular opposition, or because few have clarity in what is going on?

I want to thank my parents, Guilherme and Zuraya, as well as my sister Rebeca for their deep care in my work, their encouragement, support, and love. My parents, stellar academics in their own fields, have been a well of inspiration. I admire them and I know they are delighted that I am successfully concluding this stage of my research. My aunts and uncles, cousins and friends, Sofia, Ana Laura, Maria Fernanda, Begoña, Valeria, Paulina, Mariana, Gabriela, Laura—many of whom I've even

managed to get on Signal! Being in touch across the years and throughout all my moves has been wonderful.

Dietlind Stolle, a tireless supervisor, encouraged me throughout the program to pursue my passions with academic rigor. She always took my flights of fancy seriously but grounded me in ways necessary to keep the project on track. Her exacting standards made this dissertation a labor of love, I am so thankful that she took me on, and encouraged me to develop many methodological and intellectual skills to turn this manuscript into an innovative contribution to the field we can both be proud of. Dietlind has also fought for invaluable financial resources that kept me afloat through this long process, I am forever grateful.

I want to thank my committee members, Krzysztof Pelc, Gabriella Coleman, and Alison Harrell for their insightful critiques, ideas, and suggestions for the dissertation. McGill University and the Centre for the Study of Democratic Citizenship, where all three have been members of one of these organizations, provided me with incredible resources and opportunities to discuss my work and hear important challenges to my claims that have made the studies stronger. Leonardo Baccini, Elizabeth Gidengil, and Maria Popova gave me time and invaluable insights into the dissertation research. I am also grateful to Daniel Pemstein, defense external member, for his encouraging review.

At the CSDC and McGill, I met many wonderful students, professors, and guest speakers whose work inspired me. Thank you to the great friends I met there, Olivier Jacques, Aengus Bridgman, Costin Ciobanu, Julia Maynard, Edana Beauvais, and Scott Patterson. Summers of methodological training at ICPSR and in Germany, supported by the CSDC were instrumental to my empirical work. The Fonds de Recherche du Québec opened their grants to international students during my studies, and I was encouraged when I received a fellowship to develop my research proposal. The Faculty of Arts and the Graduate Program Studies have also provided me with support throughout my doctoral studies for which I am immensely thankful.

Immobilized or petrified? Explaining privacy concerns and the (de)mobilization against mass online surveillance in 21st-century advanced democracies

The use of mass surveillance in a democracy should be an oxymoron. Why? Because carrying out mass surveillance requires a subversion of many democratic principles, problematizing whether a country can remain democratic while engaging in undemocratic behaviors. And yet, after 20 years of the “War on Terrorism”, scores of documents obtained through freedom of information requests, whistleblowers, court cases, Congressional testimonies, and investigative journalism and security research demonstrate mass online surveillance is widely practiced throughout countries labeled “advanced democracies” by political scientists.

For a policy of such magnitude, the field has not prioritized its study, behaviorally or institutionally. This dissertation sheds light on preferences over a range of surveillance practices that construct what I call “the surveillance complex”, particularly emphasizing public opinion in advanced democracies where governments deputize companies to conduct data collection and analysis or even engage with law enforcement directly. This dissertation will introduce the concept of the surveillance complex and its elements, historicizing its edifice and the influence of its American origins. I also provide an alternative political hypothesis as to why regulation of surveillance practices has been slow-coming—particularly in America as Europe begins counter-balancing its excesses. Because governmental and corporate mass online surveillance has not been systematically studied in Political Science, I use this introduction as an opportunity to justify the study of these practices, how they influence the supply side (e.g., policy implementation and/or regulatory forbearance), and more importantly, the role they also play in shaping the demand-side (e.g., public opinion). For example, I briefly preview how *efforts* to keep policies away from public scrutiny (e.g., institutions, journalists, and

citizens) could be detrimental to the health of advanced democracies, calling on the field to rethink the predominant narrative of when democratic backsliding began.

For a time, government institutions worked toward boosting the available supply of surveillance technologies while tamping down on demand for privacy by avoiding journalistic scrutiny. Studies of post-9/11 surveillance public opinion studied attitudes toward policies that were neither confirmed nor denied. With little hard data on what policies were in place, the area languished and was not revived after Edward Snowden's cache of evidence. How do Americans feel about mass online surveillance? Do their attitudes change when governments deputize companies into monitoring, making the data accessible, or even notifying law enforcement? How do these attitudes differ from direct government surveillance and commercial services' consumer targeting practices? Are attitudes influenced by the criminalization of disliked groups? Europeans' reaction to Snowden's evidence produced institutionalized data protection changes, including redefining harms, avenues for redress, and financial penalties for companies. Did their privacy concerns increase after Snowden, producing a mandate for European politicians? What types of Europeans are most concerned with privacy? Have European citizens 'regressed to the mean' before the revelations, or have they changed in with these new rules? I provide answers to these questions throughout the dissertation. In this introduction, I summarize the dissertation's objectives, outline the methodology to answer these research questions, as well as by foreshadowing the main findings of the dissertation chapters.

The term "advanced democracies" comes from Ronald Inglehart's post-modernization theory. The concept has always been relational since it produces a hierarchy among liberal democracies, with Global North liberal democracies "above" Westernized regimes from the Global South². The term

² For example, the US and all Latin American countries are western liberal democracies in that they drew from similar European liberal traditions. Latin American countries banned slavery and racialized voting privileges earlier. Yet, the US is normatively "elevated" by Inglehart as an advanced democracy because many of whose countries were emerging from (US-backed) military and one-party regimes of competitive authoritarianism in the 1990s.

sprung in the 1990s when Global North democracies were categorized as advanced compared to newly democratized and democratizing countries. They were labeled democratic compared to the Cold War regimes' upheaval³.

Throughout this dissertation, I use this term of art tongue-in-cheek to highlight the gap in expectations about American and European aspirational governance of surveillance and its clash with their practices. I use the expression “advanced democracies” to juxtapose and jolt the reader out of our assumptions and to expose significant normative shortcomings derived from mass surveillance’s subversive effect on democratic principles. The US, in particular, is facing a deep crisis in democratic governance, with international political economy and tech governance implications reverberating across the globe. Yet, “advanced democracies” are still considered pinnacles of democratic governance. Their implicit moral gravitas gives way to international relations, where they still advise others on being reputedly democratic, despite their backsliding and other systemic governance shortcomings⁴.

What do democracy and democratic backsliding have to do with mass online surveillance? In my estimation, a lot. The answer to this question also points to why the field of political science should study democracies’ engagement in mass (online) surveillance, not just autocracies’. First, adopting mass surveillance techniques in advanced democracies should have been the first alarm in democratic deconsolidation. I argue this because, at its core, mass surveillance is a technique of socio-political dominance to incentivize and monitor compliance. For example, in *The Origins of Totalitarianism*, Hannah Arendt describes how “totalitarian regimes proclaim the nonexistence of privacy” (footnote 36) because “the private interest [must be] the same with the public [interest]” (1951, 168). In her

³ The term ‘competitive authoritarianism’ is a post-Cold War classification distinguishing democratic governance to countries with procedural voting but autocratic governance (Levitsky and Way 2010).

⁴ Hand-wringing over backsliding has generally, 1) misplaced the date around the Trump election, ignoring important bulwark dismantling that has occurred during the W.H. Bush, Obama and Biden terms, which in turn allows academics and pundits to 2) imagine that threats’ fruition are looming instead of already happened/happening.

historical recounting, she describes how “[t]otalitarian bureaucracy, with a more complete understanding of the meaning of absolute power, intruded upon the private individual and his inner life with equal brutality” (idem, 265). This intrusion into private life to ensure loyalty and compliance with the totalitarian regime is institutionalized. “After a few years of power and systematic coordination, the Nazis could rightly announce: ‘The only person who is still a private individual in Germany is somebody who is asleep’” (idem, 344).

As I contend in Chapter 3, when journalists disclosed mass surveillance policies to the public, both the Bush and Obama administrations quickly told the domestic and international publics that the policies were ultimately targeted and, thus, should not be of concern. Everyone’s data, they claimed, wouldn’t matter—only criminal minorities’ data (terrorists, but leaving the door open to others) would be used. This ‘reframing’ or redefinition relates to intergroup dynamics I explore in Chapter 3. Indeed, people are much more accepting of mass surveillance—even of their favorite groups—when they are reminded of criminals or similarly threatening groups, partially explaining the demobilization of citizens even when surveillance practices are no longer secret.

The pervasive spread of surveillance practices has largely still flown under the radar of democracy scholars (Diamond 2015) and is even absent in the competitive authoritarianism literature (Levitsky and Way 2010). Mass digital surveillance practices have received little scrutiny, and existing research is trained almost exclusively on China (Byler 2022, King, Pan and Roberts 2014, Strittmatter 2020, Chin and Lin 2022)⁵. The logic of visibility of autocratic state surveillance will likely be inverted in democracies. One can imagine that authoritarian states could feel incentivized to publicize their surveillance. Even if the technology isn’t all-seeing, it produces a “strong state” image to domestic and international audiences favorable to some authoritarian regimes. In contrast, democratic states are

⁵ A few examples are notable because of the paucity of research. These were published on the heels of 9/11 when many of the US programs’ details were not disclosed in detail and thus “theoretical”. Chapter 2 goes discusses their findings and limits in detail.

likelier to have an incentive for secretiveness to avoid public scrutiny and democratic backlash⁶. The historical record, denial, and downplaying technology suggest these considerations may come into play.

For example, most policies that opened the door for—and later entrenched—mass online surveillance’s use began with secretiveness⁷, depriving the body politic of deliberation (Gellman 2020, Schneier 2018, 112). Some arrangements were institutionalized through legal requirements for data retention,⁸ some through contractual (data-buying) arrangements between agencies, and others through ambiguity and forbearance.⁹ I provide examples in Chapter 1. These yielded an institutionalized breakdown of republican “checks-and-balances” and insulated decisions from voter-driven accountability, which I also discuss in Chapter 1. Inter-branch oversight practices ceded ground to accommodate an expanding view of how war is conducted in deference to the Executive branch and the intelligence agencies within them (Rosenzweig 2016, L. K. Johnson 2017, Ackerman 2021). This expansion made space for an “importation” of military tactics for domestic policing at the federal and local levels¹⁰ (Coyne and Hall 2018, Schuba and Main 2021). Deployment of unmanned drones and rendition—tactics developed during the War on Terror—, were made visible in the US during the

⁶ This ‘invisibility’ does not, however, explain why Political Science scholars have been less attentive to the use of mass surveillance in democracies, since other fields like Sociology, Criminology, and Communications have been attentive to its use.

⁷ In my view, autocratic states have an incentive to publicize their surveillance because it helps produce a “strong state” image to domestic and international audiences, even when the surveillance is not accurate. In contrast, democratic states have an incentive for secretiveness to avoid public scrutiny and democratic backlash.

⁸ For example, the PATRIOT ACT required new financial transaction data retention and deputized background checks against a Foreign Assets Control list (314A) or risk liability, while barring banks from disclosing if suspicious activity triggered an investigation (Runzel 2019).

⁹ See Chapter 1 for a discussion of legislative and regulatory language explicitly codifying the hands-off approach.

¹⁰ The erosion of republican checks and balances between the federal horizontal branches has also been accompanied by an erosion of federalist checks and balances, horizontally, between the national branches and the state and local branches. An example of the horizontal fusion of executive branches takes place is Section 1033 of the National Defense Authorization Act of 1997. It lets Department of Defense transfer excess military property to state and local police departments. It is estimated that transfers in 2020 totaled \$1.6 billion since 9/11, compared to \$27 million before the attacks (Katzenstein 2020).

2020 Black Lives Matter summer protests (Kanno-Youngs 2020, Schmitt and Gibbons-Neff 2022, Levinson, et al. 2020, Sanchez 2020).

Perhaps the techno-utopian¹¹ zeitgeist of the 2010s blinded political science academics to the cracks of digital technology. The field encouraged attention toward the democratizing aspect of digital technology as the Arab Spring and Occupy movements brewed online. But as the mood towards tech writ large turns somber, it is time to reevaluate the intellectual underpinnings, political choices, and effects regarding democracies' use of mass online surveillance, mainly via deputation.

Clues that this was happening were out there, but the information was mainly circulating in outlets for civil liberties-oriented tech observers, like the Electronic Frontier Foundation (Reitman 2011). When hard evidence was produced in such quantities that denials and deflections became unsustainable, the surveillance complex had been reified. Edward Snowden was not the first to reveal elements of the surveillance complex, but he was the first to take evidence with him (Hertsgaard 2016, Welna 2014).

Whistleblowers like Bill Binney, a leading NSA crypto-mathematician, and Thomas Drake blew the whistle on mass surveillance programs¹². Their cases, which I recount in Chapter 1, drew less media attention for several reasons. First, they began their efforts through the legally prescribed internal whistleblower process. With this 'advanced notice', the Bush administration discredited their accusations. When the media paid some attention to the allegations, the administration pointed to a lack of documentary evidence, omitting that they were prohibited from taking it—a lesson from which Snowden seems to have learned (Bruder and Maharidge 2020). The administration had also caught on to newspapers' wariness to publish stories critical of the war effort without giving the government a chance to comment (Ackerman 2021). When the administration refused to comment on stories,

¹¹ Technological utopianism is a deterministic view that technology will advance social progress.

¹² Former NSA officials Kirk Wiebe and Edward Loomis, and a former senior Congressional staffer, Diane Roark, also signed the complaint.

outlets like the New York Times declined to publish—until after Bush’s wartime reelection¹³ (Risen and Lichtblau 2005). Denials and undermining did not stop the Bush and Obama administrations from prosecuting them.¹⁴ Would Bush have lost the 2004 election if mass surveillance programs had been disclosed? In an alternative universe, the administration could have tested mobilizing voters’ anxiety and threat, mainstreaming acceptance of the policies during the initial stages of the War on Terror (Garcia and Geva 2016, Huddy, et al. 2005).

Governments and deputized companies have mobilized to minimize the *public’s concerns* over how the surveillance complex can impact procedural democratic governance, justice, equality, voice, and participation (Salinas and Balakrishnan 2018, Graff 2016, H. A. Popkin 2010, B. Johnson 2010, B. Johnson 2009, Schneier 2006). They have not made similar endeavors to minimize these procedures’ harmful impacts on said spheres. All this necessitates revising our understanding of how democratic guardrails have been weakened beyond electoral competition.

Efforts to divert attention carried on during slightly more than half of the War on Terror’s data surveillance policies (2001-2013). In Chapter 1, I detail these efforts, and I highlight several issues that the study of mass surveillance in democracies should consider going forward. First, it is highly improbable that the surveillance complex, which allows governments to access commercial data, was edified by a series of accidental omissions of regulation; the government’s reaction to media and whistleblowers reinforces this conclusion. Second, politics played a much more significant role than

¹³ The piece explains “The White House asked The New York Times not to publish this article, arguing that it could jeopardize continuing investigations and alert would-be terrorists that they might be under scrutiny. After meeting with senior administration officials to hear their concerns, the newspaper delayed publication for a year to conduct additional reporting. Some information that administration officials argued could be useful to terrorists has been omitted.” Risen was about to publish his book, where he would disclose the program. This moved the New York Times to publish, lest it be scooped by its own reporter. Bush and Obama administrations both demanded — under threat of imprisonment — the name of one of Risen’s sources (Risen 2018).

¹⁴ The Obama administration’s record is no better. His administration oversaw a higher number of prosecutions for whistleblowers and journalists—Snowden’s foresight in taking evidence with him made it harder to deny the policies in place but that did not stop them from trying, for example, to claim that Americans were not surveilled (only for documents to directly contradict the claims).

the market-driven narratives of surveillance capitalism allow for (Zuboff 2019). Third, efforts to squash media stories shaped readers' information ecosystem: citizens did not get a candid picture of the extent of deputized surveillance (and the surveillance complex) before Edward Snowden's revelations forced the issue. Chapters 2, 3, and 4 focus on measuring and explaining American and European public opinion regarding the surveillance complex, particularly deputation, the role of intergroup relations, and framing privacy as antagonistic to domestic security.

The continuous media coverage he generated forced all branches of government to publicly defend their previous deference to the expansive intelligence apparatus, military exceptionalism, and forbearance. Deputized private firms issued apologies and justifications for handovers/collaboration out of fear of losing customers (Kiss 2014). And yet, ten years after Snowden made "out of sight out of mind" impossible, the Political Science field has unfortunately been slow to pivot to a systematic study of the surveillance complex and the issues it raises, particularly in advanced democracies.

As discussed above, one of the defining characteristics that separated advanced democracies from democratizing countries in literature was their "longstanding"¹⁵ commitments to principles of democratic government beyond procedural voting, like equality, the rule of law, freedom of speech, and assembly. However, the turn toward mass online surveillance has jeopardized these commitments. This situation should be incorporated into indicators of democratic backsliding more systematically. Surveillance tools, like network analysis of online speech and offline movements, subvert freedom of speech and assembly (Guo 2016). Monitoring makes justice a privilege by treating everyone guilty until exonerated by surveillance (Boghosian and Lapham 2013). Only the totality of surveillance evidence clears individuals of amorphous crimes, determined after the surveillance data is analyzed (Solove 2011). Due process elements like the right to know your accuser and confront them in a court of law with exonerating evidence are hindered.

¹⁵ The United States' Voting Rights Act passed in 1965.

Other elements of a public trial, like an account of the integrity of evidence through transparent chains of custody and prohibitions on ill-gotten evidence (fruit of the poisoned tree), cannot be taken for granted when this type of surveillance is used. These subversions are a departure from inter-branch oversight and rights frameworks, where rights are only suspended after a court procedure finds someone guilty of a crime, after a public accusation is made, and evidence, with transparent chains of custody, are considered.

The ability to accumulate mass behavioral data without probable cause, which can be retroactively queried¹⁶ to look for aberrations, deviance, etc., is an innovation in criminal and social norm enforcement. Observers critique how it incentivizes individual compliance with the status quo (Gellman 2020, 172, 326) and has significant repercussions for democratic deliberation¹⁷ (Guo 2016). These are some of the cornerstone principles of democratic justice that mass online surveillance upends. The effects of all these subversions on principles of democratic governance, however, are infrequently explicit in the deliberation over mass surveillance policies' implementation and have not been systematically addressed by the political science field¹⁸. These critical issues of justice and rights are beyond the scope of this dissertation, but it is essential to justify why the field should take a holistic approach to the study of democracy's use of mass surveillance. Future research should endeavor to

¹⁶ For example, because Google collects and keeps a range of device location, search data and other browsing behaviors of everyone that interacts with its services, in what it calls a "Sensorvault", police departments have begun querying it to go back in time and produce a list of people around a radius (of unknown dimensions) on a location of interest. Chapter 1 details this program. Departments have claimed these warrantless requests are for criminal cases but there is no court or authority outside or inside Google has to verify the claims. The fact that law enforcement does not "have" a physical dossier on every individual under static storage, even though it can produce an updated one on a whim, was a loophole claimed by National Security Agency director Keith Alexander in 2012's Defense Conference (Def Con) (Gellman 2020, 170-172, Zetter 2012).

¹⁷ One of the arguments against the perfect enforcement of current or future laws (e.g., whatever comes of Dobbs in anti-choice states) that is afforded by mass digital surveillance is that organized resistance against unjust laws necessitates breaking the law. Snowden cites civil rights and social justice movements like "women's suffrage, desegregation, the right to form unions, gay marriage" as relying on "organized resistance against the law of their times. The Underground Railroad could not have run in a time of pervasive surveillance. The same could be said of the American Revolution. They [the founding fathers] wouldn't have been able to coordinate. They would have been individually popped off the street and thrown in King George's jail. Comprehensive transparency in service of comprehensive law enforcement would mean freezing in place the status quo of that society forever" (Gellman 2020, Transcription of interview with Snowden, 326).

¹⁸ Legal scholars have been active in this area, but the effects of these legal changes on normative and empirical politics remain underexplored.

understand how people's opinions of the surveillance complex interact with attitudes toward criminal justice. I hope the empirical work of this dissertation helps to shape this research agenda.

Finally, mass online surveillance, by definition, collects everyone's data. This is a guidepost for the dissertation. I, therefore, avoid minimizing that defining characteristic for a scope-limiting harm-based approach (Citron and Gray 2013, Solove and Citron 2021). Nevertheless, surveillance data can be used for *subsequent* abuse of power in law enforcement. In other words, surveillance might gaze upon all, but it lingers on some more than others (Federman 2019). Using mass surveillance data, local, state, and federal agencies can decide what categories of people are further scrutinized in subsequent processes. The picture that has emerged from the data that has become public is a system that reinforces the over-policing of marginalized communities and political activism (Passavant 2021)¹⁹.

Surveillance is a political choice about how asymmetrical power relations are practiced²⁰. From this understanding, governments' reluctance to regulate (forbearance) and enforce regulations does

¹⁹ Techniques of deputized online surveillance seem to be compounding. The copyright mechanisms that inaugurated online surveillance deputation in the late 1990s have now been leveraged against police accountability efforts by citizens who record law enforcement. Following a wave of citizen journalism documenting police brutality and disseminating it online, American police officers have begun playing Disney-owned music while being filmed to trigger the automated systems Google's YouTube uses to take the content offline (Lancaster 2022).

²⁰ Historian Sarah Igo argues privacy has always been a product of asymmetric power relations. In the 19th century privacy was linked to "an idealized bourgeois realm of domesticity", serving the patriarch and excluding female members and the household's working class employees (2018). Then, like now, technology (cameras) and aggressive journalism (Warren and Brandeis 1890), threatened the idea that men would be able to exercise their right to privacy, and the Supreme Court responded by tethering "the sanctity of a man's home and the privacies of life" and "his indefeasible right of personal security, personal liberty, and private property" (Igo 2018). In the 20th and 21st century, this power asymmetry is clearest in debates over sexual orientation and reproductive rights, where straight men legislate or rule in courts over homosexual and female bodily autonomy in ways that have no corollary to their own sexuality and bodies. The feminist retort to the idea that men's home was their castle, and they were sovereigns within it was that "the personal is political". The modern American interpretation of a constitutional "right to privacy" was derived from several court cases around contraception and access to privately held obscenity (e.g., Griswold v Connecticut 1965, Stanley v Georgia 1969, Roe v Wade 1972). In the 21st century, as many of our political, financial and social interactions become digitized, the debate over how privacy should be construed and the limits to its implementation in online spaces and through digital affordances has revived the idea that power asymmetries permeate the debate. Debates over freedom of speech come to a head with the right to privacy in the matter of search algorithms (right to be forgotten (Jones 2018)) and non-consensual distribution of nude materials (Taube, Kolmes and Vogeles 2014) or to distribute software that facilitates stalking (Greenberg 2019). Power continues to be endogenous to the

not seem accidental. Because mass surveillance is not usually overtly articulated, the lack of transparency and unaccountability makes it challenging to place it on the electoral agenda. This is another reason why its study as a public opinion topic has eluded Political Scientists.

Policies regarding how mass online surveillance is operationalized reflect a political choice, but the self-serving incentives to shield them from political accountability beget low electoral competition. This produces a vicious cycle where concerns are delegitimized and politically ignored while technologies are economically supported. It is essential to consider that reliance on deputized surveillance obscures responsibility. So far, this element in the political choices surrounding surveillance has been unarticulated²¹.

The surveillance complex is a web of relations within and, significantly, *between* market firms and governments. Each actor has its logic and surveillance techniques that it carries out within its sphere of action, which I distinguish as “government-exclusive surveillance” and “market-exclusive surveillance”. Many siloed dynamics have been dissected in sociology, criminology, economics, and business school studies. Communication scholars have taken up studying political and social activism’s

definition of privacy rights, and its enforcement, as the US Supreme Court Dobbs decision reversing Roe V. Wade reflects. Law professor and Biden White House anti-trust advisor on the National Economic Council, Tim Wu, pins the rise of the 20th century’s relatively widespread privacy expansion to “the 1960s rise of a propertied middle class [which] had put each man in his ‘castle’, each drinker in his saloon, each worker in his own office and each child in her own bedroom. Private physical spaces, along with semiprivate spaces like motels, bathhouses and dance clubs, created their own expectations of privacy”. In turn, he diagnoses the winding down of private spaces to the “forces of wealth creation [who] no longer favor the expansion of privacy but work to undermine it [through] ‘attention merchants’” (Wu 2019). Management Professor Peter Bloom argues that Cambridge Analytica highlights how data-mining practices ensures monitored subjects are nested in unaccountable capitalism. Ordinary citizens are monitored but the politically well-connected operators of the data-mining group (Facebook, the Trump campaign, Cambridge Analytica, and its conservative financiers) were held to no outside scrutiny over their practices and no criminal charges after the two whistleblowers (Wylie and Kaiser) came forward. In Bloom’s analysis, this creates an asymmetric relationship of privacy for the powerful, surveillance for the rest (2019). These interventions depart from Shoshana Zuboff’s claims that profit-maximizing corporate concerns set the stage for surveillance practices (2019), which incidentally produce negative externalities, a narrative that minimizes the role of governments in shaping the market and protecting (or exposing) citizens.

²¹ By relying on deputation to operationalize part of its mass surveillance policies, governments in advanced democracies are expanding the scope of asymmetrical power relations between governments-citizens and firms-consumers, to a triangulated government-firms-individuals power relation.

use of communication technologies (Coleman 2014, Schradie 2019). It is natural that academic focus has bifurcated into their respective matters of interest and brought their intellectual tools and expertise towards analyzing the actors and dynamics they are trained to study. However, we should not expect these fields to produce research that puts politics squarely at its center, as political science would.

The surveillance complex aggravates power dynamics in government or market surveillance because it makes it impossible for individuals to have certainty over the source or purpose of surveillance and thus do something about it collectively. If companies conduct deputized surveillance but only at the government's behest, which is to blame? Gellman succinctly articulates this frustration:

Because of that secrecy, even the best-informed journalists and policy analysts had no information on the way PRISM worked. Plaintiffs could bring no constitutional challenge in federal court. Congress faced no public pressure, and big internet companies encountered little demand for stronger defense of privacy. Voters and consumers could not ask for change because they did not know the truth (2020, 126).

Deputized mass online surveillance reinforces political and economic incentives for the body politic to keep surveillance capitalism deregulated and outside institutional oversight. As long as companies also conduct mass online surveillance for their gain and face few regulatory constraints, they will maximize their ability to collect more data ("big data"). Governments can stick their hand into the cookie(s)²² jar by inducing or compelling data sharing or covertly hacking their way in (Schneier 2018). Governments can shirk political accountability when companies act as data intermediaries or keep their data unencrypted, producing troubling consequences for democratic rule. And, as long as governments keep commercial data practices deregulated, companies can shirk shareholder accountability or consumer lawsuits. These dynamics reinforce a quid pro quo that individuals—as

²² Cookies are one way in which unknowable amounts of substantive online behavior data and metadata are collected. This is play on words is as irresistible to me as a jar of actual cookies.

citizens or consumers—are unable to impact solely through independent economic choices (e.g., boycotts). Organized political pressure to regulate the surveillance complex may be the only remedy for people who hope to regain their privacy.

There have been some recent contributions from Political Science, particularly European public opinion (Friedewald, et al. 2014, Garcia and Geva 2016, Krueger, Best and Johnson 2020, Ziller and Helbling 2020, Zhang, Kreps and McMurry 2020). However, these works have mostly focused on government surveillance. But the field can, and should, contribute to studying the interaction between markets and governments as a political economy of surveillance. For example, researchers working on political communications in democracies have analyzed how political campaigns use citizen data (Hersh 2015).

Political campaigns in the US usually involve candidates—incumbents²³ or outsiders—who contract private firms that already hold (e.g., Facebook) or can gather (e.g., data brokers) data on prospective voters. The Cambridge Analytica scandal highlighted how campaigns use this data to mobilize sympathetic voters *and* demobilize antagonistic voters²⁴. The biggest beneficiaries of campaign surveillance—candidates who win—end up deciding whether or not to regulate companies engaging in corporate and deputized surveillance. However, Political Science research on political campaigns’ use of data has so far shied away from analyzing it as a process embedded in a surveillance complex or raising the prospect of a regulatory conflict of interest²⁵. In this regard, political campaign research implicitly treats parties and candidates running for office as separate from the parties and

²³ I mention this because it highlights the point that those already in government use surveillance data for their campaigns. Reelection rates among incumbents exceeds 80% (Open Secrets 2022).

²⁴ Cambridge Analytica whistleblowers disclosed that the Trump campaign, at the behest of Steve Bannon, targeted Facebook ads to Black voters that were designed to demotivate them from voting at all, instead of motivating them to vote Republican, because they were considered impossible to entreat to vote for the nominee in 2016 (Solon 2018).

²⁵ We end up with moments of political kabuki where Senate Judiciary Committee members like Orrin Hatch, a senator since 1974, publicly asks Facebook how it makes money. Zuckerberg’s response “we sell ads” is unlikely to produce a follow-up from the Senator up if those ads include RNC and DNC political ads.

lawmakers who have the power to legislate more stringent privacy rules. Research on lobbying from data brokers on regulatory outcomes is also absent.

The emergence of a political economy of surveillance subfield could be one way to systematize research questions, measurements, and findings between fields of research that focus on state or corporate surveillance. It could also further study the politics of the surveillance complex, including deputized surveillance, the development and ownership of techniques and infrastructures, political and economic incentives, and political costs of surveillance from domestic and comparative points of view. It is my hope this dissertation plants a path forward.

Political Science also has valuable methodological and substantive contributions to make by placing citizens, their voice, and power (or dis-empowerment) at the center of research on surveillance techniques. Comparative scholarship is needed to analyze regime-type (i.e., autocratic, backsliding, and democratic) structures and the impact of political pressures on a future “fragmented” internet. International Relations scholarship would enrich our understanding of how diplomatic, intelligence, commercial, and military competition and alliances shape the political economy of mass surveillance technologies, contracts, and international norms normalizing or stigmatizing online surveillance of whole populations. Political theorists’ interventions are also needed: can countries remain democratic while engaging in non-democratic behaviors? Or, to misquote Richard Nixon, is it democratic when democracies do it?

Dissertation overview

Our understanding of advanced democracies’ online surveillance practices, where privacy rights are assumed to be universal and irrevocable, is sparse. Chapter 1 of this dissertation produces a research agenda to fill some of our knowledge gaps. Its political economy perspective seeks to entwine the previously bifurcated attention on *either* state surveillance *or* surveillance capitalism. The risk of siloed research is that it insinuates mutually exclusive practices, could produce incomplete or contradictory

findings, and even apolitical understandings of the proliferating surveillance complex. Monitoring (i.e., “just” observing), data collection, analysis, exchange, and aggregation all take place in the surveillance complex, but focusing on one sphere at the cost of the other can atomize these practices until they are so reduced that the full scope of the problem is trivialized. In this dissertation, I take on the challenge of producing a perspective that discusses how state and market surveillance interact through deputized surveillance. I give evidence of how this interaction creates a surveillance complex, arguing that insights can be gained from studying how surveillance is carried out beyond what happens within each sphere (e.g., surveillance capitalism).

Building a surveillance complex is not the product of a one-off centralized decision. I describe the historical roots that have led up to this intertwining of political and economic incentives and costs by analyzing post-World War II political demands for a state that was administratively small but militarily hefty. The arrangements were exacerbated by neo-liberal demands for further reduced state budgets. After 9/11, public commitments to pursue a war against Muslim terrorism leveraged technologies of data and metadata monitoring developed by private actors. Chapter 1 analyzes the political and economic incentives and coercive elements of deputized surveillance spearheaded by the US government on its large technology firms (or “Data Goliaths”, to borrow from cybersecurity expert Bruce Schneier).

I document some critical moments in its institutional propping up and efforts to keep government policies and companies’ deputation out of public scrutiny. In Chapter 1, I describe how reduced inter-branch oversight, minimal open institutional deliberation, and almost little political competition between parties in the US (on this topic) can influence public transparency of deputized surveillance policies. I trace those patterns to historical conditions, people, and organizations emerging after World War II. I provide evidence of forbearance, refusal to regulate, and deregulation, instantiating how the federal Executive branch has imposed itself on inter-branch oversight.

I also describe the techniques of the surveillance complex in detail, disentangling favorable incentives shaping the market's supply of technologies and data (carrots) and coercive deputation via legal requirements (sticks), in addition to the brute-force or backend access that has been a historic part of spy craft in government surveillance.

One of the ways deputized surveillance mechanisms and procedures are kept out of public deliberation has been a continuous and bipartisan reluctance to regulate them. This is a unique way of conducting public policy and I argue that this justifies particular attention to public opinion on the subject, given the informational environment. That is why almost all dissertation chapters study public opinion on the erosion of privacy in the face of mass online surveillance. Chapter 1 puts forward contextualizing evidence to justify the claim that mass online surveillance has been a pervasive *policy* outcome. It is juxtaposed to alternative apolitical explanations like the idea that mass surveillance is the byproduct of profit-maximizing markets which have accidentally gone unchecked (cf. Zuboff 2019).

The historic and contextualizing evidence matters to this dissertation. The absence of institutional scrutiny, elite dissenting speech, or factional heuristics (e.g., partisan cues) about decision-making and the implicit legitimization of outcomes around the surveillance complex could lead citizens to think themselves alone in, or even ostracized by, their concerns towards mass online surveillance. The overarching institutional preference for secrecy in erecting the surveillance complex may have fostered decades-long indirect delegitimization of citizens' privacy concerns. Without a counterfactual, the absence of information on the voting public for such a long period is hard to assess. Public deliberation has instead been shaped by moments of crisis, like security crises like 9/11 in the US and European domestic terrorist attacks, privacy crises, the Snowden revelations, or sporadic

revelations of cyberattacks and data theft. Public opinion might thus be reactionary instead of forward-looking²⁶.

The US' lack of government regulation has given some observers the impression that the technologies of surveillance flow solely from market incentives, which prioritized free-flowing data as a function of a lack of consumer demand for privacy (Dempsey 2023). The underlying assumption that market forces are the leading actor shaping technological capacities is at the core of Shoshana Zuboff's concept of surveillance capitalism (2019). This interpretation would lead to an over-focus on public opinion attitudes toward market surveillance at the cost of measuring citizens' opinions on their government's use of commercial data, whether purchased or obtained, as a legal requirement. I produce evidence emphasizing the existence of deputation as a political choice in Chapter 1 to justify the public opinion research on this phenomenon in Chapters 2, 3, and 4 in the dissertation.

I diverge from this apolitical interpretation, motivating my focus on why the study of public opinion of mass online surveillance should consider the political decisions of governments in shaping the marketplace where most individuals' data is collected. Namely, I point to the role of advanced democracies' governments in shaping the market through deregulation, forbearance, R&D investments, patent regimes, and, crucially, the deputation of companies for their own surveillance goals. These are understudied factors in understanding citizens' opinions of the surveillance complex. A more holistic analysis of public opinion requires a more nuanced understanding of the surveillance complex and its political economy.

Democratic representative governments derive their consent from the people, which in turn requires a public capable of democratic deliberation (minimally informed if possible) to legitimize political decision-making on their behalf. Given the institutional constraints on surveillance

²⁶ European regulation seems to be diverging from American forbearance by taking a proactive planning approach to the digital economy and the data collection that requires/produces.

information, people living in advanced democratic regimes face obstacles in being informed by their governments about particular aspects of mass online surveillance policies, especially deputized surveillance. In the first chapter, I introduce several events and policy decisions to support my view that American political institutions have engaged in forbearance to accommodate “intelligence exceptionalism”, obscuring surveillance policies and practices from public accountability throughout the post-war period.

The chapter diverges from the dissertation’s overall focus on political opinion to ground how the surveillance complex works and to underline why my work on public opinion contributes to surveillance/privacy studies and Political Science. I pay particular attention to describing the bridging interaction of the American government and market via surveillance deputation. Secondly, I put forward a functionalist interpretation explaining why governments have failed principled hand-tying (Elster 2000). In doing so, I set the stage for the particular conditions of public opinion: the electorate has been informed of many key elements of the surveillance complex from forced governmental and corporate admissions after cybersecurity researchers, journalists, and journalists whistleblowers have produced post-facto evidence. This sets it apart from other public opinion research, where electoral competition increases the availability of information on policies, party positions, corporate preferences, etc.

The first part of the puzzle on public opinion of mass online surveillance is investigating people’s normative preferences. Independent of whether people are aware mass online surveillance policies are currently in place, what are their policy preferences? Furthermore, do attitudes towards policies that use *deputized* mass online surveillance differ when surveillance is siloed within

governments or companies? I focus on comparative political opinion research in the United States and the European Union in three dissertation chapters, with original and second-hand data²⁷.

Government surveillance and market surveillance have their own unique logic and priorities. Previous public opinion studies focus on attitudes towards either. I contribute to public opinion on surveillance by asking about policies across the surveillance complex simultaneously. I measure how these attitudes fall along divergent dimensions in Chapter 2, drawing from a nationally representative sample of 1,493 Americans surveyed online during August 2021. Deputized surveillance allows the full force of the state—and its instruments of coercion—to be present but hidden under a patina of banal market opt-in consent. In that chapter, I empirically demonstrate that deputized surveillance produces a third, distinct, and understudied dimension of privacy concern²⁸.

I review how previous studies have measured privacy concerns, and I identify question-framing patterns regarding (primarily physical) government and market surveillance. I produce an interdisciplinary review of sociology, criminology, communications, and economics/business school literature. Building on privacy scholar Helen Nissenbaum's theory of contextual integrity, I hypothesize that people's preferences fall within a multi-dimensional space demarcated by who is carrying out surveillance. I find that normative preferences over deputized surveillance fall on a dimension separate from government-exclusive and market-exclusive surveillance practices. From the evidence, I conclude that privacy preferences should not be averaged into a single variable of analysis, as there are substantively important and statistically significant differences in types of surveillance. However, preferences over market and state surveillance are not as consistently demarcated as Nissenbaum's theory suggests. This finding is an opportunity for future research.

²⁷ The fifth chapter is a technical piece outlining the original empirical survey and experiment work conducted for chapters 2 and 3.

²⁸ These findings are limited to American's privacy concerns. Future research will endeavor to replicate data collection in Five-eyes and European Union member-states.

An understudied perspective on attitudes towards surveillance is that mass online surveillance makes us all complicit in each others' monitoring. Given the networked technological features of online surveillance, this dissertation seeks to position attitudes toward privacy and concerns for mass surveillance viewed beyond the prism of an egotropic issue to a sociotropic one about common-good decisions. We may be explicitly "just" asked to give up *our* privacy for 'national security's sake'. But we are implicitly being asked to give up everyone else's privacy, including more vulnerable, marginalized groups. Law-and-order frames are prevalent in media and (minimal) political discourse. Do these frames play a role in forming these preferences? Chapter 3 proposes one mechanism explaining deputized surveillance preference formation around this issue: the desire to surveil disliked groups. What are people's preferences when the *mass* portion of mass online surveillance is emphasized? In this chapter, I use a novel factorial vignette experiment to unpack how intergroup relations shape preferences on two deputized surveillance practices to explain the seeming collective apathy over mass online surveillance when these practices are revealed to the public.

Some critics of national security arguments point out that surveillance produces the perception that security is being enforced even when it is not ("security theater" (Levenson 2014)). Meanwhile, critical theorists and security practitioners have argued that people have accepted online surveillance partly because platforms act as trust gatekeepers and normalize its use for profit. Glen Whelan argues that people use surveillant commercial services, not despite the fact that they violate one's privacy but because they allow for surveillance of the customer/the employee (2019)²⁹. Schneier similarly argues a company's transaction monitoring ability generates trust between strangers when the firm can screen for fraud, reward positive repeat transactions, and punish negative interactions (2019).

²⁹ We get in strangers' cars because corporate mass surveillance ensures that wrongdoing will be met with forms of punishment (e.g., reputation, refunds, firing employees).

In Chapter 3, I build on Glen Whelan's assertion that digital services have incentivized a shift from trust in others to trust in their surveillance. By embedding an experiment in the aforementioned survey, I test the hypothesis that people's acceptance of deputized surveillance policies is influenced by whether they see a liked or disliked group being affected. Using a counterargument design, I analyze whether their opinion on the randomly assigned policy can be changed when they see the opposite valence group. I also calculate the cumulative effect of contradicting information and the role of ordering effects in persuasion when presenting information on how opposing valence groups are monitored through mass deputized surveillance.

This chapter advances our understanding of how commonly (mis)used media frames linking criminality and other out-groups to targeted surveillance can influence public opinion on mass surveillance. The findings reveal a persistent measurement problem with implications for discussing marketplace choice and consent under imperfect information environments. The data helps causally identify how popular mobilization of merely disliked (not even criminal) groups³⁰ can produce illiberal effects³¹ by increasing support for mass surveillance. The findings from chapters 2 and 3 problematize whether Americans are making principled choices abiding by democratic norms (e.g., universal right to privacy). They suggest opinion on policing policy is shaped by intergroup dynamics that make privacy a privilege for some groups or tradeable for security *against* other groups.

The US spearheaded the construction of the surveillance complex, but its effects are not nationally bound to it. European countries are currently negotiating conflicting impetuses. On the one hand, they are deputizing online services to monitor a broader range of online behavior (e.g., German hate speech NetDG law) and developing legal responsibilities and penalties for failing to collaborate with law enforcement. On the other hand, the post-Snowden response to citizen

³⁰ Because the United States protects hate speech no group in the list is inherently criminal by virtue of its membership. This contrasts other democratic country's intergroup dynamics, where hate speech is criminalized.

³¹ Even in Democratic-identifying respondents.

monitoring incentivized governments to respond to domestic demands for protection (Eddy 2022), resulting in the General Data Protection Regulation (GDPR). The EU also forced online services to delete European data from their systems when requested (Jones 2018). Court cases have struck down trans-Atlantic commercial data transfers because Americans cannot guarantee Europeans' privacy and data security (Toomey and Gorski 2022). European military and intelligence allies have also been openly debating their role in their domestic and foreign policing since the Snowden revelations³² (European Parliament, Sophia Helena in 't Veld 2022). Proposals on using Big Data for the digital economy/services are being debated.

In the wake of the Snowden revelations, the European Voter Study of 2014 and 2019 asked (n = 52,885) respondents to “rate the following statement from 0-10, where: *You fully support privacy rights even if they hinder efforts to combat crime (0) You are fully in favor of restricting privacy rights in order to combat crime (10)*”. Between these two survey waves, the European Union passed (in 2016) and (in 2018) began enforcing the largest privacy protection regulatory scheme of the internet era: the General Data Protection Regulation. Its enactment gave way to a change in how Europeans' data processing is handled³³, recourse and costly penalties for mishandling of data, and, significantly, a detailed set of disclosure, consent, and withdrawal of consent (along with data deletion) to internet users located in the bloc.

In Chapter 4, I analyze European citizens' preferences for the tradeoff between privacy and security through various public opinion frameworks. In doing so, I find that many respondents refuse to prioritize one side of the privacy-security tradeoff. Still, pro-privacy responses increased in 2019

³² The United States, Canada, United Kingdom, Australia and New Zealand form an intelligence alliance called Five Eyes that delegates foreign surveillance reciprocally to circumvent domestic surveillance prohibitions (Radden Keefe 2005). Among others, NSA whistleblower Edward Snowden provided journalists with ample evidence of these alliances (Molinaro 2021, Gellman 2020, Gorman 2017). Other European countries have intelligence sharing agreements forming what are called Nine-Eyes or Fourteen-eyes. Denmark, for example, is part of the Fourteen-eyes alliance and has publicly debated its participation since a national whistleblower came forward in 2020 (Moss 2020).

³³ Its passing also bolstered the lawsuits against the US-EU data transfer regime that was struck down twice, as detailed in the last paragraph of page 19.

compared to 2014 suggesting that the policy supply (GDPR) reacting to Snowden's revelations about European communications' spying can shape citizen attitudes. Two dots make a line, but they don't make a trend. I am limited by two periods from making broader claims, but notably, pro-privacy attitudes rose after GDPR compared to their levels closer to the Snowden revelations. This finding suggests that politicians and regulatory schemes can legitimize and normalize claims for privacy in Europe. This finding supports my claim that the political and information environment that shapes the supply of surveillance or privacy is not independent of public opinion formation.

Led by the response patterns, I model tradeoff refusals as an opinion choice distinct from prioritizing either side. I find ideological and political preferences are strongly associated with what side of the tradeoff people fall on. Only Conservative party voters of the European Union are statistically inclined to lean towards security. However, people's relations to the government³⁴ are rarely theorized, let alone analyzed, in the existing surveillance literature (Viola and Laidler 2022, cf. Turow, et al. 2018)³⁵.

The study of European attitudes expands our understanding of privacy attitudes from a comparative perspective. The European public is a large Western technology market that has increasingly asserted an alternative political economy of data (Laurer and Seidl 2020, O'Hara 2021, Jones 2018). However, its institutions are reacting to the international effects of the US surveillance complex. They are still deliberating whether to keep supporting America's forbearance of the surveillance complex's regulation or counter-balance it with an alternative legal regime (Lomas 2023). This international dimension is largely forsaken when observers discuss the costs and incentives of deputized American Data Goliaths and the broader surveillance complex.

³⁴ Measured by interest, approval, party preference, ideology and preference for substantive government policies.

³⁵ Chapter 4's appendix includes an exploratory country-level analysis of (institutional and event-based factors to explain the tradeoff's average scores at the country level.

Boycotts may provide an illusion of consumer choice³⁶, particularly in the face of politically-resistant institutions unresponsive to citizen demands. But the market size and deep embeddedness of Data Goliaths' role in the critical infrastructure of services³⁷ and hardware makes privacy by individual withdrawal a bigger punishment for those who exit than for these firms. Expecting individuals to boycott also shifts the onus from the actors responsible for privacy erosions onto those most aware and willing to act on their concerns. Are we facing the return of the Ancient Greek punishment by exile?

Governments that avoid regulating surveillance indirectly endorse a troubling “if you don’t like it, leave” form of governance. Such a response might erode public trust, as the basic idea that democracies manage—not shun—conflicting interests are replaced by ignoring people’s concerns. As my data will show throughout the three empirical chapters, these concerns are also not held by a small minority in the US or Europe. To undo the harms of surveillance on the democratic rule of law, we need a more precise understanding that surveillance itself is an exercise in asymmetric power. Companies prioritize their responses to shareholders and the threat of regulation because the legal costs require them to do so. More democracy requires people to mobilize as citizens—not users—to organize and resist the narrative that they are alone in their concerns and desires for privacy. Institutions desiring to rebuild trust and accountability must be open to these clamors. But we must have a clear-eyed view of the current obstacles. Protective legal regimes that shield surveillance practices, within markets or governments, from democratic debate and accountability are currently superseding collective action. The picture emerging from Europe is that organizations like None of

³⁶ The question is whether lack of choice renders boycotts unusable, or whether withdrawal as the choice is a feasible alternative to protest individually.

³⁷ Beyond internet services, these companies are expanding their repertoire into finance, health monitoring, commerce, intermediary gatekeeping smaller websites’ security (via login and identification services), and even data and website hosting and analytic services.

Your Business can aggregate citizen demands and present compelling arguments against the American surveillance complex when institutional support is present.

The surveillance complex is a behemoth that raises many troubling issues over democratic norms of decision-making, information, a broad range of rights, and justice between citizens and their governments, governments and corporations, and corporations and individual users. This dissertation seeks to put some of these issues on the Political Science research agenda along with tools to analyze them empirically. I hope not to present an exhaustive compendium of problems and answers but to start the conversation.

Bibliography

- Ackerman, Spencer. 2021. *Reign of Terror: How the 9/11 Era Destabilized America and Produced Trump*. New York: Penguin Publishing Group.
- Arendt, Hannah. 1951. *The Origins of Totalitarianism*. 1973 re-publication. New York: Harcourt Brace Jovanovich.
- Bloom, Peter. 2019. *Monitored: Business and Surveillance in a Time of Big Data*. London: Pluto Press.
- Boghosian, Heidi, and Lewis Lapham. 2013. *Spying on Democracy: Government Surveillance, Corporate Power and Public Resistance*. San Francisco: City Lights Books.
- Bruder, Jessica, and Dale Maharidge. 2020. *Snowden's Box: Trust in the Age of Surveillance*. Brooklyn: Verso.
- Byler, Darren. 2022. *In the camps: China's high-tech penal colony*. Durham: Duke University Press.
- Cagle, Matt, and Nicole Ozer. 2019. *Amazon Teams Up With Government to Deploy Dangerous New Facial Recognition Technology*. Digital, New York: American Civil Liberties Union. Accessed October 01, 2109. <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-teams-government-deploy-dangerous-new>.
- Chin, Josh, and Liza Lin. 2022. *Surveillance State: Inside China's Quest to Launch a New Era of Social Control*. New York City: St. Martin's Press.
- Citron, Danielle Keats, and David C. Gray. 2013. "Addressing the Harm of Total Surveillance: a Reply to Professor Neil Richards." *Harvard Law Review* 262-274.
- Coleman, Gabriella. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymity*. New York: Verso.
- Coyne, Christopher J., and Abigail R. Hall. 2018. *Tyranny Comes Home: The domestic fate of US Militarism*. Stanford: Stanford University Press.
- Dempsey, James. 2023. "Cybersecurity Enforcement: if government regulation is going to be increased, how will it be enforced?" *Program on Democracy and the Internet*. Stanford: Stanford University Cyber Policy Center. Accessed January 17, 2023.
- Diamond, Larry. 2015. "Facing up to the Democratic Recession." *Journal of Democracy* 26 (1): 141-155.
- Eddy, Melissa. 2022. "Right to Privacy Extends to Foreign Internet Users, German Court Rules." *The New York Times*, May 19: Section A, Page 17. Accessed April 16, 2022. <https://www.nytimes.com/2020/05/19/world/europe/germany-privacy.html>.

- Elster, Jon. 2000. *Ulysses unbound: studies in rationality, precommitment, and constraints*. Cambridge: Cambridge University Press.
- European Parliament, Sophia Helena in 't Veld . 2022. "Draft Report Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance ." European Parliament, Brussels. [https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA\(2022\)732268_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf).
- Farrell, Henry, Margaret Levi, and Tim O'Reilly. 2018. *Mark Zuckerberg runs a nation-state, and he's the king*. April 10. Accessed May 3, 2018. <https://www.vox.com/the-big-idea/2018/4/9/17214752/zuckerberg-facebook-power-regulation-data-privacy-control-political-theory-data-breach-king>.
- Federman, Adam. 2019. "Revealed: how the FBI targeted environmental activists in domestic terror investigations." *The Guardian*. Accessed September 20, 2021. <https://www.theguardian.com/us-news/2019/sep/23/revealed-how-the-fbi-targeted-environmental-activists-in-domestic-terror-investigations>.
- Friedewald, Michael, Marc Lieshout, Sven Rung, Merel Ooms, and Jelmer Ypma. 2014. "Privacy and Security Perceptions of European Citizens_ A Test of the Trade-Off Model." *9th Privacy and Identity Management for the Future Internet in the Age of Globalisation*. Patras: Springer. 39-53. doi:10.1007/978-3-319-18621-4_4.
- Garcia, Blake E., and Nehemia Geva. 2016. "Security Versus Liberty in the Context." *Terrorism and Political Violence* 48: 30-48. doi:10.1080/09546553.2013.878704.
- Gellman, Barton. 2020. *Dark mirror: Edward Snowden and the American surveillance state*. New York: Penguin Random House.
- Gilens, Martin, and Benjamin I. Page. 2014. "Testing Theories of American Politics: Elites, Interest Groups, and Average Citizens." *Perspectives on Politics* 12 (3): 564-581. doi:doi:10.1017/S1537592714001595.
- Gorman, Siobhan. 2017. "The Snowden Effect on the NSA and Reporting." In *Journalism After Snowden: The future of the free press in the surveillance state*, 199. New York: Columbia University Press.
- Graff, M. Garrett. 2016. "America's Top Spy Talks Snowden Leaks and Our Ominous Future." *Wired Magazine*, November 17. Accessed March 22, 2023. <https://www.wired.com/2016/11/james-clapper-us-intelligence/>.
- Greenberg, Andy. 2019. *Hacker Eva Galperin Has a Plan to Eradicate Stalkerware*. April 04. Accessed May 27, 2019. <https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/>.
- Guo, Jeff. 2016. "New study: Snowden's disclosures about NSA spying had a scary effect on free speech." *The Washington Post*, April 27. Accessed April 17, 2017. https://www.washingtonpost.com/news/wonk/wp/2016/04/27/new-study-snowdens-disclosures-about-nsa-spying-had-a-scary-effect-on-free-speech/?utm_term=.c0eebf3cefb3.
- Hersh, Eitan. 2015. *Hacking the Electorate: How Campaigns Perceive Voters*. New York: Cambridge University Press.
- Hertsgaard, Mark. 2016. "How the Pentagon punished NSA whistleblowers." *The Guardian*, May 22. Accessed March 13, 2023. <https://www.theguardian.com/us-news/2016/may/22/how-pentagon-punished-nsa-whistleblowers>.
- Holmes, Aaron. 2020. *Police are tapping into residents' Ring doorbells and home security cameras to stream 24/7 live video*. November. Accessed April 7, 2022. <https://www.businessinsider.com/ring-doorbells-live-video-security-camera-police-fusus-2020-11>.
- Huddy, Leonie, Stanley Feldman, Charles Taber, and Gallya Lahav. 2005. "Threat, Anxiety, and Support of Antiterrorism Policies." *American journal of Political Science* 49 (3): 593-608.

- Igo, Sarah E. 2018. "Defining Privacy—and Then Getting Rid of It." *Laphams Quarterly*, May 15.
<https://www.laphamsquarterly.org/roundtable/defining-privacy-and-then-getting-rid-it>.
- Johnson, Bobbie. 2009. "Facebook privacy change angers campaigners." *The Guardian*, December 10.
 Accessed March 22, 2023.
<https://www.theguardian.com/technology/2009/dec/10/facebook-privacy>.
- . 2010. "Privacy no longer a social norm, says Facebook founder." *The Guardian*, January 11.
 Accessed March 22, 2023.
<https://www.theguardian.com/technology/2010/jan/11/facebook-privacy>.
- Johnson, Loch K. 2017. *Spy Watching: Intelligence Accountability in the United States*. New York: Oxford University Press.
- Jones, Meg Leta. 2018. *Ctrl + Z*. New York: New York University Press.
- Kanno-Youngs, Zolan. 2020. "U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance." *The New York Times*, June 19: Section A, Page 1. Accessed March 15, 2023.
<https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html>.
- Katzenstein, Jessica. 2020. *The Wars are Here: How the United States' Post-9/11 Wars Helped Militarize U.S. Police*. Paper, Costs of War, Watson Institute, Boston: Brown University, Boston University. Accessed 2023.
https://watson.brown.edu/costsofwar/files/cow/imce/papers/2020/Police%20Militarization_Costs%20of%20War_Sept%2016%202020.pdf.
- King, Gary, Jennifer Pan, and Margaret E. Roberts. 2014. "Reverse-engineering censorship in China: Randomized experimentation and participant observation." *Science* 345 (6199): 1-10.
- Kiss, Jemima. 2014. "Snowden: Dropbox is hostile to privacy, unlike 'zero knowledge' Spideroak." *The Guardian*, July 17: Tech. Accessed February 25, 2019.
<https://www.theguardian.com/technology/2014/jul/17/edward-snowden-dropbox-privacy-spideroak>.
- Krueger, Brian S., Samuel J. Best, and Kristin Johnson. 2020. "Assessing Dimensions of the Security-Liberty Trade-off in the United States." *Surveillance & Society* 18 (1): 104-120.
- Lancaster, Joe. 2022. *City Council Furious at Cop Who Played Disney Songs To Keep from Being Recorded*. April 27. Accessed December 07, 2022. <https://reason.com/2022/04/27/city-council-furious-at-cop-who-played-disney-songs-to-keep-from-being-recorded/>.
- Laurer, Moritz, and Timo Seidl. 2020. "Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation." *Policy & Internet* 257- 277.
<https://onlinelibrary.wiley.com/doi/10.1002/poi.3.246>.
- Levenson, Eric. 2014. "The TSA Is in the Business of 'Security Theater,' Not Security." *The Atlantic*, January 31. Accessed April 17, 2023.
<https://www.theatlantic.com/national/archive/2014/01/tsa-business-security-theater-not-security/357599/>.
- Levinson, Jonathan, Conrad Wilson, James Doubek, and Suzanne Nuyen. 2020. "Federal Officers Use Unmarked Vehicles To Grab People In Portland, DHS Confirms." *National Public Radio All Things Considered*, July 17. Accessed March 15, 2023.
<https://www.npr.org/2020/07/17/892277592/federal-officers-use-unmarked-vehicles-to-grab-protesters-in-portland>.
- Levitsky, Steven, and Lucan A. Way. 2010. *Competitive Authoritarianism: Hybrid Regimes After the Cold War*. New York: Cambridge University Press.
- Lomas, Natasha. 2023. *MEPs raise concerns over draft EU-US data transfer deal*. April 14. Accessed May 8, 2023. <https://techcrunch.com/2023/04/14/dpf-libe-committee-concerns/>.

- Molinaro, Dennis G., ed. 2021. *The bridge in the parks: the Five Eyes and Cold War counter-intelligence*. Toronto: University of Toronto Press.
- Moss, Sebastian. 2020. "Danish whistleblower details NSA collaboration, submarine cable spying, surveillance data center." *Data Center Dynamics*, November 18. <https://www.datacenterdynamics.com/en/news/danish-whistleblower-details-nsa-collaboration-submarine-cable-spying-surveillance-data-center/>.
- O'Hara, Kieron, Hall, Wendy. 2021. *Four Internets: Data, Geopolitics, and the Governance of Cyberspace*. New York: Oxford University Press.
- Open Secrets. 2022. "Reelection Rates Over the Years." *Open Secrets*. December. <https://www.opensecrets.org/elections-overview/reelection-rates>.
- Passavant, Paul Andrew. 2021. *Policing protest*. Durham: Duke University Press.
- Popkin, Helen A.S. 2010. "Privacy is dead on Facebook. Get over it." *NBC Tech News*, January 13. Accessed March 22, 2023. <https://www.nbcnews.com/id/wbna34825225>.
- Radden Keefe, Patrick. 2005. *Chatter: dispatches from the secret world of global eavesdropping*. New York: Random House.
- Reitman, Rainey. 2011. *Facebook's Hotel California: Cross-Site Tracking and the Potential Impact on Digital Privacy Legislation*. Technical report, San Francisco: Electronic Frontier Foundation.
- Risen, James, interview by Jeremy Scahill. 2018. *All the News Unfit to Print: James Risen on his battles with Bush, Obama, and The New York Times* (January 03). Accessed March 21, 2023. <https://theintercept.com/2018/01/03/all-the-news-unfit-to-print-james-risen-on-his-battles-with-bush-obama-and-the-new-york-times/>.
- Risen, James, and Eric Lichtblau. 2005. "Bush Lets U.S. Spy on Callers Without Courts." *The New York Times*, December 16. Accessed March 31, 2017. <http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html>.
- Rosenzweig, Paul. 2016. *The Surveillance State: Big Data, Freedom, and You*. Palo Alto: The Teaching Company.
- Runzel, Tamara. 2019. *Sapling*. November 25. Accessed March 15, 2023. <https://www.sapling.com/2246673/open-bank-account-no-id>.
- Salinas, Sara, and Anita Balakrishnan. 2018. "Mark Zuckerberg has been talking and apologizing about privacy since 2003 — here's a reminder of what he's said." *CNBC Tech*, December 19. Accessed March 22, 2023. <https://www.cnn.com/2018/12/19/facebook-ceo-mark-zuckerberg-privacy-apologies.html>.
- Sanchez, Chelsey. 2020. "NYPD Pulled a Protestor Into an Unmarked Vehicle—But This Policing Tactic Is Far From New." *Harper's Bazaar*, August 1. Accessed March 15, 2023. <https://www.harpersbazaar.com/culture/politics/a33457941/nypd-protest-unmarked-vans-plainclothes-officers-arrest/>.
- Schmitt, Eric, and Thomas Gibbons-Neff. 2022. "Air Force Investigates Military Planes That Monitored Protesters." *The New York Times*, June 18: Section A, Page 19. Accessed March 15, 2023. <https://www.nytimes.com/2020/06/18/us/politics/investigation-military-surveillance-planes-george-floyd-protests.html>.
- Schneier, Bruce. 2018. *Click Here to Kill Everybody: security and survival in a hyper-connected world*. New York: W. W. Norton and Company.
- . 2006. *The Eternal Value of Privacy*. May 18. Accessed March 22, 2023. https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html.
- . 2019. "There's no Good Reason to Trust Blockchain Technology." *Wired*, February 06. Accessed February 25, 2019. <https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/>.

- Schradie, Jen. 2015. "Silicon Valley Ideology and class inequality: a virtual poll tax on digital politics." In *Handbook of Digital Politics*, edited by Stephen Coleman and Deen Freelon, 67-84. Cheltenham: Edward Elgar Publishing.
- . 2019. *The Revolution That Wasn't: How Digital Activism Favors Conservatives*. Cambridge: Harvard University Press.
- Schuba, Tom, and Frank Main. 2021. "Chicago Police Department launched secret drone program with off-the-books cash." *Chicago Sun Times*, May 12. Accessed April 13, 2022. <https://chicago.suntimes.com/city-hall/2021/5/11/22425299/cpd-chicago-police-drone-secret-emails-hack-lori-lightfoot-dodsecrets-city-hall>.
- Solon, Olivia. 2018. "Cambridge Analytica whistleblower says Bannon wanted to suppress voters." *The Guardian*, May 16. <https://www.theguardian.com/uk-news/2018/may/16/steve-bannon-cambridge-analytica-whistleblower-suppress-voters-testimony>.
- Solove, Daniel J. 2011. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven: Yale University Press.
- Solove, Daniel J., and Danielle Keats Citron. 2021. "Privacy Harms." *George Washington Law Faculty Publications & Other* 63. https://scholarship.law.gwu.edu/faculty_publications/1534.
- Strittmatter, Kai. 2020. *We Have Been Harmonized: Life in China's Surveillance State*. New York City: Custom House.
- Taube, Dan, Keely Kolmes, and Colette Vogele. 2014. *Preliminary Report: Without My Consent Survey of Online Stalking, Harassment and Violations of Privacy*. Survey summary, San Francisco: Without My Consent. https://withoutmyconsent.org/sites/default/files/wmc_prelim_survey_report.pdf.
- Toomey, Patrick, and Ashley Gorski. 2022. *The Supreme Court just made a US-EU Privacy Shield agreement even harder*. March 21. Accessed December 07, 2022. <https://thehill.com/opinion/judiciary/598899-the-supreme-court-just-made-a-us-eu-privacy-shield-agreement-even-harder/>.
- Turow, Joseph, Michael Hennessy, Nora Draper, Ope Akanbi, and Diami Virgilio. 2018. *Divided We Feel: Partisan Politics Drive Americans' Emotions Regarding Surveillance of Low-Income Populations*. Academic, University of Pennsylvania, Annenberg: Annenberg School for Communication. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3609974.
- Viola, Lora Anne, and Pawel Laidler. 2022. *Trust and transparency in an age of surveillance*. New York: Routledge.
- Wagner, Kurt. 2018. *This is how Facebook collects data on you even if you don't have an account*. April 20. Accessed January 17, 2022. <https://www.vox.com/2018/4/20/17254312/facebook-shadow-profiles-data-collection-non-users-mark-zuckerberg>.
- Warren, Samuel D., and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4 (5): 193-220.
- Welna, David. 2014. "Before Snowden: The Whistleblowers Who Tried To Lift The Veil." *NPR Morning Edition*, July 22. Accessed March 13, 2023. <https://www.npr.org/2014/07/22/333741495/before-snowden-the-whistleblowers-who-tried-to-lift-the-veil>.
- Westin, Alan F. 1967. *Privacy and Freedom*. New York: Atheneum.
- Whelan, Glen. 2019. "Trust in Surveillance: A Reply to Etzioni." *Journal of Business Ethics* 156: 15-19. doi:10.1007/s10551-018-3779-4.
- Wu, Tim. 2019. "How Capitalism Betrayed Privacy." *The New York Times*, April 10: SR3. Accessed April 14, 2019. <https://www.nytimes.com/2019/04/10/opinion/sunday/privacy-capitalism.html?login=email&auth=login-email>.

- Zetter, Kim. 2012. "NSA Chief Tells Hackers His Agency Doesn't Create Dossiers on All Americans." *Wired*, July 27. www.wired.com/2012/07/nsa-chief-denies-dossiers.
- Zhang, Baobao, Sarah Kreps, and Nina McMurry. 2020. "Americans Perception of Privacy and Surveillance in the COVID 19 Pandemic." *Working paper* 1-24.
- Ziller, Conrad, and Marc Helbling. 2020. "Public Support for State Surveillance." *European Journal of Political Research*.
- Zuboff, Shoshana. 2019. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: Public Affairs.

Chapter 1 Deputation in the surveillance complex

Abstract

I conceptualize advanced democracies' systems of mass online surveillance as part of a "surveillance complex". I discuss the US' use of legal and informal mechanisms between governments and corporations to provide surveillance data, which I conceptualize as one of deputation. I produce a historical account of the political economy of the surveillance complex, highlighting the American government's role in shaping high technological supply and low political accountability. This chapter contrasts alternative explanations of contemporary online surveillance which place companies as the main drivers, and governments passive or incapable of keeping up with technology. This distinction highlights the deployment of mass surveillance as a politically self-interested choice, making the invisible hand visible. To support this perspective, I give evidence of how companies' ability to pursue profit models based on surveillance data (e.g., surveillance capitalism (Zuboff 2019)) has been fostered by direct government investments (e.g., NSF grants, data purchases), forbearance (e.g., non-enforcement of privacy laws), deregulation, and deliberate inaction (e.g., an explicit refusal to regulate, not just its absence/tolerance by default).

Introduction

As discussed in the dissertation's introduction, an emphasis on the government's role in the proliferation of mass online surveillance matters to the public's opinion formation, and thus the prospects of its regulation, in two ways. First, acknowledging the interest advanced democracies have in accessing data helps explain the main conditions of public opinion development. Democratic governments' preference for secrecy around the use of surveillance reduces the amount of information available to the public. Evidence for secrecy preference predominance is discussed through historical accounts of the post-World War II military-industrial complex intelligentsia, and post-9/11 pushback against whistleblowers and journalists, as well as reduced inter-branch competition in the form of deference to the Executive (Rosenzweig 2016), particularly its intelligence agencies (dubbed 'intelligence exceptionalism' (Johnson 2017)).

Second, the state's preference for secrecy, however, is not guaranteed. That is, public opinion has been shaped by sporadic informational 'shocks' that disrupt secrecy's 'informational void'. June 2023 will mark the 10-year anniversary of the Edward Snowden revelations. While the PATRIOT

ACT was publicly passed, its debate was short (45 days) and was marked by an unusual “rally around the flag” period of bipartisan support for “doing something”³⁸. The law provided for additional secrecy in the form of one-sided court hearings where arguments, evidence, and verdicts would be shielded from public view, including the accused’s knowledge. Further efforts to shield the specifics surveillance programs from public scrutiny were embedded in the PATRIOT ACT and ancillary deputizing data-collection requirements (e.g., Section 314A Foreign Assets Control list) and enforced through National Security Letters and other instruments. Before Snowden, the American government had on the whole, been ‘successful’ in shielding the surveillance complex from public scrutiny. In the next sections I will elaborate how Snowden disrupted this pattern by providing journalists with an unprecedented amount of documents that made denials harder to believe and refusals to comment unsustainable³⁹.

³⁸ It is worth remembering that George W. Bush had lost the popular vote, and Democrats blamed the Supreme Court for ‘handing the election’ over to him. Nine-months after taking office, but two weeks after 9/11, “nearly 9 in 10 Democrats and independents approved of the Republican president, with Democratic approval trailing Republicans by 10 percentage points” (Bump 2017). See source for three-year period data. The PATRIOT Act’s passing was carried out early enough that it escaped the start of bipartisan decline in support (a regression to the mean) 3 months after.

³⁹ For example, “after Mr. Snowden disclosed the program of collecting the records of Americans’ phone calls, intelligence officials told reporters that, for technical reasons, it consisted mostly of landline phone records”, but NSA documents disclosed in 2015 documented that “In 2011, AT&T began handing over 1.1 billion domestic cellphone calling records a day to the N.S.A. after “a push to get this flow operational prior to the 10th anniversary of 9/11,” according to an internal agency newsletter”, as well as “billions of emails” from 2003 to 2013, including “live” access (Angwin, Savage, et al. 2015).

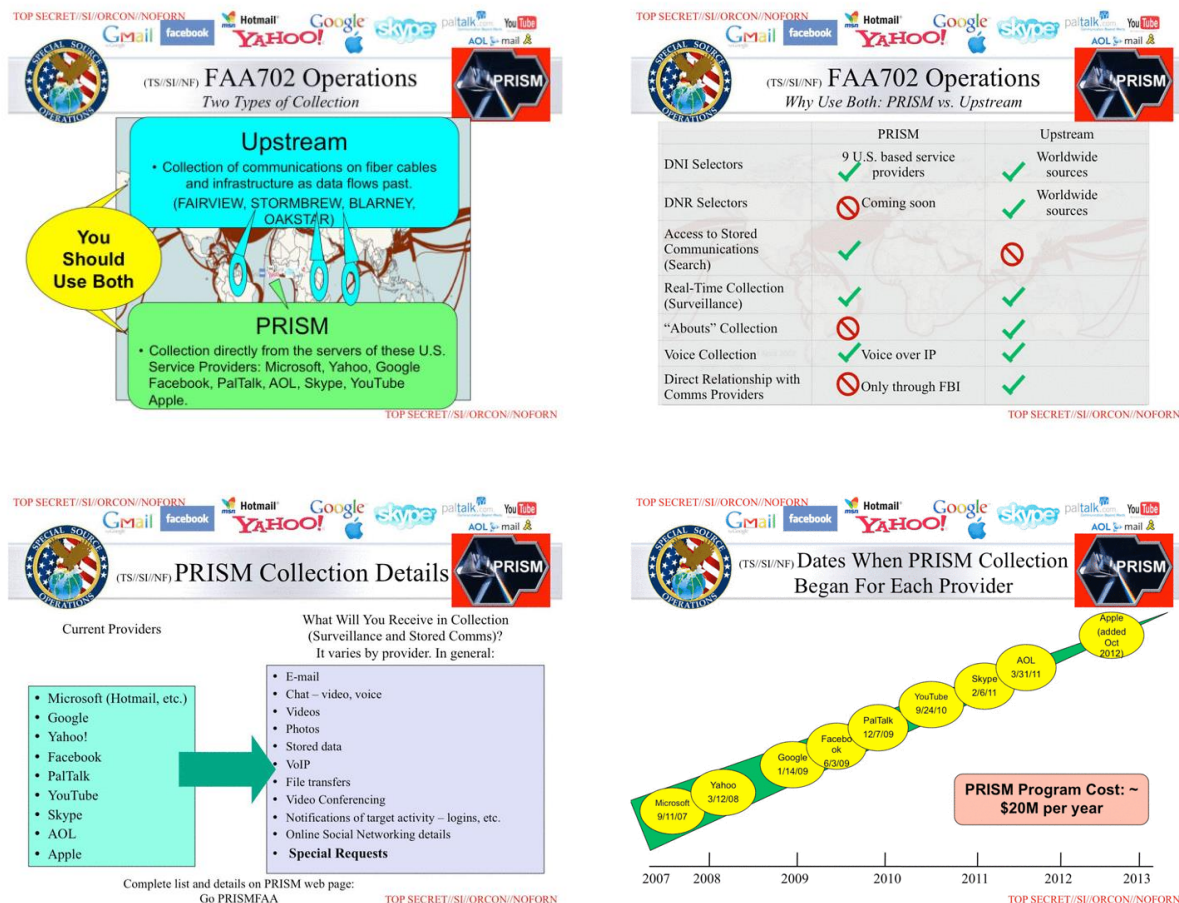


Figure 1 Snowden slides from PRISM/US-984XN NSA Overview.
Source: <https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document>

Publication of surveillance policies and programs mobilized the Obama administration into a defense of these programs (Harris 2013), usually by invoking the desire to preempt terrorism. Thus, bipartisan secrecy gave way to a reductive framing of the policies' purpose and impact, retroactively explaining as little as possible. In America, inter-branch competition on surveillance policies on the subject remains minimal⁴⁰, even as trade partners like Europe are strongly diverging in their regulatory frames and exerting pressure on trans-Atlantic data flows. This makes mass online surveillance public

⁴⁰ There are signs of some regulatory appetite in the Biden Executive, particularly in the FTC and SEC, and there have been Legislative calls for anti-trust regulation especially as some data collection coincides with electoral competition on issues like reproductive rights (post Dobbs decision) and social media content filtering. But these are not fundamental repudiations of mass online surveillance, intelligence exceptionalism, the underlying claim to state secrets privilege, nor have the circumscribed proposals come into effect.

opinion *sui generis* compared to other policies, where a moderate or robust public debate is present and attempts at suppressing information are absent.

The convergence of government and corporate interests in persistent identification allows mass surveillance innovation and implementation without solely relying on government contracts to shape the supply of surveillance technologies. Beyond the embedded decision-making obscurity, this departure from outsourcing alone further complicates people's capacity to see the forest for the trees. The independent but converging interest of governments and companies requires a holistic development of measures to adequately capture attitudes towards privacy and surveillance techniques multi-dimensionally. In this chapter I focus on explaining the components of the surveillance complex, especially the under-conceptualized deputation mechanism. Given the constraints on the informational environment, which I will further document in this chapter, the 'demand' (public opinion) for surveillance is not completely exogenous to the supply of technology and information. I focus on the latter in this chapter and pivot to public opinion in the subsequent chapters of the dissertation.

The surveillance complex encompasses surveillance conducted by the state, market surveillance on consumers, and, importantly, the state's deputation of the market as an intermediary. Edward Snowden's revelations made it clear that much of the United States domestic and foreign surveillance was carried out by deputizing companies⁴¹. The practice of online surveillance deputation began with the 1998 Digital Millennium Copyright Act (Urban and Quilter 2005) and ancillary content monitoring/free speech court cases (The Electronic Frontier Foundation 2018). Through the DMCA the US government created a system of legal protections ("safe harbor") for online service providers,

⁴¹ Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple, Dropbox were all part of PRISM (Seifert 2013, The Washington Post 2013).

conditioned on their ability to act on copyright holders⁴² complaints. In this incipient version of deputized surveillance, online service providers like Yahoo!, Google or smaller forums, and Internet Service Providers (ISPs) like Verizon, AOL, etc., were put in charge of post-hoc monitoring online speech that was flagged by copyright holders and became the first instance of dispute adjudication.

The government's creation of a conditional safe harbor as the main copyright dispute resolution mechanism did not rely on contracts. This crucial feature is why I use the term "deputation", to encompass more than the outsourced, contract-based relationships that characterize the military-industrial complex. It was cost-free economically, but it was also politically costless for the state. For example, the government was spared from dedicating judicial resources, criminalizing an increasing number of people engaging in piracy in the Napster era, reaching ridiculous or contradictory judgements, or having copyright holders exert pressure on the government to increase penalties (Maxwell 2011, Van der Sar 2013, Van der Sar 2006, B. Jones 2008). Copyright deputation paved the way for broader deputation into other law-and-order functions, particularly with the passing of the PATRIOT ACT 45 days after 9/11.

The resulting arrangement seemed to be a success from an administrative perspective. Deputizing copyright surveillance cleared federal courts from adjudicating most competing claims of online content copyright, particularly around fair use (e.g., education, satire, and transformative use like 'remix culture' (Lessig 2008, Masnick 2020))⁴³. The explosive growth of internet adoption at the turn of the century has made deputation a valuable resource, since it keeps the judicial docket clear from small claims. The DMCA's deputized copyright allowed claim holders to force intermediaries like Google to delete search results ("takedowns"), Internet Service Providers to cut off internet access

⁴² The language of the bill led to a proliferation of third-party representatives filling on behalf of copyright holders, sometimes called "copyright trolls". There are no penalties for submitting false copyright claims, and no requirement to be the copyright holder, anyone can make a complaint. This produces issues in accountability, as third parties can be hired to act overzealously, and firms can frequently escape negative press from negative externalities like reducing fair use claims.

⁴³ Courts still intervene to resolve copyright disputes among corporations, since these are not online piracy cases.

after warnings (“three strikes” proposals) or pass on notices of monetary compensation (claim letters). Courtroom cases involving individuals’ pirating would become sporadic efforts of last resort. Online service providers were effectively deputized to remediate corporate copyright needs by setting up surveillance systems of online traffic, like Internet Protocol tracing, to identify and serve infringement notices (see *By hook or by crook: degrees of collaboration* section).

Surveillance deputation grew beyond copyright enforcement between commercial parties, into a mechanism that would provide governments with access to individuals’ data without them always having to build a parallel data-collection operation. This impetus runs deep. For example, the 2015 USA FREEDOM Act included a reform to the PATRIOT Act’s Section 215, which was used to collect telephone records. Billed as a buffering mechanism between the NSA and FBI’s access to “tangible things”⁴⁴, it further institutionalized corporations’ central role in data-collection and storage through the Call Details Record program⁴⁵.

In this chapter, I provide historical evidence of how deputation is a crucial component of digital surveillance. I describe how it builds on post-World War II arrangements of American political economy, like the military-industrial complex and intelligence exceptionalism—an institutional deference to intelligence agencies’ decision-making (Johnson 2017). I also outline how deputized surveillance departs from its military-industrial complex origins. In my opinion, the absence of an

⁴⁴ Section 215 gave the government permission to require companies, using what is commonly described as a ‘secret order’ issued by the Foreign Intelligence Surveillance Act, to produce telephone, internet financial, or business records or “any other ‘tangible thing’ deemed ‘relevant’ to an international terrorism, counterespionage, or foreign intelligence investigation”. This includes banking transaction data, as per the Customer Identification Program, which “implements section 3261 of the USA PATRIOT Act and requires banks, savings associations, credit unions and certain non-federally regulated banks (‘bank’) to have a Customer Identification Program (‘CIP’)” (Financial Crimes Enforcement Networks 2004)

⁴⁵ The NSA revealed during a 2020 House Committee on the Judiciary oversight meeting that it had found itself to have been “unable to stay within the limits USA FREEDOM put on Section 215’s “Call Detail Records” (CDR) authority”, that the data collected was so unreliable it had to be deleted, and that they could/would not point to its role in “avert[ing] any kind of an attack on American soil” (McKinney, *The FISA Oversight Hearing Confirmed That Things Need to Change* 2019). It is currently reevaluating its use after pausing and deleting data from 2015-2019. The legal authority to collect CDR through the USA FREEDOM Act still stands, although there is no way of knowing what it has concluded or whether it has resumed (Bradford Franklin 2019).

intellectual articulation of deputized surveillance has siloed focus on either state surveillance or surveillance capitalism. This has produced incomplete and often apolitical understandings of the proliferating ecosystem of monitoring, data collection, analysis, exchange, and aggregation (see chapter 2 for alternatives). Such an issue lays the groundwork for motivating the dissertation’s work measuring privacy attitudes under a more comprehensive scope, the surveillance complex.

In the next section, I will historicize how deputized surveillance draws from the military-industrial complex’s legacy of obscurity in decision-making, shielding it from political interference. However, deputized surveillance departs from the military-industrial complex because, unlike the production of military weapons, identifying people, as citizens⁴⁶ or as consumers, is of interest to each of the parties independently⁴⁷. This further removes decision-making of specific technologies from an area where democratic scrutiny can be applied. Data collection, algorithms to analyze it, and the decisions taken become black boxes even to the government agencies that access and use the data. Because the market for data is larger than the state’s demand (unlike outsourced military-industrial complex demand⁴⁸), deputized surveillance produces more than hardware for law enforcement agencies (jets, radars, Stingray interceptors, drones). The use of surveillance within market firms and increasingly commercialized to individuals increases the normalization of surveillance, and minimizes domestic audience concerns by conveying a veneer of “opt-in” consumer consent.

⁴⁶ I will mainly use the term citizens to distinguish individuals vis-à-vis the state from individuals vis-à-vis corporations. However, one of the talking points Obama and his administration tried using after the Snowden was to state that only non-Americans were targeted (Henderson 2013). This presumed the domestic audience would be reassured, perhaps forgetting that a country with a high rate of immigration would likely have many people communicating with foreigners (Brewster 2015). The statement was false, as NSA programs allowed for data collection of non-Americans and, incidentally *and* deliberately, of Americans (Solomon 2017, Barrett 2020). Furthermore, it was misleading since the NSA has no process for identifying who is American—its targeting and minimization procedures “permit the NSA to *presume* that prospective surveillance targets are foreigners outside the United States absent specific information to the contrary—and to presume therefore that they are fair game for warrantless surveillance” (American Civil Liberties Union 2013). It is operating under a foreigner until proven American standard.

⁴⁷ Whereas, for example, military contractors do not have a market incentive for producing land mines if there is no external demand for it.

⁴⁸ This is the case even if comparing to classified programs, where the decision-making *exists* within the government even if it is not accessible to most people, even most government officials.

As I will show in this chapter, deputized surveillance is more likely to evade public scrutiny, deliberation, and accountability, compared to an already weak scrutinization of “in-house” government surveillance. This evasion is valuable to democracies, where governments are, at least on paper, bound to privacy rules. By incentivizing market actors to conduct mass surveillance for their own profit *and/or* on behalf of the government and then piggybacking on data from those “outsourced”⁴⁹ practices, advanced democracy governments make issues of consent and choice impossible for citizens to resolve individually. This chapter historicizes the emergence of deputized surveillance within the surveillance complex by drawing on insights from the post-World War II military-industrial complex arrangements, America’s efforts to police online content during the early days of the internet, surveillance capitalism literature, and contemporary journalistic and whistleblower evidence of the currently known practices.

Historical roots of deputation

Seventy years of deputized national security, praxis, and ideology

The United States’ reliance on deputation has roots in post-World War II factional arrangements accommodating an older impulse toward small government and newer expansionist foreign policy. American mass surveillance of domestic and international online communications has drawn on previous political solutions between corporations and the government. Thus, it would be an error to place surveillance deputation solely as a function of new (i.e., digital) technological circumstances (DiBella 2019, cf. Zuboff 2019). In this section I historicize the military-industrial complex’s legacy of

⁴⁹ This is the only time I am using the word outsourced. I’ve avoided this term in favor of deputation for two reasons. First, outsourcing is a business practice which means it is a contractual obligation between two firms. Governments are not firms, and, as I will argue in this chapter, data access arrangements are not always codified in contracts. Governments’ ability to coerce firms into collaborating, “by hook or by crook” is distinct from how firms trade and contract out services. Thus, I am wary of importing the language and logic of business scholarship when the field of political science has a much more appropriate term for the dynamics at hand—deputation.

obscurity in decision-making, to support later arguments that this attribute is a valuable consideration furthering deputation of firms for mass online surveillance.

Historian Michael J. Hogan traces the emergence of the United States' military-industrial complex as the result of public debate on a "peacetime military establishment" during the Truman administration. As the country transitioned from the end of World War II and prepared for the Cold War, the debate culminated with his signing of the National Security Act, institutionalizing incentives for corporate participation in military strategy. Cold War domestic politics asked the population to be in a constant and passive state of war, with an ever-growing but backgrounded militarized state. The 20th century debates on how to transition from a "hot" war with a clear end-point to a "cold" war (with no victory to claim) required new political arrangements.

The New Deal's social security benefits kicked off panic around the government's increased capacity to centralize and institutionalize an administrative state. Government activity intensified during World War II (Igo 2018), but did not subside with its end. After the war, GI benefits like housing, investment loans, and access to education kept the government involved in spheres previously reserved for the market. Some Americans wondered when, how, and where to pare back the state. Journalists argued, "[t]his is peace not war [...], and in peace, we must devise controls to take over from the military if we are to have a strong democracy". But defense establishment proponents, bolstered by growing anti-communist sentiment, saw the specter of war looming at every turn. For this camp, the era in which a line could be drawn "between citizen and soldier, civilian and military, war and peace, had disappeared forever" (Hogan, 465).

The US debated whether it could "prepare for total war [...] without becoming a garrison state and destroying the very qualities and virtues and principles we originally set out to save". Two camps—liberal internationalists and conservative nationalists—opposed a third emerging group, dubbed by Hogan the "defense establishment" camp. These groups debated whether the US could, for example,

develop military nuclear technologies without giving unseemly amounts of power to the military, and without creating an inefficient overseeing bureaucracy. Liberal internationalists wanted to maintain civilian control, while conservative nationalists wanted to avoid ballooning up the state in any capacity. These three camps debated the size and shape of the federal government and the checks and balances on its power.

When the coalition of “antistatist[s], antimilitarist[s], and isolationist[s]” articulated its fear of the garrison state in terms of the budget, the emerging defense establishment camp, which was also ideologically conservative, made coalitional inroads with the conservative nationalist camp⁵⁰. Historian Mark Stoler argues the debate was poisoned by “partisan politics, and [...] the cultural tendency of all parties to frame the debate in absolutist terms” doomed any liberal-conservative coalition capable of checking the defense establishment (2000).

The transformation away from the “old isolationism [that] forced them to build a national security state at home [...] altered the architectural face of the federal government” (Hogan 1998, 3). The infrastructure to carry out “forever wars” is rooted in these Cold War political and economic arrangements. The Truman administration’s bargain deputized hardware manufacturing to companies, creating the “military-industrial complex” (Eisenhower 1961). But, as I discuss below, it also deputized think tanks like RAND to develop aspects of its military and diplomatic strategies. Military hardware firms and think tanks lobbied the US government to engage in an arms race with the USSR, expanding its security needs by setting up military bases in Europe. In a convergence of interests, outsourced firms would provision the military with equipment and other resources to pursue its “Pax Americana” abroad. The specifics of what military equipment was produced, how, or why, was ensconced from inter-branch deliberation, developed at arms-length by corporations and think tanks.

⁵⁰ This dynamic was reinforced by neoliberal objections to direct public spending.

Like surveillance deputation, the government's reliance on companies, and as I will show later, think tanks allowed the federal government to shirk economic and political costs of technological innovation. Instead of being seen as a bloated Keynesian jobs program, investments via the market provided the public with normative justifications for corporate, not state-led, research and development (MacLean 2017). The state could remain administratively "weak", which was attractive to the conservative camps that prized budget austerity. The state could also become "strong" in its access to military offensive capabilities, which was appealing to the defense establishment and liberals who wanted an era of Pax Americana.

Deputation's institutionalization has impacted the government's access to all sorts of technologies was the post-war patent system. This began with federal funding for universities' nuclear energy research, expanding later to research in other fields. The "corporate laboratory" would be conducted as university research, cleared for classified weapons, but controlled in the private sphere. Labs' research results would belong to the private sector, and the government would have to purchase their technology at market prices⁵¹. These terms applied to government tech startup investments, starting with federal government contracts to IBM (Cappello 2017).

Federal investments also led to a DARPA-CIA-NSA program, the Massive Digital Data Systems (MDDS) project, managed via the National Security Foundation. Intelligence agencies wanted to seed funding for creating private companies to further information gathering⁵². Efforts to develop a technique of "query optimization of very complex queries that are described using the 'query flocks'

⁵¹ This arrangement has come to a head during COVID-19 where institutions with public funding contributed to research, but vaccines were ultimately developed, controlled and sold by corporate pharmaceuticals. This framework also spilled over to article publication and has led to the privatization of knowledge by journal publishers. The Biden administration is now planning on undoing this arrangement when public funds have supported research.

⁵² It is also worth remembering the intelligence community's working relationship with the pre-commercial internet, (D)ARPANET (Packard 2020). Some argue that intelligence gathering affordances were built into its protocols and standards, like the use of unencrypted transfer protocols like http⁵² (Radden Keefe 2005), which made wiretapping digital communications easier, compared to encrypted protocols like https://.

approach⁵³ (Nesbit 2017), which would later be dubbed the Total Information Awareness program (Radden Keefe 2005, 75). This project incentivized university researchers like Sergey Brin and Larry Page to create systems that would recognize behavioral patterns. Their work became Google.

The dependency on market forces to develop national security technologies increased with time. President Truman handed President Eisenhower the Korean War, and the former's farewell address was capped off by the infamous warning on the military-industrial complex (1961). Eisenhower worried that "federally funded scientists would join what he later called a military-industrial complex powerful enough to dominate public policy at the expense of sound democratic and fiscal principles" (Hogan, 383). His attempt to limit the power of science advisors through Executive control was thwarted and his concerns rebuffed by subsequent administrations.

Historian Daniel Bessner chronicles one of the most important ways in which the military-industrial complex's deputation was institutionalized during the Cold War, including the "propaganda efforts" of social scientists like Hans Speier. Bessner details how Speier, the founding director RAND corporation's Social Science Division, became the most influential "American defense intellectual" (2018, ix). Throughout his book, he documents how Speier's guiding principal was the anti-democratic drive to shield defense decisions from public accountability. He ideated and edified a think tank where discussion and deliberation about war could be kept away from both inter-branch scrutiny and voters (idem pp. 7, 76, 87, 226). According to Bessner, Speier and many of his colleagues correspondence, papers authored for RAND and discussions with policymakers, reflected the belief that "to defend democracy in an epoch of war [...] the United States needed to become more authoritarian" (idem p. 72).

⁵³ The intelligence agencies "predicted that potential terrorists would communicate with each other in this new global, connected world—and they could find them by identifying patterns in this massive amount of new information. Once these groups were identified, they could then follow their digital trails everywhere" (Nesbit 2017). The ethos was the idea that "birds of a feather flock together". If a national security threat's search requests humans could be tracked and sorted, its other community members could also be identified. This surveillance research was renewed under the 2003 "Total Information Awareness" program.

Hans Speier, a Jewish-German academic, led an effort to study and systematize Nazi propaganda by working outside military and diplomatic corps, through the Rockefeller Foundation. Speier was part of a group of academics pioneering “mass public opinion” studies in the United States. His cohort shared a post-war pessimism that citizens could be easily convinced to commit inhumane atrocities. In their view, the election of Hitler proved democracy was dangerous. They led efforts to counter German propaganda with American propaganda. They explicitly considered both propaganda, unlike the more contemporary perspective where propaganda (mis/disinformation) is said to be countered with truth. Indeed, their view was that counter-propaganda efforts itself had to be concealed from the public to be efficacious. These two overtly anti-democratic impulses, shielding decision-making from inter-branch accountability and shaping public opinion in secret, became a bedrock of the ever-expanding post-war military-industrial complex (Cappell 2021).

For a time, RAND was at the center of the emerging national security apparatus of think tanks, government institutions, and academic centers, providing a body of intelligentsia for the boots-on-ground private military contractors. RAND itself was the product of a 10 million dollar investment by General Henry Arnold, who had been the commander of the Army Air Forces during World War II. Douglas Aircraft Company, “one of the nation’s largest aircraft manufacturers” (Bessner 2018, 140) was produced B-29 bombers during WWII. General Arnold convinced Douglas to create and fund a private research group, “Project RAND”. The group became too large to be operated in the Douglas Aircraft offices and was spun out into its own company, the RAND corporation. Speier, the founding director RAND’s corporation’s Social Science Division, became a stalwart defender of the company’s role in producing military, intelligence and other public policies for the government, but shielded from democratic accountability (Johnson 2017). This impetus is especially acute in the effort to shield intelligence bureaucrats and police decision-making, where a system of classification and state secrets, detailed below, institutionalizes a lack of accountability (Colaresi 2014).

RAND was also at the center of the creation of a piece of legislation called the Privacy Act of 1974—the advisory committee for Secretary Eliot Richardson (Department of Health, Education, and Welfare) produced a study on privacy and computers. “A central contribution of that advisory committee, chaired by Willis H. Ware of the Rand Corporation, was the articulation of a code of fair information practices, which greatly influenced the Privacy Act and subsequent data protection legislation in other countries” (1989, 306), according to history scholar and first Information and Privacy Commissioner for the Province of British Columbia, David Flaherty. The act was “created in response to concerns about how the creation and use of computerized databases might impact individuals’ privacy rights” (Flaherty 1989, 309), as computer records made their way into the workplace, government and finance industries (Westin and Harris 1981). Centered around a limited number of federal government agencies use of individual’s data, it is considered a weak bill due to its inability to produce enforcement⁵⁴ and its role in placing privacy within the Executive branch (via the Office of Management and Budget (OMB) and (1989, 306). Flaherty characterized Reagan’s OMB as “lack[ing] political will to act on privacy matters during the Reagan presidency” (1989, 306) which is not surprising given his signing of Executive Order 12333 (see Harper 2014 and page 12). It did, however, restrict information between government agencies⁵⁵—a barrier that was undone through the PATRIOT Act with Counterterrorism Czar Richard A. Clarke’s support (2004).

According to Bessner and other historians cited above, the architects of the post-World War II/Cold War order deliberately set out to insulate this part of the government from democratic governance mechanisms. The excesses of an Executive branch insulated from democratic accountability was revealed during the second Nixon administration. Spurred by the President’s

⁵⁴ “The Privacy Protection Study Commission, would not have the power to enforce violations of the Act, but instead would submit recommendations to Congress regarding further implementation and enforcement”, “government violations of the Act had to be “willful or intentional” in order for an individual to receive damages (Flaherty 1989, 308)” and OMB would cap the misdemeanor to a \$5,000 penalty (Electronic Privacy Information Center 2003).

⁵⁵ Although this too was a weak protection, since “matching programs” do not include matches performed during a specific investigation of a particular person”, according to the law (Electronic Privacy Information Center 2003).

meddling in the Democratic National Committee, domestic and foreign surveillance was put to public scrutiny for the first time. However, Loch K. Johnson, a participant of the Church committee, and scholar of American intelligence, national security and foreign policy considers that moment of scrutiny an aberration in the broader scheme of things. Drawing from his experience as a special assistant to the chair of the Senate Select Committee House Subcommittee on Intelligence from 1975 to 1976, a staff director of the House Subcommittee on Intelligence Oversight from 1977 to 1979, and participant of the 1995-1996 Commission on the Roles and Capabilities of the US Intelligence Community, he concludes that the Legislative and Judicial branches of government have institutionalized deference to the Executive—particularly its intelligence agencies.

In his 2017 analysis of the state of surveillance in America, Johnson argues that the normal state of affairs in these branches is an attitude of ‘out of sight out of mind’ (2017, 248), producing a “conspicuous exception to the bedrock of checks and balances” of republican interbranch oversight. In his estimation, three elements perpetuate the “benign neglect” attitude. Party leadership’s unwillingness to seat Congressmembers who are true reformists in committees (ostrich-type members pervade (20, 275-288)) and electoral incentives not to participate in intelligence committees (classified nature is an obstacle to capitalizing on participation (308)) are internal institutional constraints. A dependency on scandals, requiring large scale media attention, produces a “shock theory of intelligence accountability” that can pressure members to act—or seen to be acting. However, media shocks provide only sporadic opportunities for scrutiny, they are post-facto (i.e., reactionary) which makes reform’s scope limited and dependent on the intensity of journalists’ attention (i.e., temporary) (246-274).

Deference to the Executive on bellicose matters and to the intelligence community in particular was exacerbated during the “forever wars” era of the War on Terror. Troublingly, the

Executive branch, including the Presidency itself⁵⁶, also suffers from an “intelligence exceptionalism”, which insulates⁵⁷ surveillance gathering practices’ scrutiny from within (Johnson 2017, 432, 433). Thus, the breakdown of interbranch oversight Johnson raises puts a strain on republican governance. Law scholar and practitioner Paul Rosenzweig argues many specifics of how law-and-order policies operate would be jeopardized if outed for public deliberation. For him, the viability of surveillance programs requires a level of invisibility. However, according to Rosenzweig, democratic deliberation can also be produced by a system of “delegated control”. Here, representative democracy plays a crucial role, operationalized by interbranch oversight. For example, intelligence committees’ closed sessions, requirements for clearance, and institutionalized secrecy, should help resolve the tension (2016). Both authors conclude that Legislative and Judicial deference to intelligence exceptionalism, which I exemplify below, has not met the challenge.

Deputized surveillance is a crucial element of a broader surveillance complex constituted by the state’s (exclusive) surveillance of citizens and the market’s surveillance of consumers. The ability to deputize surveillance further removes decisions, particularly technological affordances, from the government’s purview. The government can credibly wash its hands from the exponential *ability* to identify people based on data gathered by commercial firms. Simultaneously, voters could not

⁵⁶ Johnson reminds the reader that the Church Committee concluded “these ambiguous arrangements are intentional, designed to protect the president and to blur accountability— the infamous doctrine of plausible deniability, whereby unelected bureaucrats frequently decided when and where covert actions would occur, all in the name of keeping the president’s hands clean and the reputation of the United States unsullied. Put another way in bumper-sticker form: No Overseers Allowed!” (Johnson 2017, 313). But intelligence exceptionalism works both ways. The President and the other two branches of government have their own agency and could push back harder against the intelligence community. In sum, according to Johnson, the conditions for plausible deniability are maintained by intelligence agencies, and purported overseers. Deputation further removes surveillance decisions, particularly technological decisions, from the government’s purview. This observation furthers my own argument that a general repudiation of regulation of the surveillance complex is a function of the government’s unwillingness to subject its decision-making and deputation arrangements to democratic scrutiny from the voters.

⁵⁷ Many aspects of intelligence gathering, and increasingly domestic policing, are afforded institutional deference and also help agencies guard their boundaries against intrusion. For example, over-classification reinforces an ever-constraining boundary of what can be known. The history of the state secret privilege itself is an example of how inter-branch deference cedes oversight to abuse of power (American Civil Liberties Union 2018). Not pushing back very frequently makes any aberration seem utterly unacceptable and mobilizing of the intelligence community’s boundaries.

challenge the government's *willingness* to act on this ability for almost half the War on Terror, because they were kept in the dark by their government.

In the next section, I will discuss the way in which state's and market's independent desire for online behavioral data converged and bolstered incentives for each party to participate in deputized mass online surveillance. I discuss choices in the American government to highlight why surveillance capitalism alone (nor inertia to it) does not present a full story of the current situation.

Twenty years of the surveillance complex

Over the past twenty years, two forces, often seen as running parallel, have had outsized roles in shaping the internet's features and affordances. One force is the market. After the dot-com bubble, companies sought to outsource content production to their users. Users were first incentivized to "help" companies' services by filling out map restaurant review data and other content like blogs, videos, etc. The data produced by users became valuable labor. Still, as post-dot-com bubble companies pivoted to advertising, the metadata inherent to users' interaction with websites gave way to a *targeted* advertising industry that would finance free-to-use online services. Thus, people's metadata *also* became content, privatized by companies and creating a profitable business model dubbed "surveillance capitalism" (Zuboff 2015). The tech and advertising industry's ability to surveil individualized online consumer behavior is expanding to match people across devices and matching identities with online behavior and offline behavior using location, credit data, and even facial recognition (Kwet 2019).

The second force is the American government's legal and technological ability to search and seize online data in a way that disrupts the privacy regime of "analog" communications. The government moved from being limited to targeted data collection to technological access to mass data

collection, with orders of magnitude more data, including metadata⁵⁸. For example, Post-Watergate, legal limits to government surveillance were chipped away almost as soon as was politically expedient. The Foreign Intelligence Surveillance Act (FISA), which has played a large role in the NSA's use of surveillance, passed in 1978. FISA created an exception to the Fourth Amendment's requirement for probable cause when the purpose of a wiretap or search was to gather foreign intelligence. In 1981 President Ronald Reagan signed Executive Order 12333 which gave legal cover for companies to give the American government, via the Central Intelligence Agency, data on communications that take place outside the US even if they involve Americans and removed from court or Congressional oversight (Harper 2014). The 1994 Communications Assistance for Law Enforcement Act (CALEA), expanded deputation. This piece of legislation is a prime example of how deputation works, differently to government-led surveillance. CALEA "forced telephone companies to redesign their network architectures to make it easier for law enforcement to wiretap digital telephone calls" (The Electronic Frontier Foundation 2017). The government took the change in technologies to argue previous wiretapping standards of physical phone lines should not apply. The transition to digital communications seemed to create a legal vacuum in the courts, Congress, and the Executive branches, as every instance let this argument stand.

Executive prerogatives on surveillance were in place before 9/11. Laws like FISA, which required active participation from all three branches (in its drafting, passing and upholding, and execution), and public executive orders like President Reagan's 12333 reflected a widespread effort among American government officials, throughout the decades and across party lines, that shielding surveillance from public deliberation and democratic accountability. The external shock from 9/11

⁵⁸ The legal limits erected after Watergate were chipped away almost as soon as was politically expedient. The Foreign Intelligence Surveillance Act (FISA), which has played a large role in the NSA's use of surveillance, was passed in 1978. It created an exception to the Fourth Amendment's requirement for probable cause when the purpose of a wiretap or search was to gather foreign intelligence. In 1981 President Ronald Reagan signed Executive Order 12333 which gave legal cover for companies to give the American government, via the Central Intelligence Agency, data on communications that take place outside the US even if they involve Americans and removed from court or Congressional oversight (Harper 2014).

ostracized those who remained concerned over mass surveillance. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, abbreviated as the [US] PATRIOT Act, passed only 45 days after 9/11⁵⁹, institutionalized the surveillance complex, further, relying on deputation, further exacerbating opportunities to shield policies from interbranch oversight.

According to civil liberties organizations, the bill undid protections that were “part of a longstanding law enforcement wish list that had been previously rejected by Congress, in some cases repeatedly”. The shock of 9/11 let the provisions take root⁶⁰. The PATRIOT Act, and its subsequent renewals in 2008, 2015, and 2018 (2023 debate is ongoing)⁶¹, have expanded the government’s ability to access records of all sorts⁶² held by third parties (Section 215), and to attach gag-orders silencing disclosure (Section 213, “National Security Letters”) with the assistance of a classified judicial order (see discussion on Foreign Intelligence Surveillance Act below). The original bill also allowed indefinite detention of non-citizens, even without a trial, opening the door to Guantanamo Bay and black sites abroad⁶³ (American Civil Liberties Union 2022).

Between 2005 and 2008, NSA employees tried to blow the whistle: Verizon was providing the government with direct access to copy all incoming data (Risen and Lichtblau 2005). Whistleblowers like Bill Binney⁶⁴, a leading NSA crypto-mathematician, tried to blow the whistle on the NSA’s use of his software to “scoop up information on Americans without a court order” (Welna 2014). In 2002

⁵⁹ The legislation was drafted by George W. Bush’s Attorney General John Ashcroft, sent to the Senate floor with no discussion, debate, or hearing, where it passed the Senate 98 to 1 (and 1 absent) through an up-or-down vote procedure that bypassed requests for amendments. The House passed it 357 (211 Republicans, 1 Independent, 145 Democrats) to 66 nays (62 Democrats, 1 Independent and 1 Republican), 9 absent.

⁶⁰ But how does it explain continuous support? I turn to this question in chapter 3.

⁶¹ Section 702 is again up for renewal. The Biden administration is currently lobbying Congress to renew it (Savage, Biden Administration Asks Congress to Reauthorize Warrantless Surveillance Law 2023), even as one Republican member has been known to have been “looked up” by the FBI (Savage 2023).

⁶² See footnote 44 “tangible things”.

⁶³ Chicago also has a blacksite, see footnote 91.

⁶⁴ Former NSA officials Kirk Wiebe and Edward Loomis, and a former senior Congressional staffer, Diane Roark, also signed the internal NSA complaint.

he contacted congressional committees and submitted a complaint to the Pentagon's Office of the Inspector General. He was rebuffed by both, but that did not stop a dozen FBI agents from entering his home with guns or keep the federal government from charging him. Thomas Drake, a computer expert, also tried engaging with Congress when he submitted a complaint over the NSA's surveillance programs—some of which started before September 2001 (Hertsgaard 2016). After encountering Legislative resistance to exercise the constitutionally proscribed oversight, Drake's home was also stormed by FBI agents. He was indicted in 2010 by the Obama administration for violating the Espionage Act after taking his complaints to the press.

AT&T and Verizon were part of what was later disclosed to be a "Special Source Operation" division. which according to internal documents, "is responsible for more than 80 percent of the information the N.S.A. collects, one document states" (Angwin, Savage, et al. 2015). Verizon lawyers, including then-senior council and future Attorney General Bill Barr, worried that the exposure of their collaboration to wiretaps would open them up to consumer lawsuits. Indeed, a group of customers for both companies claimed that the N.S.A.'s tapping of the Internet violated the Fourth Amendment protection against unreasonable searches (*Hepting v. AT&T* and *Electronic Frontier Foundation v. Verizon/MCI* were tried together, or "enjoined"). The Obama administration argued to dismiss under state secrets privilege. It argued that mere collection of their data—if such a thing had occurred, was not harmful⁶⁵; only government search or review of the records was. In a catch-22, it further argued that the defendants could not prove standing, defined by search or review of records, because that was a state secret (Crocker 2015). The Supreme Court was swayed by the argument that public discussion of telecom surveillance would reveal state secrets and damage national security, ending one avenue for citizens to exert accountability (Angwin, Savage, et al. 2015). Journalist Spencer Ackerman reported that Barr additionally lobbied Congress directly (2021, 35). The legislative branch passed the

⁶⁵ See discussion on harms based approach in dissertation introduction and further in this chapter.

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, and retroactively immunizing telecommunication companies from responding to government requests under the PATRIOT Act's section 702, including phone and email metadata and substantive communications (Johnson 2017, 180, American Civil Liberties Union 2008).

By the time Snowden blew the whistle, internet use became ubiquitously accessible in the US, with always-on wifi, mobile data, GPS tracking, and online devices dotting our physical surroundings. As a response to an overwhelming amount of documentary evidence, all American government branches moved from an “ostrich” attitude, refusing to regulate the surveillance complex, to proactively legitimating monitoring digital communications, including access to deputized data-collection.

These critical incidents document the mobilization of institutional resources, within all branches of government, where plausible deniability or inertia cannot be argued. Congressional members refused to act on whistleblower information that mass surveillance was occurring. The Executive branch moved to suppress whistleblowers' ability to present their first-hand knowledge as evidence, prosecuting sources and journalists like Risen. The judiciary also participated in maintaining the surveillance complex via the secret FISA courts (Gellman 2020, 101) and by publicly dismissing Fourth-amendment cases cited above. Even when the FISA courts are required to participate, they have been accused of acting “hand in glove” (Abramson 2013) with government lawyers making requests to the court, approving 99% of all wiretap applications by its own calculations (Walton 2013).

The government, for its own part, fights to keep information out of the public consistently. Even in 2015, when information about phone companies' deputation documenting direct government access was public knowledge, “the government has [still] been fighting in court to keep the identities of its telecom partners hidden” (Angwin, Savage, et al. 2015). This support is ongoing, as surveillance programs come up for renewal (in 2015 and this year, 2023).

Government and market surveillance are often analyzed in separate spheres, yet they don't just run in parallel; they are entwined. Examples of notorious American legislation, like the PATRIOT Act, the original Foreign Intelligence Surveillance Act, and its 2008 amendments (including Section 702), point to how governance practices like deputation entwine both. Yet, academia's siloed critiques have shifted focus from the state to social networks and back to the state, resulting in disassociated and reactive scholarship. The Snowden revelations made clear there was a collaborative relationship. The internet's operation privatized by the US in the 1990s into the commercially run system of ISPs and OSPs we now use (Packard 2020). But many of the underlying technologies, protocols, standards, and services (like unencrypted email) sprung from the university-military collaboration. They often reflect their Department of Defense DARPA/NET origins. For example, it took more than two decades for most websites to voluntarily switch from the original unencrypted `http://` transfer protocol to a secured `https://`, but browsers still load both. Path dependency restricts many technologies. The US' government ability to shape technologies through direct investments (e.g., Google seed funding), and forbearance, can provide it with generous access to online data collected by corporations. I detail these additional efforts in the next section.

Why would the American government close itself off from the data tap? Spier produces a two-step answer on how to avoid direct democratic pressure from voters. First and foremost, they can be disengaged by avoiding exposure to information on surveillance policies. If that fails, the government should shape public opinion, by using propaganda, he would argue. After 2016, entire subfield in political opinion has devoted itself to splitting hairs over what is propaganda, misinformation, and disinformation. I will not argue for any particular label. What I will argue is that after the Snowden revelations, the Executive branch—most visibly the President—engaged in a media campaign to shape public opinion defending the surveillance programs (Henderson 2013), even

capitalizing on his 2008 campaign as a skeptic who had become “informed” while in office (Harris 2013).

However, the President kept further details of the programs to a minimum, and, I would argue, engaged in process of “reframing” mass online surveillance as targeted surveillance, by continuously invoking unverifiable assurances that only terrorists were affected by these policies. Implicitly, he was relying on the harms-based definition of a privacy violation (use of surveillance data, not surveillance itself) that had been successfully used in Court cases. In chapter 3 I test whether a similar reframing or redefinition of a mass online surveillance policy that only makes salient disliked groups is more acceptable than when the policy makes liked groups salient.

Obama helped reproduce this minimal-information cognitive dissonance by capitalizing on a sense that, unlike Bush, he had thought things through and could be trusted to make decisions on the subject through deep consideration of the matter⁶⁶. Despite this, the district and circuit courts in 2015 found that aspects of the original Section 215 unconstitutional, particularly because of retroactive identification of what is relevant in a terrorist/criminal subjects everyone else to an unconstitutional search-and-seizure where ‘irrelevant’ documents are obtained (McKinney 2020). 2015 and 2018 amendments to the PATRIOT Act restituted bulk data collection capabilities.

Electoral competition on mass surveillance was also kneecapped because the NSA revelations moved the Democrat President to mobilize a “liberal” campaign of legitimization and support for a mass online surveillance program begat by his Republican predecessor (Ackerman, *Reign of Terror*

⁶⁶ Johnson bluntly asserts that “Both the Bush and Obama Administrations chose to ignore the PATRIOT Act’s limits on surveillance and they took advantage of loopholes; plus, the legal standard of probable cause of criminal activity was set aside. At the time, members of Congress anticipated neither the NSA’s warrantless wiretaps nor its metadata collection. The PATRIOT Act and FISA were further modified to permit the NSA to tap the telephones of terrorists who communicated to one another overseas, but whose conversations were routed through international communication nodes located in the United States. This was a sensible idea, but one that should have been adopted as an amendment to FISA through the normal legislative process, not stuffed down the throats of lawmakers by executive branch insistence. The upshot of this maneuvering by two consecutive White Houses (Bush and Obama), under the flimsy cover of the PATRIOT Act, eventually became clear: the three branches of government had approved sweeping surveillance programs that were out of step with a democratic public’s right to privacy, even in an era of global terrorism” (2017, 180).

2021, Samuelsohn 2014). The gist of the argument was more or less, “I heard you, now trust me to use these tools ‘the right way’⁶⁷”. Despite assurances, 2015 assessments conducted around the time of the second renewal’s debate considered that reforms had been minimal, at the margins (Childress 2015), ineffective at keeping the NSA from breaching them (McKinney 2019), and that a sunset of Section 215 would still leave the government with plenty of other options for mass surveillance (Crocker and Cohn 2015).

Simultaneously, the American government has also kept shaping mass data collection practices by deputized firms like Alphabet (Google’s parent company), Microsoft, Facebook, and Amazon (collectively described as data Goliaths (Schneier 2015)). I document under-explored aspects of government’s role in the surveillance complex in the next section. The US’ continued influence on the political economy of surveillance has incentivized the European Union to pursue its own regulatory schemes, which I discuss in Chapter 4.

In the next section I will outline the range of tools used by the government to induce, convince or compel companies to collaborate in deputized surveillance. I will also argue nonregulation, in addition to forbearance (Dewey and Di Carlo 2021), should not be interpreted as a (default) lack of action, but as a political *choice* to shape markets, making the invisible hand visible. The American hands-

⁶⁷ One might ask, why bother with secrecy if people can be sufficiently scared into tolerating mass online surveillance? I would argue there are several reasons why this is a second-tier option to secrecy. First, the government cannot ‘take back’ information. So, it has to gamble on the idea that a specific group will remain sufficiently and credibly scary. Indeed, the PATRIOT Act was passed publicly, with visible support from almost all legislators, partly because the threat/anxiety levels were high (Huddy, et al. 2005). But a public scapegoating tactic years on is harder to sustain. For example, because the idea of terrorism is so amorphous, Republicans engaged in racial profiling, linking terrorism to Muslims. This increasingly made Democrats uncomfortable, especially when one of its candidates was branded as a “secret Muslim”. Democrats branded Republicans as engaging in a sustained campaign of intolerance, which played into a larger electoral competition dynamic of hate vs hope, and now anti-woke vs woke/inclusive.

January 6 could have been a point of true polarization, where Democrats and even Independents were highly mobilized *against* Republicans. If Biden had wanted to really capitalize on it, he could have for example, nominated a way more aggressive AG, who would have leaned on deputized surveillance and publicly justified it as helping identify insurrectionists much more. It would not have been implausible that Republicans would have done this had the parties been reversed (and they did use mass surveillance during BLM protests). But as discussed above, information can’t be taken back. Now that the House is in Republican control, the Democratic President is asking the Republican majority to renew Section 702 of the PATRIOT Act. Insurrectionist scare tactics would have been highly alienating and difficult to forget.

off approach to regulation also includes overt deregulation, although this is less frequently observed⁶⁸. While the Biden administration’s Federal Trade Commission (FTC)⁶⁹ and Securities and Exchange Commission (SEC)⁷⁰ have proposed some limits and penalties for corporations’ surveillance practices. The move follows that administration’s effort to securitize privacy, as many sectors become wrapped up in “critical infrastructure” (The White House 2023, Section 3. Shape Market Forces to Drive Security and Resilience). However, the government itself remains legally free to piggyback off corporate surveillance infrastructure on the cheap—politically and economically. In February 2023 it also began lobbying Congress to renew Section 702 of the PATRIOT Act⁷¹.

By hook or by crook: degrees of collaboration

Throughout the last 20 years, the American government’s track record on privacy protection enforcement has been extremely permissive. For Flaherty, privacy issues in the United States “are raised in a political climate and need to be sold to the executive and legislative branches. This is an especially telling condition in a data protection system that relies critically on special sectoral legislation” (Flaherty 1989, 310), meaning an industry or issue-centered patchwork approach. Indeed, one of the last privacy laws passed arose out of President Reagan’s failed nomination of Judge Robert Bork—when a journalist obtained his video-rental history. Despite rejecting the nominee, Congress, shocked by the disclosure of a high-profile member of government’s data, legislated on the non-

⁶⁸ The repertoire of possible actions can be: active deregulation, active nonregulation, and active regulation, forbearance (regulation but no enforcement), active investment, and passive nonregulation.

⁶⁹ The FTC has limited statutory ability to pursue privacy cases under its mandate to “prohibit unfair or deceptive acts or practices” (US Congress 1938), the Fair Credit Reporting Act and the Children’s Online Privacy Protection Act (COPPA). Thus, privacy can only be violated if it was promised.

⁷⁰ The SEC has a Privacy of Consumer Financial Information and Safeguarding Personal Information regulation, usually shortened to “Regulation S-P”. It was derived from the Gramm-Leach-Bliley Act of 1999 formulated in 2000 and updated ‘for nomenclature’ in 2009. These impose “three requirements on registered broker-dealers, investment companies, and investment advisers (‘covered institutions’) related to protecting certain ‘nonpublic personal information’ (Bryan, et al. 2023)”. The SEC’s primary point of interest on privacy is viewed through the lens of data/cybersecurity, so proposals awaiting public comments issued on March 15, 2023 geared towards “imposing new requirements related to investigation and reporting of data breaches” (idem). The move follows an effort to securitize privacy, as many sectors become wrapped up in “critical infrastructure” (The White House 2023, Section 3. Shape Market Forces to Drive Security and Resilience).

⁷¹ So at least we are seeing some policy check-and-balance within the Biden Executive branch.

disclosure of VHS records. But “one of the chief limits of such an incremental approach, since coalitions and ripe conditions have to be constructed anew as each need arises” (idem). As videos went digital, “Netflix lobbied successfully to change the Video Privacy Protection Act to allow for sharing on social networks [Facebook specifically]. President Obama signed those changes into law in January [2013]” (Tsukayama 2013), increasing the market’s ability to share online data between itself by deregulation.

An insight of this dissertation is that America’s continued bipartisan non-regulation/forbearance shapes the conditions of technological supply and informs citizens’ concerns towards mass surveillance (compare to Chapter 4 on Europe). In this section, I will discuss how the government shapes, on the one hand, an expectation at the citizen level that surveillance is ordinary and legal when corporations do it and, on the other hand, fosters at the firm level an expectation that few—if any—data monitoring goes too far. Government forbearance, nonregulation and deregulation develops an expansive scope for surveillance supply and simultaneously institutionalizes the minimization of voter demand for privacy. This, in turn, can reinforce the government’s incentive to keep deputizing its own surveillance of the market, as citizens’ concerns can be demobilized or treated as minority aberrations/nuisance (Chapters 2 and 3 produce evidence that complicates this argument. The technical data in Chapter 5 provides raw proportions for American attitudes in 2021).

Cybersecurity expert and political commentator, Bruce Schneier, has argued that the US has little reason to prevent private companies from engaging in online surveillance and data collection partly because government agencies rely on companies to reduce the cost of their surveillance (2015, 2017). As mentioned in the introduction, the practice of deputizing online monitoring took shape with American companies’ response to the 1998 Digital Millennium Copyright Act incentives . The government was worried about how online content could be folded into a profitable market with clear property ownership rules that favored prominent content creators. With this law, the US government

kept most disputes off the court, giving those accused of copyright infringement few legal avenues to dispute the facts. What effect did deputation have on internet companies' technologies?

The practice of deputizing copyright dispute adjudication produced legal incentives for Google and other web hosting services to develop automated content surveillance. In time, Google and other firms have developed methods to inspect massive amounts of data to get ahead of copyright complaints, building the infrastructure for preemptive internet filters like YouTube's music identification system and algorithmic copyright enforcement (Perel and Elkin-Koren 2016). This type of online surveillance deputation for copyright enforcement has been more public-facing because firms have framed it as constructive cooperative partnership agreements with content producers.

The government's ability to remove itself as the rightful arbiter of copyright claims through trial has primarily succeeded in shifting the economic onus and much public deliberation on competing for fair use claims onto a licensing (i.e., rental) system. Firms have moved into this space because of legal incentives and economic benefits. Deputized copyright violations surveillance has fostered the dismantlement of "terminal" markets where people own (i.e., purchase) digital content. This was made explicit when "buyers" were shocked to find their "purchased" copies of George Orwell's 1984 were removed from their Amazon Kindle devices (Stone 2009). The terms of services are digital licenses, basically, a one-time fee rental, which do not produce ownership.

Snowden evidenced the market's more secretive collaboration on surveillance with other priorities of the American government. Many companies were forced to acknowledge their role in deputized surveillance and deal with the fact that their users did not like this. One of the moves they made to reconstitute user trust, in an attempt to shape public consumer opinion, was to begin publishing transparency records.⁷² These reports document the number of government demands a company

⁷² These records replicated the copyright takedown transparency reports with one important caveat. Copyright takedowns identify which links were flagged as infringing, and by whom. Government takedown requests are aggregated by country, but the data that triggered the request is not made public, even when the company refuses.

receives every six months to 1) take down data and 2) identify users. Companies like Twitter and Google began documenting these (in 2016 and 2013 respectively), including documenting their compliance rate, to shape document a counter-narrative that they did not give into every request. However, Google's initial reports did not include disclosure of National Security Letter requests (Auerbach and Galperin 2013). To this day, in a less advertised show of government deference, both companies submit their draft results for clearance to the US government. The Ninth Circuit Court of Appeals ruled in *Twitter v. Garland* on March 2023 that an Obama-era Department of Justice request (defended by Biden's AG, Merick Garland) from the FBI to censor Twitter's 2014 report did not constitute violation of the First Amendment. The EFF, amicus brief authors in the case, note that this step backwards in transparency was exacerbated in the appeals ruling. "Not only did the Ninth Circuit uphold the lower court's ruling, it went out of its way to find that a large, well established body of prior restraint law did not apply", further separating the Bill of rights' application in digital spaces from pre-internet communication.

transparency.twitter.com/en/reports/information-requests.html#2016-jul-dec

Information Requests

Government Non-Government Jul - Dec 2016 Download Report

01. Latest Data: Government

Map data Bars data

Search for a country 1-7 of 50 1 2 ... 11 View All

Country	Information requests			Compliance rate			Accounts specified			Pre-2016
	Routine	Emergency	Combined	Routine	Emergency	Combined	Routine	Emergency	Combined	
Worldwide	4,917	1,145	6,062	63.5 %	66.6 %	64.4 %	9,856	1,479	11,335	2,251
United States	1,892	412	2,304	82 %	80 %	82 %	5,112	506	5,618	1,941
Japan	790	187	977	64 %	65 %	64 %	1,007	209	1,216	0
United Kingdom	575	106	681	79 %	81 %	79 %	792	225	1,017	32
France	445	56	501	69 %	73 %	69 %	525	62	587	5
Turkey	458	35	493	0 %	0 %	0 %	1,011	65	1,076	0
Germany	247	28	275	51 %	79 %	54 %	371	33	404	1
India	151	17	168	25 %	12 %	23 %	403	24	427	120

Information requests (government) Jul 1 - Dec 31, 2016

About the numbers

Figure 2 First Twitter government transparency report, 2016

Perhaps more important but less discussed in retrospective accounts of the revelations, shareholders did not like those deals being scrutinized. Companies like Apple used public relations strategies, such as visibly fighting selected high-profile data requests (e.g., San Bernadino phone unlocking) in court. They have also publicly marketed “privacy” as part of their technologies. Their attempts to appease users and differentiate itself from other computing companies stood in contrast from Microsoft, Google and Amazon cloud computing (AWS), who have all tried to compete for military contracts. Apple is now facing a class-action false advertising lawsuit given the revelations that it has continued providing data to law enforcement and it plans on instituting bulk image recognition (Brown 2022).



Figure 3 Apple's privacy billboard marketing

Many companies publicly protested and decried their ignorance and shock. A growing industry of third-party intermediaries, or data-brokers, has facilitated the transfer and aggregation of data from apps and websites to the US government, who has turned to purchases after the 2018 Carpenter decision brought back warrant requirements when compelling companies to produce sensitive data (more below).

However, analysis years later shows that collaboration agreements (even with Apple), did not end after Snowden (Kroll 2021). Yet, companies remain deputized into investigative work, including monitoring, that used to be done by police *after* a crime was reported. If anything, the political pressure on technology firms to monitor users' online behavior has reached a crescendo after the January 06 insurrection⁷³ (Hill 2021). Because of the illiberal nature of the insurrection, supporters of deputized surveillance used the opportunity to try to “shift the Overton window” (Astor 2019). Clearview A.I., a company with law enforcement contracts, took the opportunity to highlight the benefits to collecting video surveillance, embedding facial recognition capabilities, and aggregating them to online posts (2021). These echo previous attempts to reframe mass surveillance deputation as being targeted, and used for liberal (pro-democracy) purposes, in order to build public legitimacy.

Because of a growing interest in encryption after the Snowden revelations, the US government renewed its public attack on the technology (Jarvis 2021). It stated that without companies' collaboration handling over data, as the PATRIOT Act and the 2008 FISA Amendment section 702 demanded, encryption technologies would blind it from monitoring terrorist plots, implying the government would stop terrorism before it happened (Director of National Intelligence 2022). Panic over whether the government would be “in the dark” in national security has been debated (Klimburg 2017, Gasser, et al. 2016). Critics like Barton Gellman, one of three journalists who published the Snowden NSA revelations, retort there is little evidence offered by intelligence agencies to prove that weakening digital security to intrude on everyone's privacy has yielded some national security gain (2020). Critics like cybersecurity expert Bruce Schneier argue that the US has only itself to blame for legitimizing the use of undisclosed source code vulnerabilities (zero-day exploits), producing a market

⁷³ At present, the developer of the Clearview AI facial recognition software is stepping up his attempt to normalize its use by offering it for free to the Ukrainian government to identify Russian soldier corpses with Russian social media, who obviously cannot consent and are reviled in the American left (and some of the American right) (Hill, Facial Recognition Goes to War 2022). It has also recruited a former Obama ambassador and Biden administration lawyer Lee Wolosky to its advisory board in a bid to increase its legitimacy.

for their sale, and unleashing a host of tools that break the internet and increase cyberattack risks (2018). Commercial surveillance relations where the government is the client (e.g., Palantir) are very much a part of how deputized surveillance works, but it is not the sole mode of relation between states and the market.

In the next section, I discuss how the government uses a range of incentives (carrots) *and* coercive (sticks) tools to obtain data by hook or by crook. The diversity of strategies is pivotal to my preference for using deputation instead of outsourcing as the descriptor. It expands our view of the state's relation to firms beyond formal contracts, which predominated the hardware-centric pre-internet military-industrial complex. Other more coercive relations take shape through National Security Letters or hostile covert actions to access data held by private firms (Perlroth 2021). Dual-use software also adds a layer of complexity and decentralization in decision-making over technological innovation that further justifies a broader lens than the concept of outsourcing military hardware production allows.

Carrots

Companies that collect user data have so far been subjected to little oversight. The pattern of nonregulation and forbearance (discussed below) has led to the growth of data brokers. Some companies are obscure, but they are so lucrative that large firms like Oracle “owns and works with over 80 data brokers”, according to a 2019 Financial Times report which calls that firm, Nielsen, and Salesforce “super⁷⁴ data broker(s)—the privacy deathstars” (Ram and Murgia 2019). Data brokers are “middlemen of surveillance capitalism [...] aggregating information on everything from consumer shopping to internet behavior. However, many companies also scrape data that is publicly viewable” (Sherman 2021).

⁷⁴ Data brokers have grown so profitable that their collective lobbying expenditure rivals in 2020 “rivalled the spending of individual Big Tech firms like Facebook and Google” (Ng and Varner 2021). 25 data broker firms totaled \$29 million, including 9.5 million from the top spender, Oracle. Facebook spent \$19,680,000, Amazon \$18,725,000, and Google \$8,850,000 according to Ng and Varnier’s findings.

Data Goliaths like Facebook, Google, Twitter, and Snapchat have data broker customers, including Acxiom, Oracle, and the credit monitoring company Experian (Ram and Murgia 2019), creating “a kind of distributed surveillance economy ... [that is] also collaborating with each other and large old-school data brokers like Acxiom”, according to Wolfie Christl, a researcher at the Austrian non-profit Cracked Labs.

Only recently have companies who mishandle massive amounts of data been asked to pay relatively minute fines (compared to their profits), often until years later. So far, data brokers have been exempted⁷⁵, because the legal basis for these fines is the FTC’s limited statutory ability to pursue cases where “unfair or deceptive acts or practices” have occurred. Since data-brokers make no claim to user privacy, these companies have become a useful intermediary in maintaining surveillance capitalism *and* selling to the government (Klosowski 2021).

In contrast, fines have recently been handed down to Data Goliaths (Bond and Allyn 2020). The firm’s prominence makes milquetoast reprimands a bipartisan political win⁷⁶—as long as the fine is small enough that doesn’t change the market’s incentive structure. This tendency has also led others to observe diffident regulation generates an incentive for companies to maximize data collection for their profit (Wu 2019, Wu 2016). The US is also unique in its sectoral approach to privacy legislation. The US applies limited protection standards to only three types of data: health, education, or finance. However, protections are not proactively enforced and do not extend to intermediaries⁷⁷.

⁷⁵ The US Federal Trade Commission announced in September 2022 that it was suing a location data broker, Kochava, under the US FTC Act’s unfair methods of competition mandate. Courts will have to decide whether the argument that this statute’s regulation of practices can be used as a means of minimizing online location data trade, and whether these practices are “unfair”. The FTC Act defines unfair when (1) the practice “is likely to cause substantial injury to consumers”; (2) the practice “is not reasonably avoidable by consumers themselves”; and (3) the injury is “not outweighed by countervailing benefits to consumers or to competition.” (Schwartz 2022) The FTC is alleging the consumers are users of online apps, but Kochava doesn’t deal with users, the users’ data is the product. Its consumers are any number of advertisers and perhaps not implausibly given federal agencies’ purchases of commercial data, the government itself.

⁷⁶ See competing anti-trust books published in 2021 by Republican Senators Josh Hawley and Democrat Amy Klobuchar.

⁷⁷ For example, Facebook has received health data from installing pixels in hospital websites (Feathers, et al. 2022). This may not even be a violation of the only healthcare privacy bill, HIPPA, depending on whether there is patient consent for sharing data embedded in a Privacy Notice or Terms of Service disclosure and a Business Associate Agreement

Furthermore, even though Data Goliaths handle these types of data, they have so far been able to maintain the perception that they should not be regulated as health companies⁷⁸, education companies, or financial institutions⁷⁹. According to public policy scholar Priscilla Regan, the United States “has adopted the most aggressive self-regulatory approach”. In her estimation, the country’s privacy regime is an exception, given the absence of any national authority which could enforce contractual privacy promises. That, “in effect, let[s] businesses respond to the market demands of consumers for their preferred⁸⁰ level of privacy protection” (Regan 2012, 402). As data goes digital, education, health, and finance data have been monetized and “app-ified”, escaping systematic legal scrutiny. This blindspot is caused by the US’ threshold for privacy, which makes wrongful disclosure of data, not its collection, the bar for legal standing. Harm is defined in terms of the data’s outcome instead of the process (Citron and Gray 2013, Solove and Citron 2021). In other words, individuals must be able to claim/prove harm from the disclosure of their health, education, or financial data to seek monetary recourses from companies. Without a way for citizens-cum-consumers to directly impose a price for surveillance, an industry of data brokers, aggregators, and storage has emerged to support ad tracking, targeted political campaigning⁸¹, and reap financial benefits for collaborating in deputized surveillance.

(Meditology Services 2022). In any case the violation would be on the hospital’s side, not on Facebook’s. Two lawsuits has been filed.

⁷⁸ Google owns Fitbit, Facebook has access to any medical data exchanged where websites embed its pixels (Feathers, et al. 2022), Apple has its own health monitoring hardware and software in its Apple watch, Amazon was an employer healthcare telemedicine provider until the end of 2022 and is pivoting towards acquiring the “primary care start-up One Medical for \$3.9 billion” (O’Donovan 2022), as well as using its web services for training AI and producing diagnostic services.

⁷⁹ After the Trump administration tax breaks incentivized repatriating offshore account wealth, Apple took its blockbuster profits and became a finance institution by issuing its own credit card in 2019.

⁸⁰ Consumer demand, however, is severely limited by corporations’ misleading promises and obfuscation of information about data collection and use.

⁸¹ The New York University’s Cybersecurity for Democracy project has attempted to analyze targeted political ads on Facebook. In an auditing process, they revealed systematic under-reporting in the self-disclosed database. Laura Edelson, co-founder of the project, concluded that “We can’t trust Facebook to do a good enough job identifying or disclosing political ads on its own. We need mandated transparency powering independent research to identify weaknesses and hold platforms accountable” (Cybersecurity for Democracy 2021), but attempts to produce an independent dataset with user-submitted data led the company to block all access (Edelson and McCoy 2021), as well as further weakening internally produced data available for journalists (Roose 2021).

These decisions have led to a moral hazard: companies have financial incentives to collect and sell as much data as possible and ask forgiveness later—if asked to do so at all. By virtue of their visibility, Data Goliaths are more likely to face some regulatory scrutiny than the data brokers they interact with. However, legal scrutiny does not ensure chastisement. For example, by 2007, Facebook was already using its data access for advertising (Newcomb 2018, Angwin, Parris Jr. and Mattu 2016). A lawsuit alleged that it violated several federal privacy and consumer laws (Lane v. Facebook, Inc. 2021). But Facebook successfully argued that the size of the fine would be so big it would be bankrupted, echoing banks’ “too big to fail” arguments. Instead of pursuing economic punishment to dissuade future abuse of collected data by Facebook or any other company, the government decided to enforce *no* legal penalty, effectively sending the message “if you get caught, it will be ok”. Instead, the Department of Justice chose to put Facebook under a consent decree that required audits. When the company was later accused of violating that consent decree over third-party app access to data, the company had made \$55 billion in profits that year alone and set aside \$7 billion for the prospective fine. When the government announced the fine, 2 billion dollars lower than expected, Facebook’s stock price went up. The stock rise signaled markets were comfortable factoring in sporadic privacy fines as a “cost of business”⁸². As long as consequences are weak, stochastic, and do not interfere with profits, Data Goliaths will face no pressure to change their practices. Investors will also be unlikely to finance firms with competing business models, further making it impossible for consumers to “just leave” and use those imaginary services.

Government funding of tech startups is another crucial component of the corporate surveillance infrastructure that governments later relied on for deputation. More than a dozen multi-million dollar grants have been awarded through the National Science Foundation to foster private-

⁸² The two Democratic commissioners’ dissent construed the fine as “a substantial undervaluation [...] The fact that Facebook’s stock value increased with the disclosure of a potential \$5 billion penalty may suggest that the market believes that a penalty at this level makes a violation profitable” (Feiner and Rodriguez 2019).

public collaborations in the tradition of RAND. Some grants have addressed intelligence community needs by shaping accessibility to pivotal technology companies. Some examples are chip maker Qualcomm⁸³ (National Science Foundation 1987), anti-virus service Symantec (which functions by scanning a computer), Netscape browser, and development of technologies like Doppler radar and fiber optics (Nesbit 2017). One notorious investment (alluded to on page 5) was the \$4.5 million “cooperative agreement” grant for Stanford’s Digital Library Initiative (National Science Foundation 1994), which led to the web crawling prototype that would become Google (PolitiFact 2012). The research drew the attention of the Department of Defense and became part of the Total Information Awareness effort after 9/11.

One aspect of the political economy of the surveillance complex that has been less critiqued is that digital services and hardware face no “regulation” within the market (through competition), which further entrenches deputized surveillance. Two complimentary tactics take place, forbearance of existing privacy laws (already weak and in a patchwork), and an (explicit) resistance to regulate privacy. These tactics have exacerbated harms in ways that are having ripple effects across industries. For example, the incentives to collect as much data as possible, and to do so to maintain constant identifiability across online and offline behaviors has increased the amount of actors holding sensitive and identifiable data. This has directly resulted in greater ease for conducting identity theft, as identities themselves are easily bought after cybersecurity intrusions. So, for example, a hack on Hilton hotels helps produce access to millions of passport records (Lieber 2018). This data can then be used to attempt to reset passwords and access bank accounts, producing identity theft within the financial system and IRS (Federal Trade Commission 2017).

⁸³ Qualcomm produces semiconductors, software, and services related to wireless technology, and has patents for 5G components.

Despite a push to make cybersecurity a national priority and align markets with state requirements (The White House 2023), securitizing privacy through a critical infrastructure plan puts into play previously institutionalized and explicit nonregulation efforts. James Dempsey, senior policy advisor to the Stanford Program on Geopolitics, Technology and Governance and UC Berkeley School of Law lecturer, has compiled a list of government assessments concluding that there is a “consistent theme in US. cybersecurity policy: [a] reluctance to regulate [the] private sector” (Dempsey 2023). Evidence of this are legislative bills (across administrations) that codify government’s nonregulation. The government has tied its hands, not in regards to surveillance, but in regards to measures germane to cybersecurity, which experts and the Biden administration agree include data protection/privacy.

Consistent Theme in U.S. Cybersecurity Policy: Reluctance to Regulate Private Sector

- “... we should, to the extent feasible, seek to avoid outcomes that increase gov’t regulation ...” PDD-63 (1998) [Clinton](#)
- “While the President and Congress can order Federal networks to be secured, they cannot and should not dictate solutions for private sector systems.” Defending America’s Cyberspace (2000) [Clinton](#)
- “In general, the private sector is best equipped and structured to respond to an evolving cyber threat.” National Strategy (2003) [Bush](#)
- “We can achieve these goals through a partnership with the owners and operators of critical infrastructure.” EO on Critical Infrastructure (2013) [Obama](#)
 - “voluntary information sharing program”
 - “voluntary consensus standards and industry best practices”
 - “voluntary program to support the adoption of the Cybersecurity Framework”
- It is the policy of the executive branch to use its authorities and capabilities to **support** the cybersecurity risk management efforts of the owners and operators of the Nation’s critical infrastructure. Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017) [Trump](#)
- Establishing a voluntary, collaborative effort between Fed Gov and critical infrastructure – Nat’l Security Memo on Critical Infra (2021) [Biden](#)

“Nothing in this Act or the amendments made by this Act shall be construed to grant the Secretary **any** authority to **promulgate regulations or set standards** relating to the cybersecurity of **private sector critical infrastructure** that was not in effect on the day before the date of enactment of this Act.”

National Cybersecurity Protection Act, 2014

“Nothing in this subtitle or the amendments made by this subtitle may be construed to grant the Secretary **any** authority to **promulgate regulations or set standards** relating to the cybersecurity of **non-Federal entities** ... that was not in effect on the day before the date of enactment of this Act.”

Nat’l Cybersecurity Protection Advancement Act, 2015

“Nothing in this Act or an amendment made by this Act **may be construed** --

(a) as conferring **new authorities** ..., including programmatic, **regulatory or enforcement authorities**, outside of the authorities in existence on the day before the date of enactment of this Act.”

Cybersecurity and Infrastructure Security Agency Act of 2018

Figure 4 Dempsey presentation slides on Cybersecurity non-enforcement and non-regulation

In instances when the government refuses to enforce anti-trust law, or exacts fines so weak they are negligible, Data Goliaths operate under natural monopoly conditions. Dewey and Di Carlo argue that advanced democracies use forbearance to shape the market when direct government subsidies are internationally fraught or controversial, politically or economically (2021). The lack of regulation creates incentives for companies to maximize their profits from data-gathering, whether by directly selling ads, selling data, or providing access to the data when governments require it. Whether through nonregulation, forbearance or deregulation, the widespread use of consumer surveillance disincentivizes the production of privacy-strengthened technologies.

Furthermore, Data Goliaths make consumer choice nearly impossible for the average user. These monopolies are funded partly by their collaboration with governments, have killed or bought out many competitors who could have offered privacy alternatives if the market was not so incentivized against it (Freeman 2018, Nakashima 2018). This aspect has been ignored in privacy studies because of its focus on individual user behavior, which assumes technology consumption and privacy individuals' preferences and choices are developed under conditions of competition, consent, and information that leads to meaningful choices (Svirsky 2019, Han, et al. 2020, Acquisti and Grossklags 2007, Acquisti, Brandimarte and Loewenstein 2015).

Active dismantling of regulation is clear in one instance: in 2017 the Republican congressional majorities passed a bill to overturn the FCC's ban on automatic sale of consumer data by ISPs. The FCC had required ISPs to obtain express consent for selling their consumers' website history to third parties. This bill is one of the few Big Tech bills that actively institutionalized *deregulation*. The ISP default becomes surveillance capitalism: customers must become independently informed and expressly opt-out.

Cooperation on deputation can be profitable (Gellman and Miller 2013). Google has developed contracts with the Pentagon to monitor its military hardware equipment and has vied for

cloud services contracts. The deals produced internal pushback⁸⁴ from Google’s workforce over concerns that its artificial intelligence technology would be used to analyze drone surveillance footage through Project Maven (Simonite 2021). In the fiscal year of 2011, companies designated as “corporate partners” were collectively paid \$394 million, according to a classified budget in the Snowden files (Gellman 2020, 191). The “black budget” (i.e., the redacted military budget) topline total for the National Intelligence Program hasn’t been disclosed to the public by the agency since 2007. According to Gellman, who had access to some figures through Edward Snowden’s documents, it totaled \$75.6 billion that year (52.6 plus a separate 23 for military intelligence programs), and cumulative expenditures totaling \$500 billion since 2001 (Gellman and Miller 2013). But the federal black budget doesn’t include state and local police data-gathering programs (see Backends subsection), and it is unknown whether these budgets would cover discretionary spending on data purchases.

Furthermore, no budget—public or confidential—would tally the forecasted savings (absence of cost) the government benefits from *not* having to produce in duplicate if it were to build an alternative infrastructure to deputized firms. Technology, storage, and computational analysis costs are all offloaded by accessing market data collected through National Security Letters, backdoors, zero-day exploits, and other hacking techniques (Satter 2020) (see the following two subsections). Thus, all the above figures are conservative estimates.

Until 2018, prosecutors needed to clear a “reasonable ground” standard in court when seeking cell tower records from a carrier. In June 2018, the U.S. Supreme Court made it more challenging to access call data by mandating that law enforcement provide probable cause for a crime. Pressured by the *Carpenter v. United States* decision, federal, state, and local police sought to avoid seeking individual warrants with a higher threshold of suspicion. As a response, agencies have entrenched their

⁸⁴ This worker mobilization led to Google pausing some of its work but ultimately led to the highly controversial firing of several AI ethics researchers (Wong 2020, Grant and Eidelson 2022), including Timnit Gebru and Margaret Mitchell, both co-leads of the AI team (Schiffer 2021).

reliance on deputized surveillance “carrots”, bulk buying communications, metadata, and geographical location, from data brokers and directly from apps. At the federal level, Homeland Security, the Department of Defense, the Secret Service, and even the Internal Revenue Service (IRS) have been buying these data types from apps and phone providers (Morrison 2020, Tau 2020). Local police departments have also gained video feed access to Amazon’s doorbell Ring cameras, which is augmented with facial recognition⁸⁵ software (Cagle and Ozer 2019, J. Cox 2019).

Sticks

Deputation became a prime tool of policing, and governance in the digital age as the government’s ability to monitor data became smaller relative to the massive communication flows handled by online service providers (Radden Keefe 2005). The American state, historically decentralized in its policing and further weakened at the federal level by additional neoliberal budget pressures (Passavant 2021), has increasingly deputized policing practices to corporations as firms gained the ability to monitor, retain, collate, and analyze individual data⁸⁶. Deputized surveillance is not just the product of contracts between the US government and American companies (one reason *not* to conceptualize the practice as outsourcing). Its more coercive elements have been institutionalized through the courts, Congressional bills that retroactively legalize methods, and executive prerogatives like former President Ronald Reagan’s directive 12333 on foreign data collection and implementation of classification of state secrets decisions. Court orders, legislative bills, and executive-branch memos are

⁸⁵ Amazon has its own facial recognition services, called “Rekognition”, but third-party developers, including Clearview AI and lesser known companies, have engaged with police departments and federal law enforcement on independent facial recognition contracts.

⁸⁶ MIT researchers uncovered how Minnesota’s police department engaged in covert surveillance of activists called Operation Safety Net, in the aftermath of the(ir) murder of George Floyd (Ryan-Mosley and Richards 2022). The department expanded its scope to include “tools to scour social media, track cell phones, and amass detailed images of people’s faces” on “individuals who weren’t suspected of any crime” even after Chauvin’s trial ended—when concerns over public order should have decreased. An older, widespread tactic used by police departments is independently-run cellphone towers, called Stingrays (Cullen and Zimonjic 2017). Attempting to understand how cellphone and geolocation data is used during criminal trials, journalists and defense attorneys have uncovered a legal strategy dubbed “parallel construction”, which is explained in detail on page 20.

often interpreted by the Executive and the Supreme Court in a classified and secretive, parallel system (Colaresi 2014, Gellman 2020, Risen and Lichtblau 2005) propped up by the PATRIOT Act (Wyden 2021) and the Foreign Intelligence Surveillance Act (including the 2008 FISA 702 Amendment). Congressional oversight is often weak and delayed, driven by a mix of undue trust in military decision-making and “benign neglect” (Johnson 2017).

Several layers of secrecy, institutionalized by classification decisions, make public deliberation of these programs impossible. For example, National Security Letters censor companies from disclosing they have been contacted by the government with data requests, de facto creating a free speech loophole that criminalizes alerting any user⁸⁷—whether their data was handed over or not. By one estimate, the FBI has requested more than half a million subpoenas for consumer records from private companies since 2001 (J. Valentino-DeVries 2019). The FBI issued these without judicial approval and attached indefinite gag orders⁸⁸. In 2013 the constitutionality of the NSL’s gag order conditions was challenged. The US district court ruled that these instruments impinged on free speech, *and* the government had not provided a compelling argument as to why disclosing the NSL was received harmed national security interests. However, the judge’s ruling that blanket prohibitions should cease was vacated by the Ninth Circuit Court and sent back to the district court, leaving the censorship mechanism that accompanies deputized surveillance in play.

⁸⁷ Users, customers or shareholders cannot be told, the gag orders are all-encompassing. A digital “warrant canary” has been proposed by some privacy advocates, as a type of “dead man switch” (Doctorow 2013). A public notice that data has not been requested would be visible, and taken down when a national security letter is received. In 2015 Reddit removed its warrant canary from their transparency report but of course was unable/unwilling to confirm whether the lack of a canary was deliberate (Zetter 216). However, security experts have highlighted that there is nothing stopping a warrant from including a prohibition against a warrant canary, as Australia (a Five Eyes partner) has done (Schneier 2015), especially if gag orders are not unconstitutional.

⁸⁸ One subsample, disclosed after a Freedom of Information Act request, shows that for about 700 subpoenas, credit agencies Equifax, Experian and TransUnion, financial institutions like Bank of America, Western Union and the Federal Reserve Bank of New York received a large number of NSLs. Major telecommunications providers such as AT&T and Verizon, tech companies like Google and Facebook, also received a large number of NSLs. A smaller number of subpoena requests went to Kansas State University and the University of Alabama at Birmingham, “probably because of their role in providing internet service”, according to Valentino-DeVries.

Journalist Barton Gellman details how these coercive elements of mass deputized surveillance work. Because deputized surveillance's inner workings are deliberately obscured, I quote at length from his book. The following shines a light on how the US government institutionalized the more coercive elements of surveillance deputation. In 2001, the executive branch “had to come up with a radically new—and entirely secret—interpretation of law” built on Section 215 of the PATRIOT Act. This section had given the FBI “simplified access to business records that the FISA Court found ‘relevant to’ an authorized investigation of terrorism. Relevance”, he explains:

“is a legal standard that typically limits the scope of the government’s power. It covers this, not that. It distinguishes what investigators may take from what they may not. Under Presidents Bush and Obama, the Justice Department turned that concept on its head. Government lawyers secretly persuaded the FISA Court that **every record of every call** met the relevance test because a terrorist plot might involve a party or parties unknown. The NSA proposed to find those ghosts by way of ‘contact chaining’” (Gellman 2020, 141, bolded emphasis mine).

This process gathers networked data from a person of interest, everyone they’ve contacted, everyone *they’ve* contacted, and so on. Storage and computationally intensive, the NSA decided three “hops” in the chain would be enough—but the math on that scope associates almost the entire American population. Gellman also details how during the Obama administration,

“the NSA, in concert with the FBI, dipped into this treasure trove [of data] under a secret interpretation of the legal authority that Congress granted in 2007 and 2008. Until then, the government could not search a Skype or AOL account without a Foreign Intelligence Surveillance Court warrant. Each warrant required probable cause to believe that a specific account belonged to an agent of a foreign power. The court nearly always granted those warrants, but it did perform an individual review. After Congress passed the Protect America

Act and the FISA Amendments Act, Justice Department lawyers persuaded the court that it could authorize surveillance of an unlimited number of accounts with a single order. The court's decision, based solely on government briefs, was classified as 'sensitive compartmented information'" (Gellman 2020, 112).

After individual judicial review requirements were lifted, the "NSA sent classified orders to Google by the tens of thousands, specifying accounts it wanted to tap. As long as the agency asserted a lawful foreign intelligence purpose and sent orders in valid form, Google had to comply", without being able to verify the veracity of this assertion (Gellman 2020, 269). Oversight was also weakened with the introduction of "emergency data requests"⁸⁹ that do not require court orders. In 2022 Apple and Facebook acknowledged they had provided user data, including physical address, phone number, and IP addresses, to the cybercrime group Lapsus\$—a group of hackers in the UK and US who submitted emergency requests posing as law enforcement (Turton 2022). The data handed over to Lapsus\$ facilitated financial fraud since it was used to bypass banking security and harassment campaigns.

Increasingly, US local and state police departments replicate arrangements developed by federal intelligence gathering agencies, rendering domestic constitutional protections meaningless (Lynch 2021). For example, Google has agreed to provide police departments with individuals' identifying data who are near an "area of interest"—*all* individuals whose devices ping off a cell tower or whose IP address falls under a radius of unknown size⁹⁰. This arrangement allows law

⁸⁹ According the Bloomberg analysis of Apple and Facebook transparency reports from July to December 2020, Apple received 1,162 emergency requests from 29 countries. According to its report, Apple provided data in response to 93% of those requests. Meta (Facebook) said it received 21,700 emergency requests from January to June 2021 globally and provided some data in response to 77% of the requests (Turton 2022). According to Google's transparency report for the same period, Google handed over "more than 80% of those requests, affecting the accounts of more than 89,000 users" (Bhuiyan 2022).

⁹⁰ In another echo of how foreign intelligence tactics have been imported into domestic policing, this framework of device proximity is exactly the "evidence" used by Barak Obama and his successor, to send fatal drone strikes. As a reminder, the administration worked off the presumption that *devices* whose movements fit a pattern belonged to terrorists, and anyone caught in the radius of a bomb payload should also be presumed to be a terrorist because nothing else could explain why they would be near a terrorist (Jaffer 2016).

enforcement to access Google’s “sensorvault” (J. Valentino-DeVries 2019, a) after providing only a time and a place of interest while avoiding legal standards necessary for courts to issue warrants (Valentino-DeVries 2019, b). In return, police departments get a list of all persons whose devices were in the vicinity, despite no probable cause being issued and reviewed by a court. Google’s transparency report showed it had “received approximately 20,000 geofence warrants between 2018 and 2020 [...] 95.6% came from state and local police agencies, with nearly 20% of all state requests coming solely from agencies in California” (Lynch 2021).

Federal agencies like the US’ Drug Enforcement Administration (Masnick 2014), and FBI (Cushing 2016) produce information from warrantless searches and roving wiretaps from Stingray cell towers that are routinely passed on to other law enforcement agents (e.g., local or state law enforcement). Parallel construction is a retroactive process by which, after obtaining that surveillance data, police *then* apply for a search warrant, knowing what to look for since it has already been identified (Matsakis 2018). Courts characterize this practice, documented by Human Rights Watch (2019), as a process that launders the “fruit of the poisonous tree” into the evidence chain. Judges have also accused agencies of misleading them with applications for cell site location. The FBI’s non-disclosure agreements signed when providing access to Stingray devices have directed law enforcement to engage in parallel construction to protect both parties from public accountability (Cushing 2015). In one memo to a New York sheriff’s department, the bureau stated it was preferable to accept dismissing a case than disclose that evidence was gathered using warrantless Stingray wiretaps (Cushing 2018). According to one legal scholar, “[p]arallel construction insulates surveillance techniques from judicial review, undermines checks and balances, and deprives individuals of the privacy benefits that court review would require. It also undermines fundamental principles of due process” (Babazadeh 2018).

Three issues arise from this situation. First, there is an operational and institutional breakdown in differentiating intelligence collection, which sets its sights on foreign data and domestic policing. There is also an institutional breakdown in federalism, as local domestic police forces adopt technologies and legal tactics⁹¹ previously held by national agencies without their accompanying (albeit weak) internal mechanisms of oversight, like Inspector General officers. And finally, all these tactics and technologies run on mass surveillance—the individual cases that become known to law enforcement are the tip of an iceberg. They are not a product of targeted surveillance. Those cases are whittled down in a process that makes everyone (Americans and non-Americans) guilty until proven (momentarily) innocent⁹².

Backends

Lastly, governments of all kinds engage in their own surveillance. Still, they are increasingly sticking their hands in the market's mass surveillance cookie[s] jar instead of conducting their own targeted surveillance. American intelligence has been at the forefront of developing methods of “passive” bulk interception of corporate-owned data. The most significant innovation came when it figured out how to tap into communications as they travel through transatlantic fiber optic cables and when they reach internet exchanges (communication hubs in large cities that route traffic to smaller regions) (Radden Keefe 2005)⁹³. In the US, fiber optic cable and internet exchanges are held by corporate firms. The phrase “passive collection” is often used to convey that collection has occurred without those corporations' active involvement in disclosure and cooperation or the coercion of companies

⁹¹ Chicago's police force has at least one known black-site prison, Homan Square, where indefinite detention without trial takes place (Ackerman 2015), and has used off-the-books funds from forfeiture proceeds to purchase drones (Schuba and Main 2021) that it used to monitor protesters (CBS News Chicago 2014).

⁹² The Dobbs decision adds another layer of complexity: momentary innocence, as certain behaviors become criminalized in the future, one is proven innocent at the time of one or another request but is no longer cleared of all past wrongdoing with any certainty. This is an issue for legal scholars to grapple with but must be flagged as digital records are cheap and easy to keep in perpetuity.

⁹³ Radden Keefe's book goes into some technical detail about the United State's transition from surveillance of radio frequencies in outposts throughout the Western hemisphere to when it figured out how to intercept the light signals that pulse through fiber optic cables without distorting them, which would have produced signals corruption and thus tipped their hand.

described in the Sticks section⁹⁴. I lean towards using the term backends because it highlights the covert nature without introducing valence qualifiers that could minimize the fact that this sort of interception is still a governance choice of deputized surveillance within the surveillance complex.

After export controls on encryption were lifted (Levy 2002), American firms could develop commercial software for international sale with encryption. The broader availability of encrypted technologies made wiretapping harder. The desire for access to data has led to a systematic attack on encryption, a search for software vulnerabilities, and malware development. Security experts argue that it produces international insecurity and “makes us more vulnerable to cyberattacks” (Schneier 2017), like the WannaCry and NotPetya ransomware that spread from Ukrainian systems to other countries, including the US (Perlroth 2021). Governments, spearheaded by the US government’s demand and supply of technical knowledge, have created a demand for “zero-day exploits”, which are software vulnerabilities that are undisclosed to manufacturers so they can be leveraged to get device-level access (Sanger 2014). The result has been an international marketplace for cyber-mercenaries (DeSombre, Gjesvik and Ole Willers 2021, de Arimatéia da Cruz and Pedron 2020, McFate 2019)⁹⁵. Some famous zero-day exploits have been identified in the media by who they affect. The San Bernadino shooter’s iPhone was cracked by an Israeli company called Cellebrite after Apple refused to weaken its encryption. NSO, also an Israeli company, was hired by the Saudi Arabian Crown Prince Mohammed bin Salman to infect journalist Jamal Khashoggi’s phone with a zero-day exploit that monitored his communications and location, leading to his murder. But the *technologies* of zero-day exploits that pick encryption locks are not designed on a case-by-case basis. The technologies can

⁹⁴ The difference between active and passive surveillance is not as binary as the terms suggest. As discussed in the introduction of this chapter, major telecom companies like AT&T and Verizon have given governments wholesale access to their infrastructure, which some might consider “passive” because it (only) required non-interference.

⁹⁵ Some cyber-mercenaries are former NSA employees (Mazzetti, et al. 2019), others work with NSA tools (like EternalBlue, which was used to build WannaCry) that were hacked and freely distributed online (Perlroth and Sanger, Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool 2017). The focus by the US on cyber-offense built on surveillance tools (Buchanan 2017) has unfortunately produced cyber-defense sabotage (Borges Monroy 2022, Perlroth 2021).

infect devices that are produced in massive quantities and distributed throughout the world. Some zero-day exploits require targeted infections, but newer versions with zero-click capabilities don't. And, as some cyberattacks show, these technologies can also leverage systems' interconnectedness to spread far and wide.

In its quest to undermine encryption, the US has collaborated with the UK to distribute purportedly encrypted phone hardware in the black market that was compromised, allowing both nations to wiretap communications (Zhuang, Peltier and Feuer 2021). This operation was a public admission after years of cybersecurity experts' accusations that the US was intercepting newly purchased laptops in transit and tampering with them to place physical wiretapping equipment inside (Sottek 2013, Gellman 2020). Hardware security sabotage occurs on top of the vast passive data collection at the backbone level of transatlantic fiber optics, in server exchanges, and wireless stations across allies' countries (Radden Keefe 2005).

The backend component drives the point that state surveillance does not exist as a separate infrastructure from market surveillance. Further, it reveals the limits of corporate resistance when such a thing occurs. Governments have no political or economic reason to duplicate their own surveillance efforts when so much data can be accessed by hook or by crook. Deputation is supported by a range of actions: active deregulation of market surveillance, forbearance of actual enforcement of privacy protections, or coercively obtained through secret legal orders or undisclosed technological lockpicks. State surveillance and corporate surveillance intersect through deputation as a governance strategy of data monitoring, producing a surveillance complex that is larger than the sum of its two parts.

Conclusion

Traditional understandings of state surveillance (Foucault 1995, Lyon 2019) as targeted and mobilized retroactively after a crime is committed fall short of explaining current practices. This chapter provides historical and contemporary evidence of how deputized surveillance operates in the United States, but

this governance strategy has been adopted throughout advanced democracies. I began by arguing that the current use of deputation for online surveillance has its roots in the particular state capabilities and political arrangements of the United States after it grew into its role of global military power, as World War II drew to a close and the Cold War ramped up. The chapter focuses on explaining what policies have been implemented and allowed deputized surveillance to flourish, and I detail how the government mobilizes both collaboration and coercion to access market-produced surveillance. I argue for interpreting these policies' continued use and defense as a function of the American government's reliance on market innovation because it deflects economic and political costs to building a redundant surveillance infrastructure. I have argued that this dynamic motivates the creation of a surveillance complex that implicates more than the government's own surveillance of inhabitants⁹⁶ and the market's surveillance of consumers/would-be consumers ("surveillance capitalism" (Zuboff 2019, Bruno 2012)) as separate spheres.

To explain how deputized mass online surveillance works, I discussed how America's distinct legal regime aligned with the country's economic and political needs. But, as I discussed in the dissertation's introduction and this chapter's first section, this governance policy challenges assumptions of democratic governance.

This chapter has focused heavily on the United States' role in incentivizing and institutionalizing a surveillance complex that reaches beyond its borders. A clear understanding of the American institutional context is essential for several reasons. First, its firms monopolize much of the non-US Western market and dominate non-Western technology markets, as Darren Byler argues in his work on Western firms' complicity in the Chinese surveillance of Uyghurs (2022). Foreign governments, particularly military allies, collaborate with American deputized surveillance under

⁹⁶ The issue of non-citizenship and foreign status, including a very low legal bar of "possibly foreign" used in FISA courts, and the nature of mass surveillance techniques, compels me to stay away from describing it as "government surveillance of its citizens".

intelligence agreements such as Five Eyes, Nine Eyes, and Fourteen Eyes⁹⁷. Furthermore, non-American governments are also vulnerable to the cost-avoiding dynamics outlined above in their own data monitoring, making copycats in other democracies likely. The US' moral authority defining what "democracies" do and don't do (including a sociological influence of political science academia) lends credibility to deputized surveillance as an alternative to the type of overt government surveillance that co-constitutes how autocracies are defined. Academic critiques of democratic backsliding and political pressures to unwind policies associated with overt government-exclusive surveillance can be deflected by relying on deputized surveillance. This results in the troubling and understudied globalization of the American-made surveillance complex.

Beyond domestic effects, surveillance has also become a backbone of Western foreign policy decision-making in diplomatic and military intelligence gathering. The Obama administration used surveillance data to fulfill a campaign promise: keeping boots "off the ground" in the Middle East required relying on unmanned drone air strikes (Ackerman, *Reign of Terror* 2021). As human intelligence is removed (Brooks 2016), drone targeting has relied on signal (phone and GPS) surveillance to conduct "signature strikes". That is, drone strikes are being approved on the basis of cellphone location *data* patterns of use, even when positive identification that the intended *people* are using those devices cannot be secured. This means that, for all but the most high-profile extraterritorial assassinations, the US government has retroactively defined that the people holding certain devices

⁹⁷ The history of the UKUSA agreement is explored in Radden Keefe's 2005 book, which included the UK's largest commonwealth nations at the time of WWII, Canada, Australia and New Zealand, which is based on a document that at the time "has never been acknowledged by any of the governments involved" (Radden Keefe 2005, xvii). According to retired Brigadier-General James S. Cox, "Five Eyes sigint [signals intelligence] organizations remain officially responsible and accountable to their own governments, each of which retains the power of 'veto' over national sigint activity" and "Each Five Eyes partner collects information over a specific area of the globe in accordance with their national priorities, but their collection and analysis activities are orchestrated to the point that they essentially act as one" while "[d]uring the Cold War, the agenda and tenor of these meetings were very much set by the US, because of the immense scope of NSA activities and the preeminence of American global responsibilities" (J. S. Cox 2012, 6). The Snowden NSA files corroborated its existence, as well as two other intelligence sharing arrangements with the US: the Nine Eyes brings in Denmark, France, the Netherlands and Norway; the Fourteen Eyes' inclusion of Belgium, Germany, Italy, Spain and Sweden.

were terrorists, given the devices' behaviors (a sort of "being at the wrong place at the wrong time"), extrapolating this conclusion from probabilistic models⁹⁸ (United Nations Special Rapporteur on Counter-Terrorism and Human Rights 2013, Scahill 2013). Clearly, the implications of mass online surveillance in advanced democracies are vast, despite the chronic blindspot in Political Science. This dissertation seeks to undo some of these oversights, but not everything can be addressed. Scrutiny over the global surveillance complex requires centering the discussion on and examining American deputation of mass surveillance to its companies, with a clear view of understanding how this practice allows governments to shirk political and economic costs at home and with their allies.

The US's institutionalization of the surveillance complex doesn't just legitimize copycat versions in democratic and non-democratic regimes. Its market power shapes resilience against foreign pushback. Recurring European lawsuits against the US-EU data sharing agreements were launched after the Snowden revelations made it clear that American technology firms cannot guarantee following new European data protection rules (Schrems 2020, Schrems 2022). Facebook has threatened to leave the European market entirely due to the Safe Harbor and Privacy Shield revocations (Hern 2020). For American Data Goliaths, the economic incentives and political concerns are centered around the threat of American regulation, first and foremost. Closing access to the data

⁹⁸ Drone warfare has been characterized as extrajudicial assassination, (Crockford 2012) relies on mass surveillance, and engages with similar patterns of covert governance, including non-public FISA and military trials (e.g. Guantanamo Bay) and "secret" memos interpreted by the Executive branch and classified by it (Jaffer 2016). Drone warfare has been used outside of Iraq and Afghanistan, where US military forces have not received Congressional authority to engage in offensive action. For example, since 2002 the US authorized over 300 drone strikes in Yemen, more than half of those authorized during the Trump administration (Deutsche Welle 2021, 38:00-38:20, New America 2021). Obama reportedly had a "kill list" he would personally vet before authorizing extrajudicial drone operations. It has not been reported whether this practice was carried out by Trump or Biden, or to what degree drone targets were supervised by other high-rank military officers. A concern is the future use of AI in warfare. The United Nations' Convention on Certain Conventional Weapons debated banning autonomous weapons at the end of 2021 but the Biden administration rejected calls for a binding agreement to halt their use (Associated Foreign Press 2021). The US' public budget for autonomous weapons R&D was US\$18 billion during the Trump administration (Dawes 2021). This is an area of development where the old-fashioned military-industrial complex and deputized surveillance may come to a head.

cookie jar could have disastrous consequences for these firms economically⁹⁹ and politically. Republicans have already threatened anti-trust retaliation over content moderation, some of which follows European mandates. Financial and political incentives are aligned for American data Goliaths to prioritize their home countries' government demands for data. Closing off a market is not without precedent—Google decided to shut down news services in Spain rather than comply with domestic compulsory licensing copyright laws¹⁰⁰. The European response to the growth of deputized American Data Goliaths does not exist in a vacuum. Google has worked on “slowing down and delaying the European Union’s ePrivacy Regulation process, ‘working behind the scenes hand in hand with the other companies’” including Facebook¹⁰¹ and President Obama directly lobbied European leaders to water down GDPR when it was being drafted (2015).

Even other five-eye members’ attempts to hold American Data Goliaths accountable—if only symbolically—have been met with extreme pushback. After the Cambridge Analytica scandal, where users’ data was shared with the Trump campaign without their consent, the UK government held an international parliamentary hearing with eight other countries, requesting the presence of Facebook’s CEO, Mark Zuckerberg. Weeks before, in the US, House and Senate members publicly and privately questioned him. On three separate interparliamentary inquiry sessions, the company only made available lower-tier representatives who could not give knowledgeable answers. This was interpreted in the UK’s official report as a “deliberate strategy of concealment of knowledge and responsibility” (Digital, Culture, Media and Sport Committee of the UK House of Commons 2019, 16). To industry

⁹⁹ For example, 2018 Facebook filings to the Securities and Exchange Commission stated that American and Canadian users were 3 times more valuable to advertisers (priced at \$34.9 USD) than European users, and 10 times more valuable than Asia-Pacific region users (Fisher 2019).

¹⁰⁰ This may have produced a chilling effect on other countries that were considering similar protections to their journalism and publisher industries.

¹⁰¹ Ironically, this lobbying effort was only made public because of an anti-trust lawsuit launched by 12 American states (McCabe 2021).

insiders, it demonstrated “the company’s unwillingness to be accountable to [foreign] government” (Kates 2019)¹⁰².

These trans-Atlantic events hint at the limits of individual user choice and even foreign regulatory pressures. American data Goliaths clearly prioritize American legal incentives and constraints. To the extent that American regulators refuse to create a clear and systematic cost to violating privacy through anti-trust, racketeering, or fraud laws or through direct privacy regulation, foreign pressures to secure non-Americans’ privacy will likely remain a Sisyphean task. As I have argued above, there are few economic and political incentives for the governments in advanced democracies to publicly assume their mass online surveillance system and abolish deputized data collection. This means governments have a conflict of interest that cannot be rectified without public pressures for accountability, raising the stakes for further secrecy of their deputation of companies.

Contemporary observers of the American government¹⁰³, law, history and political science scholars cited here, and a recent European Parliament report echoes Bessner’s interpretation that deputized military and intelligence policies diminish public accountability. Deputized surveillance’s “gangrenous” technologies’ impact “reverberates on its own constituent governments’ democratic health and peoples’ freedom” (European Parliament, Sophia Helena in 't Veld 2022).

These efforts negatively impact the public’s ability to become informed, reflect their values back onto elected officials, and erodes the quality of democratic life itself, of its own right and in the effects surveillance produces on how it governs its people. In this chapter, I have documented the US

¹⁰² Emily Rosenberg argues that American Big Tech is actually a consequence of American empire, built through “Americanized consumerism” that is “closely tied to symbolic modernization via mass-production and mass-marketing. As American production declines, the advertising industry, underpinned by mass ad tracking technologies, becomes the largest American export (2014).

¹⁰³ State Department section chief for Internet freedom Bureau of Democracy, Human Rights and Labor under Secretary Clinton, John Napier Tye has commented that as a direct result of a draft speech, in response to the Snowden revelations, when he penned that “if U.S. citizens disagree with congressional and executive branch determinations about the proper scope of signals intelligence activities, they have the opportunity to change the policy through our democratic process” he was directed by White House council to remove it because it was untrue, even after reforms were announced by former President Barak Obama (Napier Tye 2014).

government's actions, across time, between many different administrations, and across branches of government, arguing that this institutionalization of surveillance has attempted to produce low public scrutiny over mass online surveillance policies. This impetus reproduces itself across time because it meets few obstacles, in the form of democratic accountability or budgetary accounting, by voters or by interbranch competition. The public's knowledge of the surveillance complex, and its opinion, has been formed *despite*, not because of governments, and deputized corporations. When journalists, activists, researchers and whistleblowers have been able to shine a light to these obscured practices, surveillance complex actors have attempted to further obfuscate, gaslight, misdirect or reframe the least amount of information as possible, to return to a status quo. In the remaining dissertation chapters, I pivot towards analyzing the state of American and European Union public opinion on a range of practices ensconced in the surveillance complex.

Bibliography

- Abramson, Larry. 2013. "FISA Court: We Approve 99 Percent Of Wiretap Applications." *National Public Radio*, October 15. Accessed April 17, 2023. <https://www.npr.org/sections/thetwo-way/2013/10/15/234840282/fisa-court-we-approve-99-percent-of-wiretap-applications>.
- Ackerman, Spencer. 2021. *Reign of Terror: How the 9/11 Era Destabilized America and Produced Trump*. New York: Penguin Publishing Group.
- . 2015. "Homan Square revealed: how Chicago police 'disappeared' 7,000 people." *The Guardian*, October 19. <https://www.theguardian.com/us-news/2015/oct/19/homan-square-chicago-police-disappeared-thousands>.
- Acquisti, Alessandro, and Jens Grossklags. 2007. "What Can Behavioral Economics Teach Us about Privacy?" In *Digital Privacy: Theory, Technologies, and Practices*, edited by Alessandro Acquisti, Stefanos Gritzalis' Costos Lambrinoudakis and Sabrina di Vimercati, 363-377. New York.
- Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. 2015. "Privacy and human behavior in the age of information." *Science* 347 (6221): 509-514.
- American Civil Liberties Union. 2018. *Background on the State Secrets Privilege*. Accessed March 26, 2023. <https://www.aclu.org/other/background-state-secrets-privilege>.
- . 2013. *Documents Confirm How the NSA's Surveillance Procedures Threaten Americans' Privacy*. Accessed March 25, 2023. <https://www.aclu.org/fact-sheet/documents-confirm-how-nsas-surveillance-procedures-threaten-americans-privacy>.
- American Civil Liberties Union. 2022. *Surveillance Under the USA PATRIOT Act*. New York City: American Civil Liberties Union. <https://www.aclu.org/other/surveillance-under-usapatriot-act>.
- American Civil Liberties Union. 2008. "Talking Points on the FISA Amendments Act of 2008." <https://www.aclu.org/other/talking-points-fisa-amendments-act-2008>.
- Angwin, Julia, Charlie Savage, Jeff Larson, Henrik Moltke, Laura Poitras, and Risen James. 2015. "AT&T Helped U.S. Spy on Internet on a Vast Scale." *The New York Times*, August 15: A1. Accessed April 02, 2019. <https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html?smid=tw-nytimes&smtyp=cur>.
- Angwin, Julia, Terry Parris Jr., and Surya Mattu. 2016. "Facebook is quietly buying information from data brokers about its users' offline lives." December 30. Accessed December 2017. <http://www.businessinsider.com/facebook-data-brokers-2016-12>.
- Anonymous. 2022. *Active Agency Map*. April 1. Accessed April 7, 2022. <https://www.google.com/maps/d/u/0/viewer?mid=1eYVDPh5itXq5acDT9b0BVeQwmESBa4cB&ll=42.895241166788324%2C-82.87607876449249&z=4>.
- Associated Foreign Press. 2021. "US rejects calls for regulating or banning 'killer robots'." *The Guardian*, December 2. Accessed April 16, 2022. <https://www.theguardian.com/us-news/2021/dec/02/us-rejects-calls-regulating-banning-killer-robots>.
- Astor, Maggie. 2019. "How the Politically Unthinkable Can Become Mainstream." *The New York Times*, February 26: Section A, Page 18. Accessed March 27, 2023. <https://www.nytimes.com/2019/02/26/us/politics/overton-window-democrats.html>.
- Auerbach, Dan, and Eva Galperin. 2013. *Google Transparency Report Highlights Just How Much We Don't Know About National Security Letters*. March/June update 06/07. Accessed March 27, 2023. <https://www.eff.org/deeplinks/2013/03/new-statistics-about-national-security-letters-google-transparency-report>.
- Babazadeh, Natasha. 2018. "Concealing Evidence: 'Parallel Construction,' Federal Investigations, and the Constitution." *Virginia Journal of Law and Technology*, February 19: 60. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3319387.

- Barrett, Devlin. 2020. "Surveillance program that gathered Americans' phone data was illegal, court finds." *The Washington Post*, September 04. Accessed March 25, 2023. https://www.washingtonpost.com/national-security/phone-records-surveillance-edward-snowden/2020/09/02/97f26498-ed67-11ea-99a1-71343d03bc29_story.html.
- Bessner, Daniel. 2018. *Democracy in exile: Hans Speier and the rise of the defense intellectual*. Ithaca: Cornell University Press.
- Bhuiyan, Johana. 2022. "How can US law enforcement agencies access your data? Let's count the ways." *The Guardian*, April 4. Accessed April 13, 2022. <https://www.theguardian.com/technology/2022/apr/04/us-law-enforcement-agencies-access-your-data-apple-meta>.
- Bloom, Peter. 2019. *Monitored: Business and Surveillance in a Time of Big Data*. London: Pluto Press.
- Bond, Shannon, and Bobby Allyn. 2020. *48 AGs, FTC Sue Facebook, Alleging Illegal Power Grabs To 'Neutralize' Rivals*. December 9. Accessed November 30, 2022. <https://www.npr.org/2020/12/09/944073889/48-attorneys-general-sue-facebook-alleging-illegal-power-grabs-to-neutralize-riv>.
- Borges Monroy, Isadora. 2022. "Cyber(in)security: Throwing bits in glass houses." *Digital Issues Discussion Group*. Virtual Meeting. 25.
- Bradford Franklin, Sharon. 2019. *Fulfilling the Promise of the USA Freedom Act: Time to Truly End Bulk Collection of Americans' Calling Records*. March 28. Accessed March 25, 2023. <https://www.justsecurity.org/63399/fulfilling-the-promise-of-the-usa-freedom-act-time-to-truly-end-bulk-collection-of-americans-calling-records/>.
- Brewster, Thomas. 2015. "Obama's Attempts To Rein In NSA 'An Insult' To 96 Per Cent Of World's Population." *Forbes*, February 04. Accessed March 25, 2023. <https://www.forbes.com/sites/thomasbrewster/2015/02/04/obama-allows-for-more-spying-on-foreigners/>.
- British Broadcasting Corporation. 2021. *JBS: Cyber-attack hits world's largest meat supplier*. June 02. Accessed September 20, 2021. <https://www.bbc.com/news/world-us-canada-57318965>.
- Brooks, Rosa. 2016. *How Everything Became War and the Military Became Everything: Tales from the Pentagon*. New York: Simon & Schuster.
- Brown, Christopher. 2022. "Apple Hit With Class Action Over Tracking of Mobile App Activity." *Bloomberg Law*, November 11. <https://news.bloomberglaw.com/litigation/apple-hit-with-class-action-over-tracking-of-mobile-app-activity>.
- Bruno, Fernanda. 2012. "Surveillance and participation on Web 2.0." In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin D. Haggerty and David Lyon, 343-359.
- Bryan, Kristin, Shea Leitch, Glenn A. Brown, Ericka Johnson, and James Brennan. 2023. *Divided SEC Proposes Slew of Cybersecurity Regulations for Securities Market Entities*. March 24. Accessed March 27, 2023. <https://www.privacyworld.blog/2023/03/divided-sec-proposes-slew-of-cybersecurity-regulations-for-securities-market-entities/>.
- Buchanan, Ben. 2017. "Nobody But Us: The Rise and Fall of the Golden Age of Signals Intelligence." *National Security, Technology, and Law*, September 07, Aegis Series Paper No. 1708 ed.: 1-32.
- Bump, Philip. 2017. "Americans united after 9/11. When did we rip back apart?" *The Washington Post*, September 11. Accessed March 26, 2023. <https://www.washingtonpost.com/news/politics/wp/2017/09/11/americans-united-after-911-when-did-we-rip-back-apart/>.
- Byler, Darren. 2022. *In the camps: China's high-tech penal colony*. Durham: Duke University Press.
- Cagle, Matt, and Nicole Ozer. 2019. *Amazon Teams Up With Government to Deploy Dangerous New Facial Recognition Technology*. Digital, New York: American Civil Liberties Union. Accessed October

- 01, 2109. <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-teams-government-deploy-dangerous-new>.
- Cappell, Bill. 2021. "The Pentagon has never passed an audit. Some Senators want to change that." *NPR*, May 19. Accessed April 2, 2022. <https://www.npr.org/2021/05/19/997961646/the-pentagon-has-never-passed-an-audit-some-senators-want-to-change-that>.
- Cappello, Lawrence. 2017. "Big Iron and the Small Government: On the History of Data Collection and Privacy in the United States." *Journal of Policy History* 29 (01): 177-196.
- CBS News Chicago. 2014. "Activists Say Chicago Police Used 'Stingray' Eavesdropping Technology During Protests." *CBS News*, December 06. Accessed November 30, 2022. <https://www.cbsnews.com/chicago/news/activists-say-chicago-police-used-stingray-eavesdropping-technology-during-protests/>.
- Childress, Sarah. 2015. "How the NSA Spying Programs Have Changed Since Snowden." *PBS Frontline*, February 09. Accessed March 25, 2023. <https://www.pbs.org/wgbh/frontline/article/how-the-nsa-spying-programs-have-changed-since-snowden/>.
- Citron, Danielle Keats, and David C. Gray. 2013. "Addressing the Harm of Total Surveillance: a Reply to Professor Neil Richards." *Harvard Law Review* 262-274.
- Clarke, Richard A. 2004. *Against All Enemies: Inside America's War on Terror*. New York: Free Press.
- Clearview A.I. 2021. *Capitol Riots*. Accessed March 25, 2023. <https://www.clearview.ai/capitol-riots>.
- Colaresi, Michael. 2014. *Democracy Declassified: The Secrecy Dilemma in National Security*. New York City: Oxford University Press.
- Cox, James S. 2012. *Canada and the Five Eyes Intelligence Community*. Strategic Studies Working Group Papers, Canadian Defence & Foreign Affairs Institute & Canadian International Council.
- Cox, Joseph. 2019. 'They Would Go Absolutely Nuts': How a Mark Cuban-Backed Facial Recognition Firm Tried to Work With Cops. May 06. Accessed May 07, 2019. https://www.vice.com/en_ca/article/xwny7d/mark-cuban-facial-recognition-suspect-technologies.
- Coyne, Christopher J., and Abigail R. Hall. 2018. *Tyranny comes Home: The domestic fate of US Militarism*. Stanford: Stanford University Press.
- Crocker, Andrew. 2015. *EFF Case Analysis: Appeals Court Rules NSA Phone Records Dragnet is Illegal*. May 09. Accessed March 25, 2023. <https://www.eff.org/deeplinks/2015/05/eff-case-analysis-appeals-court-rules-nsa-phone-records-dragnet-illegal>.
- Crocker, Andrew, and Cindy Cohn. 2015. *Don't Worry, the Government Still Has Plenty of Surveillance Power If Section 215 Sunsets*. May 31. Accessed March 26, 2023. <https://www.eff.org/deeplinks/2015/05/dont-worry-government-still-has-plenty-surveillance-power-if-section-215-sunsets>.
- Crockford, Kade. 2012. *Is the Obama administration's drone war legal? Why should we be concerned?* December 04. Accessed April 14, 2022. <https://www.aclu.org/blog/national-security/targeted-killing/obama-administrations-drone-war-legal-why-should-we-be>.
- Crosby, Andrew, and Jeffrey Monaghan. 2018. *Policing Indigenous Movements: Dissent and the Security State*. Black Point: Fernwood Press.
- Cullen, Catherine, and Peter Zimonjic. 2017. *RCMP, CSIS launch investigations into phone spying on Parliament Hill after CBC story*. April 05. Accessed February 25, 2019. <https://www.cbc.ca/news/politics/goodale-spying-investigation-phone-1.4055107>.
- Cushing, Tim. 2015. *FBI Says It Has No Idea Why Law Enforcement Agencies Are Following The Terms Of Its Stingray Non-Disclosure Agreements*. May 18. Accessed September 20, 2021. <https://www.techdirt.com/articles/20150515/08573531016/fbi-says-it-has-no-idea-why-law-enforcement-agencies-are-following-terms-stingray-non-disclosure-agreements.shtml>.

- . 2018. *New Documents Show FBI Instructing Law Enforcement To Throw Out Cases Rather Than Give Up Info On Stingray Use*. April 8. Accessed September 20, 2021. <https://www.techdirt.com/articles/20150408/10242230590/new-documents-show-fbi-instructing-law-enforcement-to-throw-out-cases-rather-than-give-up-info-stingray-use.shtml>.
- . 2016. *Stingray Memo From FBI To Oklahoma Law Enforcement Tells PD To Engage In Parallel Construction*. May 09. Accessed September 20, 2021. <https://www.techdirt.com/articles/20160507/10052134369/stingray-memo-fbi-to-oklahoma-law-enforcement-tells-pd-to-engage-parallel-construction.shtml>.
- Cybersecurity and Infrastructure Security Agency. 2020. *Critical Infrastructure Sectors*. October 21. Accessed September 20, 2021.
- Cybersecurity for Democracy. 2021. *Researchers' audit reveals flaws in Facebook's identification of political ads*. December 09. Accessed April 16, 2022. <https://medium.com/cybersecurity-for-democracy/researchers-audit-reveals-flaws-in-facebook-s-identification-of-political-ads-81e2015a451a>.
- Dawes, James. 2021. *UN fails to agree on 'killer robot' ban as nations pour billions into autonomous weapons research*. December 20. Accessed April 16, 2022. <https://theconversation.com/un-fails-to-agree-on-killer-robot-ban-as-nations-pour-billions-into-autonomous-weapons-research-173616>.
- de Arimatéia da Cruz, José, and Stephanie Pedron. 2020. "Cyber Mercenaries: A New Threat to National Security." *International Social Science Review* 96 (2): 35. <https://digitalcommons.northgeorgia.edu/cgi/viewcontent.cgi?article=1454&context=issr>.
- DelBene, Suzan. 2018. *ENCRYPT Act Would Block States From Seeking Crypto Backdoors*. June 07. Accessed February 19, 2019. ENCRYPT Act Would Block States From Seeking Crypto Backdoors.
- Delhey, Jan, Kenneth Newton, and Christian Welzel. 2011. "How General Is Trust in "Most People"? Solving the Radius of Trust Problem." *American Sociological Review* 76: 786-807. doi:10.1177/0003122411420817.
- Dempsey, James. 2023. "Cybersecurity Enforcement: If Government Regulation Is Going to Increase, How Will It Be Enforced?" *Cyber Policy Center Winter Seminar Series*. Program on Democracy and the Internet at Stanford's Cyber Policy Center. 36.
- DeSombre, Winnona, Lars Gjesvik, and Johann Ole Willers. 2021. *Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets*. Washington D.C.: The Atlantic Council. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/>.
- Deutsche Welle. 2019. "Court orders Germany to question US drone strikes." *Deutsche Welle*, March 19. Accessed April 16, 2022. <https://www.dw.com/en/court-orders-germany-to-question-us-drone-strikes/a-47979480>.
2021. *Drones, Hackers and Mercenaries: The Future of War*. Performed by Deutsche Welle. <https://www.youtube.com/watch?v=TmlBkW6ANsQ>.
- Dewey, Matías, and Donato Di Carlo. 2021. "Governing through non-enforcement: Regulatory forbearance as industrial policy in advanced economies." *Regulation & Governance* 16 (3): 930-950. doi:10.1111/rego.12382.
- Dhir, Amandeep, Torbjørn Torsheim, Ståle Pallesen, and Cecilie S. Andreassen. 2017. "Do Online Privacy Concerns Predict Selfie Behavior among Adolescents, Young Adults and Adults?" *Frontiers in Psychology* (8): 815. Accessed October 02, 2019. doi:10.3389/fpsyg.2017.00815.
- DHS. 2021. *Department of Homeland Security Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators*. July 20. Accessed September 20, 2021.

- <https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators>.
- Diamond, Larry. 2015. "Facing up to the Democratic Recession." *Journal of Democracy* 26 (1): 141-155.
- DiBella, Sam. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* – Book Review. November 10. Accessed March 12, 2022. <https://blogs.lse.ac.uk/businessreview/2019/11/10/the-age-of-surveillance-capitalism-the-fight-for-a-human-future-at-the-new-frontier-of-power-book-review/>.
- Digital, Culture, Media and Sport Committee of the UK House of Commons. 2019. *Disinformation and 'fake news': Final Report*. Governmental report, London: UK Parliament, 111. <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf>.
- Director of National Intelligence. 2022. *Section 702 Overview*. Power Point presentation, United States Government, Washington D.C.: Director of National Intelligence. <https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf>.
- Doctorow, Cory. 2013. "How to foil NSA sabotage: use a dead man's switch." *The Guardian*, September 09. Accessed April 13, 2022. <https://www.theguardian.com/technology/2013/sep/09/nsa-sabotage-dead-mans-switch>.
- DoJ. 2021. *Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside*. June 07. Accessed September 20, 2021. <https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>.
- Eddy, Melissa. 2022. "Right to Privacy Extends to Foreign Internet Users, German Court Rules." *The New York Times*, May 19: Section A, Page 17. Accessed April 16, 2022. <https://www.nytimes.com/2020/05/19/world/europe/germany-privacy.html>.
- Edelson, Laura, and Damon McCoy. 2021. "We Research Misinformation on Facebook. It Just Disabled Our Accounts." *The New York Times*, August 10: Section A, Page 17. Accessed April 16, 2022.
1961. *Presidential Farewell Address*. Performed by Dwight Eisenhower. <https://www.archives.gov/milestone-documents/president-dwight-d-eisenhowers-farewell-address>.
- Electronic Privacy Information Center. 2003. *The Privacy Act of 1974*. Washington, D.C.: EPIC. Accessed March 27, 2023. <https://epic.org/the-privacy-act-of-1974/>.
- European Parliament, Sophia Helena in 't Veld . 2022. "Draft Report Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance ." European Parliament, Brussels. [https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA\(2022\)732268_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf).
- Feathers, Todd, Simon Fondrie-Teitler, Angie Waller, and Surya Mattu. 2022. *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*. June 16. Accessed June 20, 2022. <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>.
- Federal Trade Commission. 2017. *Taking Charge: What to do if your identity is stolen*. Washington, D.C.: United States Government. Accessed March 27, 2023. <https://www.justice.gov/usao-wdmi/file/764151/download>.
- Federman, Adam. 2019. "Revealed: how the FBI targeted environmental activists in domestic terror investigations." *The Guardian*. Accessed September 20, 2021. <https://www.theguardian.com/us-news/2019/sep/23/revealed-how-the-fbi-targeted-environmental-activists-in-domestic-terror-investigations>.

- Feiner, Lauren, and Salvador Rodriguez. 2019. "FTC slaps Facebook with record \$5 billion fine, orders privacy oversight." *CNBC*, July 24: <https://www.cnbc.com/2019/07/24/facebook-to-pay-5-billion-for-privacy-lapses-ftc-announces.html>.
- Financial Crimes Enforcement Networks. 2004. "Ten of the Most Common Questions about the Final CIP Rule." Public guidance. <https://www.fincen.gov/sites/default/files/guidance/finalciprule.pdf>.
- Fisher, Sara. 2019. *Facebook users in the U.S. and Canada are the most valuable*. February 22. Accessed February 22, 2019. <https://www.axios.com/facebook-users-valuable-united-states-europe-c7ee74ad-8012-400f-a142-fe110dd6b6af.html>.
- Flaherty, David H. 1989. *Protecting privacy in surveillance societies: the Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill: The University of North Carolina Press.
- Foucault, Michel. 1995. *Discipline and Punish: The Birth of the Prison*. Second Edition. Translated by Alan Sheridan. New York: Vintage Books, Random House.
- Franz, Vera , and Malte Spitz. 2020. *Q&A: A Big Step for Global Privacy Rights*. July 20. Accessed April 16, 2022. <https://www.opensocietyfoundations.org/voices/q-and-a-a-big-step-for-global-privacy-rights>.
- Freeman, Joshua Benjamin. 2018. *Behemoth: a history of the factory and the making of the modern world*. New York: W.W. Norton & Company, Inc.
- Gasser, Urs, Jack Goldsmith, Susan Landau, Joseph Nye, Bruce Schneier, and Jonathan Zittrain. 2016. *Don't Panic: Making Progress on the "Going Dark" Debate*. Boston: Berkman Center for Internet & Society at Harvard University.
- Gellman, Barton. 2020. *Dark mirror: Edward Snowden and the American surveillance state*. New York: Penguin Random House.
- Gellman, Barton, and Greg Miller. 2013. "'Black budget' summary details U.S. spy network's successes, failures and objectives." *The Washington Post*, August 13. http://webcache.googleusercontent.com/search?q=cache:https%3A%2F%2Fwww.washingtonpost.com%2Fworld%2Fnational-security%2Fblack-budget-summary-details-us-spy-networks-successes-failures-and-objectives%2F2013%2F08%2F29%2F7e57bb78-10ab-11e3-8cdd-bcdc09410972_.
- Gilens, Martin, and Benjamin I. Page. 2014. "Testing Theories of American Politics: Elites, Interest Groups, and Average Citizens." *Perspectives on Politics* 12 (3): 564-581. doi:doi:10.1017/S1537592714001595.
- Google. 2014. *HTTPS as a ranking signal*. August 07. Accessed December 3, 2022. <https://developers.google.com/search/blog/2014/08/https-as-ranking-signal>.
- Gorman, Siobhan. 2017. "The Snowden Effect on the NSA and Reporting." In *Journalism After Snowden: The future of the free press in the surveillance state*, 199. New York: Columbia University Press.
- Grant, Nico, and Josh Eidelson. 2022. *Two of Google's Ethical AI Staffers Leave to Join Ousted Colleague's Institute*. February 02. Accessed April 10, 2022. <https://www.bloomberg.com/news/articles/2022-02-02/google-loses-two-ethical-ai-staffers-to-timnit-gebru-s-institute>.
- Greenberg, Andy. 2019. *Hacker Eva Galperin Has a Plan to Eradicate Stalkerware*. April 04. Accessed May 27, 2019. <https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/>.
- Greenwald, Glenn, and Spencer Ackerman. 2013. "NSA collected US email records in bulk for more than two years under Obama." *The Guardian*, June 27. Accessed February 25, 2019. <https://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama>.
- Han, Catherine, Irwin Reyes, Álvaro Feal, Joel Reardon, Primal Wijesekera, Narseo Vallina-Rodriguez, Amit Elazari, Kenneth A. Bamberger, and Serge Egelman. 2020. "The Price is (Not) Right:

- Comparing Privacy in Free and Paid Apps." *Proceedings on Privacy Enhancing Technologies* 3: 222-242.
- Hann, Il-Horn, Kai-Lung Hui, Sang-Yong Tom Lee, and Ivan P. L. Png. 2014. "Overcoming Online Information Privacy Concerns An Information Processing Theory Approach." *Journal of Management Information Systems* 24 (2): 13-42. doi:10.2753/MIS0742-1222240202.
- Harper, Lauren. 2014. "Reagan-era EO 12333 Comes Under Scrutiny, Authors of 9/11 Commission Report Call for More IC Transparency, and Much More: FRINFORMSUM 7/24/2014." *Unredacted*, July 24. <https://unredacted.com/2014/07/24/secret-reagan-era-eo-12333-comes-under-scrutiny-authors-of-911-commission-report-call-for-more-ic-transparency-and-much-more-frinformsum-7242014/>.
- Harris, Shane. 2013. "Making you Comfortable with Spying is Obamas Big NSA Fix." *Foreign Policy*, August 09: Passport. Accessed May 23, 2019. <https://foreignpolicy.com/2013/08/09/making-you-comfortable-with-spying-is-obamas-big-nsa-fix/>.
- Henderson, Greg. 2013. *Obama To Leno: 'There Is No Spying On Americans'*. August 07. Accessed March 25, 2023. <https://www.npr.org/sections/thetwo-way/2013/08/06/209692380/obama-to-leno-there-is-no-spying-on-americans>.
- Hern, Alex. 2020. "Facebook says it may quit Europe over ban on sharing data with US." *The Guardian*, September 22. Accessed March 13, 2022. <https://www.theguardian.com/technology/2020/sep/22/facebook-says-it-may-quit-europe-over-ban-on-sharing-data-with-us>.
- Hertsgaard, Mark. 2016. "How the Pentagon punished NSA whistleblowers." *The Guardian*, May 22. Accessed March 13, 2023. <https://www.theguardian.com/us-news/2016/may/22/how-pentagon-punished-nsa-whistleblowers>.
- Hill, Kashmir. 2021. "Democrats Demand Answers From Justice Dept. About Trump's Role as Impeachment Threat Looms." *The New York Times*, February 9. Accessed March 27, 2023. <https://www.nytimes.com/live/2021/01/09/us/trump-biden#facial-recognition-clearview-capitol>.
- . 2022. "Facial Recognition Goes to War." *The New York Times*, April 07: Section B, Page 1. <https://www.nytimes.com/2022/04/07/technology/facial-recognition-ukraine-clearview.html>.
- Hogan, Michael. 1998. *Iron Cross: Harry S. Truman and the Origins of the National Security State, 1945–1954*. Cambridge: Cambridge University Press. doi:10.1017/CBO9780511664984.
- Holmes, Aaron. 2020. *Police are tapping into residents' Ring doorbells and home security cameras to stream 24/7 live video*. November. Accessed April 7, 2022. <https://www.businessinsider.com/ring-doorbells-live-video-security-camera-police-fusus-2020-11>.
- Horton, Alex, and Aaron Gregg. 2020. "Use of military contractors shrouds true costs of war. Washington wants it that way, study says." *The Washington Post*, June 30. <https://webcache.googleusercontent.com/search?q=cache:https%3A%2F%2Fwww.washingtonpost.com%2Fnational-security%2F2020%2F06%2F30%2Fmilitary-contractor-study%2F>.
- Huddy, Leonie, Stanley Feldman, Charles Taber, and Gallya Lahav. 2005. "Threat, Anxiety, and Support of Antiterrorism Policies." *American journal of Political Science* 49 (3): 593-608.
- Human Rights Watch. 2019. *Dark Side: Secret Origins of Evidence in US Criminal Cases*. Non-governmental organization, New York: Human Rights Watch. Accessed February 26, 2019. doi:ISBN: 978-1-6231-35645.
- Igo, Sarah E. 2018. "Defining Privacy—and Then Getting Rid of It." *Laphams Quarterly*, May 15. <https://www.laphamsquarterly.org/roundtable/defining-privacy-and-then-getting-rid-it>.

- Igo, Sarah E. 2018. "Social Insecurities: Private Data and Public Culture in Modern America." In *Shaped by the State: Toward a New Political History of the Twentieth Century*, edited by Brent Cebul, Lily Geismer and Mason B. Williams, 27-61. Chicago: University of Chicago Press.
- Jaffer, Jameel. 2016. *The Drone Memos: targeted killing, secrecy, and the law*. New York: The New Press.
- Jarvis, Craig. 2021. *Crypto Wars: The Fight for Privacy in the Digital Age, A Political History of Digital Encryption*. CRC Press.
- Johnson, Loch K. 2017. *Spy Watching: Intelligence Accountability in the United States*. New York: Oxford University Press.
- Jones, Ben. 2008. *Canadian MP: Three Strikes Law is Idiotic*. July 06. Accessed March 25, 2023. <https://torrentfreak.com/canadian-mp-three-strikes-law-is-idiotic-080706/>.
- Jones, Meg Leta. 2018. *Ctrl + Z*. New York: New York University Press.
- Kates, Graham. 2019. Facebook "misled" Parliament on data misuse, U.K. committee says. February 18. Accessed February 22, 2019. <https://www.cbsnews.com/news/facebook-misled-parliament-on-data-misuse-u-k-committee-says/>.
- Kerr, Ian, and Jennifer Barrigar. 2012. "Privacy, Identity and Anonymity." In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin Haggerty and David Lyon, 386-394. Abingdon, Oxon: Routledge.
- Klimburg, Alexander. 2017. *The Darkening Web: The war for cyberspace*. New York: Penguin Press.
- Klosowski, Thorin. 2021. "The State of Consumer Data Privacy Laws in the US (And Why It Matters)." *The New York Times*, September 06. Accessed March 27, 2023. <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/>.
- Kroll, Andy. 2021. "FBI Document Says the Feds Can Get Your WhatsApp Data — in Real Time." *Rolling Stone*, November 29. Accessed January 15, 2022. <https://www.rollingstone.com/politics/politics-features/whatsapp-imessage-facebook-apple-fbi-privacy-1261816/>.
- Kwet, Michael. 2019. "In Stores, Secret Surveillance Tracks Your Every Move." *The New York Times*, June 14. <https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html>.
- Lessig, Lawrence. 2008. *Remix: making art and commerce thrive in the hybrid economy*. New York: Penguin Press.
- Levy, Steven. 2002. *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*. Penguin Books.
- Lieber, Ron. 2018. "Marriott Hack Adds Passport Headache, but Its Intensity Is in Dispute." *The New York Times*, December 03: Section B, Page 1. Accessed March 27, 2023. <https://www.nytimes.com/2018/12/03/your-money/marriott-hack-passports.html>.
- Lynch, Jennifer. 2021. *In 2021, the Police Took a Page Out of the NSA's Playbook: 2021 in Review*. December 31. Accessed March 13, 2022. <https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html?mtrref=undefined&assetType=PAYWALL&mtrref=www.nytimes.com&assetType=PAYWALL>.
- Lyon, David. 2019. *State and Surveillance*. August. Accessed March 03, 2022. <https://www.cigionline.org/articles/state-and-surveillance/>.
- . 2007. *Surveillance Studies: An Overview*. Cambridge: Polity Press.
- MacLean, Nancy. 2017. *Democracy in chains: the deep history of the radical right's stealth plan for America*. New York City: Viking.
- Martin, Brian. 2007. "Opposing surveillance." Edited by Katina Michael and Michael M. G. *From dataveillance to überveillance and the realpolitik of the transparent society: the second workshop on the social implications of national security*. Wollongong: University of Wollongong. 71-82.

- Marwick, Alice, Claire Fontaine, and danah boyd. 2017. "Nobody Sees It, Nobody Gets Mad"—Social Media, Privacy, and Personal Responsibility Among Low-SES Youth." *Social Media + Society* 1-14.
- Masco, Joseph. 2014. *The Theater of Operations*. Duke University Press.
- Masnick, Mike. 2020. *Major Publishers Sue The Internet Archive's Digital Library Program In The Midst Of A Pandemic*. June 04. Accessed March 25, 2023. <https://www.techdirt.com/2020/06/04/major-publishers-sue-internet-archives-digital-library-program-midst-pandemic/>.
- . 2014. *Parallel Construction Revealed: How The DEA Is Trained To Launder Classified Surveillance Info*. February 03. Accessed September 20, 2021. <https://www.techdirt.com/articles/20140203/11143926078/parallel-construction-revealed-how-dea-is-trained-to-launder-classified-surveillance-info.shtml>.
- Matsakis, Louise. 2018. *How the Government Hides Secret Surveillance*. January 09. Accessed February 25, 2019. <https://www.wired.com/story/stingray-secret-surveillance-programs/>.
- Maxwell, Andy. 2011. *Judge Decimates BitTorrent Lawsuit With Common Sense Ruling*. September 7. Accessed March 25, 2023. <https://torrentfreak.com/judge-decimates-bittorrent-lawsuit-with-common-sense-ruling-110907/>.
- Mazzetti, Mark, Adam Goldman, Ronen Bergman, and Nicole Perlroth. 2019. "A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments." *The New York Times*, March 21: A1. Accessed March 24, 2019. <https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html>.
- McCabe, David. 2021. "Google said it had successfully 'slowed down' European privacy rules, according to lawsuit." *The New York Times*, October 22. <https://www.nytimes.com/2021/10/22/technology/google-privacy-lawsuit.html>.
- McCahill, Michael. 2012. "Security, surveillance and democracy." In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin Haggerty and David Lyon, 244-250. Abingdon, Oxon: Routledge.
- McFate, Seth. 2019. *Mercenaries and War: understanding Private Armies Today*. Washington DC: National Defense University.
- McKinney, India. 2020. *Section 215 Expired: Year in Review 2020*. December 29. Accessed March 26, 2023. <https://www.eff.org/deeplinks/2020/12/section-215-expired-year-review-2020>.
- . 2019. *The FISA Oversight Hearing Confirmed That Things Need to Change*. September 27. Accessed March 25, 2023. <https://www.eff.org/deeplinks/2019/09/fisa-oversight-hearing-confirmed-things-need-change>.
- Meditology Services. 2022. *Hospitals Sharing PHI with Facebook: HIPAA Analysis & Recommendations*. June 28. Accessed December 3, 2022. <https://www.meditologyservices.com/hospitals-sharing-phi-with-facebook-hipaa-analysis-recommendations/>.
- Molinaro, Dennis G., ed. 2021. *The bridge in the parks: the Five Eyes and Cold War counter-intelligence*. Toronto: University of Toronto Press.
- Morrison, Sara. 2020. *A surprising number of government agencies buy cellphone location data. Lawmakers want to know why*. December 02. Accessed September 20, 2021. <https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel>.
- Nakashima, Ryan. 2018. "Google tracks your movements, like it or not." *Associated Press*, August 13. <https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb>.
- Napier Tye, John. 2014. "Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans." *The Washington Post*, July 18. Accessed November 25, 2022.

- https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.
- National Science Foundation. 1987. *Combined Maximum Likelihood Decoding for Coded Partial Response Channels Award Abstract*. Washington D.C.: United States government. https://nsf.gov/awardsearch/showAward?AWD_ID=8660104.
- National Science Foundation. 1994. *The Stanford Integrated Digital Library Project Award Abstract*. Washington D.C.: United States government. https://www.nsf.gov/awardsearch/showAward?AWD_ID=9411306.
- Nesbit, Jeff. 2017. *Google's true origin partly lies in CIA and NSA research grants for mass surveillance*. December 08. Accessed March 17, 2020. <https://qz.com/1145669/googles-true-origin-partly-lies-in-cia-and-nsa-research-grants-for-mass-surveillance/>.
- New America. 2019. *The FTC is Currently the Primary Privacy Enforcer but its Authority is Limited*. Washington, DC: New America. Accessed March 26, 2023. <https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/the-ftc-is-currently-the-primary-privacy-enforcer-but-its-authority-is-limited/>.
- . 2021. *The War in Yemen*. November 15. Accessed April 16, 2022. <https://www.newamerica.org/international-security/reports/americas-counterterrorism-wars/the-war-in-yemen/>.
- Newcomb, Alyssa. 2018. *A timeline of Facebook's privacy issues — and its responses*. March 24. Accessed January 13, 2022. <https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651>.
- Ng, Alfred, and Maddy Varner. 2021. *The Little-Known Data Broker Industry Is Spending Big Bucks Lobbying Congress*. April 1. Accessed December 2, 2022. <https://themarkup.org/privacy/2021/04/01/the-little-known-data-broker-industry-is-spending-big-bucks-lobbying-congress>.
- Obama, Barack. 2015. *Here's the deal: The text of the Trans-Pacific Partnership*. November 05. Accessed April 04, 2019. <https://medium.com/@potus44/here-s-the-deal-the-text-of-the-trans-pacific-partnership-103adc324500#.buf03ktt8>.
- Obama, Barack, interview by Kara Swisher. 2015. *White House. Red Chair. Obama Meets Swisher*. (February 15). Accessed December 1, 2022. <https://webcache.googleusercontent.com/search?q=cache:http%3A%2F%2Ffrecode.net%2F2015%2F02%2F15%2Fwhite-house-red-chair-obama-meets-swisher%2F>.
- O'Donovan, Caroline. 2022. "Amazon Care is dead, but the tech giant's health-care ambitions live on." *The Washington Post*, September 4. Accessed November 30, 2022. <https://www.washingtonpost.com/technology/2022/09/04/amazon-care-health-one-medical/>.
- Oppel Jr., Richard A. 2013. "Taping of Farm Cruelty Is Becoming the Crime." *The New York Times*, April 06: Section A Page 1. <https://www.nytimes.com/2013/04/07/us/taping-of-farm-cruelty-is-becoming-the-crime.html>.
- Packard, Noel. 2020. "The ARPANET into the Internet: a tale of Two Networks." *Studies in Media and Communication* 13.
- Passavant, Paul Andrew. 2021. *Policing protest*. Durham: Duke University Press.
- Perel, Maayan, and Niva Elkin-Koren. 2016. "Accountability in Algorithmic Copyright Enforcement." *Stanford Technology Law Review* 61. <https://law.stanford.edu/wp-content/uploads/2016/10/Accountability-in-Algorithmic-Copyright-Enforcement.pdf>.
- Perlroth, Nicole, interview by Hari Sreenivasan. 2021. (April 21). <https://www.pbs.org/video/nicole-perlroth-how-they-tell-me-world-ends-oe8g8v/>.

- . 2021. *This is How they Tell me the World Ends*. New York City: Bloomsbury Publishing.
- Perlroth, Nicole, and David E. Sanger. 2017. "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool." *The New York Times*, May 12: A1. <https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html>.
- Peterson, Andrea. 2013. "LOVEINT: When NSA officers use their spying power on love interests." *The Washington Post*, August 24. <https://www.washingtonpost.com/news/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/?noredirect=on>.
- PolitiFact. 2012. "Government had role in Google." *Tampa Bay Times*, July 14. <https://www.tampabay.com/news/politics/national/government-had-role-in-google/1240267/>.
- Radden Keefe, Patrick. 2005. *Chatter: dispatches from the secret world of global eavesdropping*. New York: Random House.
- Ram, Aliya, and Madhumita Murgia. 2019. "Data brokers: regulators try to rein in the 'privacy deathstars'." *The Financial Times*, January. Accessed November 30, 2022. <https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521>.
- Regan, Priscilla M. 2012. "Regulating surveillance technologies: Institutional arrangements." Chap. 4.2.a in *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin Haggerty and David Lyon, 397-404. Abingdon, Oxon: Routledge.
- Risen, James, and Eric Lichtblau. 2005. "Bush Lets U.S. Spy on Callers Without Courts." *The New York Times*, December 16. Accessed March 31, 2017. http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html?_r=0.
- Roberston, Adi. 2020. *Senate passes surveillance bill without ban on web history snooping*. May 14. Accessed September 20, 2021. <https://www.theverge.com/2020/5/14/21257782/surveillance-bill-congress-senate-pass-usa-freedom-reauthorization-act>.
- Roose, Kevin. 2021. "Inside Facebook's Data Wars." *The New York Times*, October 04: Section B, Page 1. <https://www.nytimes.com/2021/07/14/technology/facebook-data.html>.
- Rosen, Jeffrey. 2013. *The Lies Aren't What Make Obama's NSA Stance So Awful*. August 12. Accessed September 20, 2021. <https://newrepublic.com/article/114276/obama-surveillance-comments-dishonesty-isnt-only-problem>.
- Rosenberg, Emily S. 2014. "U.S. mass consumerism in transnational perspective." In *America in the world: the historiography of American foreign relations since 1941*, edited by Frank Costigliola and Michael J. Hogan, 307-337. New York: Cambridge University Press.
- Rosenzweig, Paul. 2016. *The Surveillance State: Big Data, Freedom, and You*. Palo Alto: The Teaching Company.
- Ryan-Mosley, Tate, and Sam Richards. 2022. *The secret police: Cops built a shadony surveillance machine in Minnesota after George Floyd's murder*. Boston: MIT Technology Review. Accessed April 13, 2022. <https://www.technologyreview.com/2022/03/03/1046676/police-surveillance-minnesota-george-floyd/>.
- Samuelsohn, Darren. 2014. "Stone: White House viewed surveillance report as 'liberal'." *Politico*, January 24. <https://www.politico.com/blogs/under-the-radar/2014/01/stone-white-house-viewed-surveillance-report-as-liberal-181849>.
- Sanger, David E. 2014. "Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say." *The New York Times*, April 12. Accessed March 13, 2022. <https://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html>.

- Sanger, David E., and Charlie Savage. 2013. "Obama Is Urged to Sharply Curb N.S.A. Data Mining." *The New York Times*, December 13: A1. <https://www.nytimes.com/2013/12/19/us/politics/report-on-nsa-surveillance-tactics.html>.
- Satter, Raphael. 2020. "'Woefully lax': report slams CIA cybersecurity after hacking tool leak." *Reuters*, June 16. Accessed September 21, 2021. <https://www.reuters.com/article/us-usa-cia-wikileaks-idUSKBN23N2CY>.
- Savage, Charlie. 2023. "Biden Administration Asks Congress to Reauthorize Warrantless Surveillance Law." *The New York Times*, February 28: Section A, Page 11. <https://www.nytimes.com/2023/02/28/us/politics/biden-warrantless-surveillance-section-702.html>.
- . 2023. "Lawmaker Says He Was Target of F.B.I. Surveillance Material Searches." *The New York Times*, March 09: Section A, Page 16. Accessed March 26, 2023. <https://www.nytimes.com/2023/03/09/us/politics/fbi-surveillance-darin-lahood.html>.
- Scahill, Jeremy. 2013. *Dirty Wars: The World is a Battlefield*. New York: Nation Books.
- Schiffer, Zoe. 2021. *Google fires second AI ethics researcher following internal investigation*. February 19. Accessed April 10, 2022. <https://www.theverge.com/2021/2/19/22292011/google-second-ethical-ai-researcher-fired>.
- Schneier, Bruce. 2015. *Australia Outlaws Warrant Canaries*. March 31. Accessed April 2022. https://www.schneier.com/blog/archives/2015/03/australia_outla.html.
- . 2018. *Click Here to Kill Everybody: security and survival in a hyper-connected world*. New York: W. W. Norton and Company.
- . 2015. *Data and Goliath: the hidden battles to collect your data and control your world*. New York: W.W. Norton & Company.
- . 2017. "Why the NSA Makes Us More Vulnerable to Cyberattacks: the Lessons of WannaCry." *Foreign Affairs*, May 30: Online only. Accessed December 7, 2017. <https://www.foreignaffairs.com/articles/2017-05-30/why-nsa-makes-us-more-vulnerable-cyberattacks> 1/7.
- . 2019. "There's no Good Reason to Trust Blockchain Technology." *Wired*, February 06. Accessed February 25, 2019. <https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/>.
- Schrems, Max. 2022. *CNIL decides EU-US Data-Transfer to Google Analytics illegal*. April 02. Accessed April 16, 2022. <https://noyb.eu/en/update-cnil-decides-eu-us-data-transfer-google-analytics-illegal>.
- . 2020. *EU-US data transfers*. July 30. Accessed April 16, 2022. <https://noyb.eu/en/project/eu-us-transfers>.
- Schuba, Tom, and Frank Main. 2021. "Chicago Police Department launched secret drone program with off-the-books cash." *Chicago Sun Times*, May 12. Accessed April 13, 2022. <https://chicago.suntimes.com/city-hall/2021/5/11/22425299/cpd-chicago-police-drone-secret-emails-hack-lori-lightfoot-dodsecrets-city-hall>.
- Schwartz, Adam. 2022. *FTC Sues Location Data Broker*. September 07. Accessed December 3, 2022. <https://www.eff.org/deeplinks/2022/09/ftc-sues-location-data-broker>.
- Seifert, Dan. 2013. *Secret program gives NSA, FBI backdoor access to Apple, Google, Facebook, Microsoft data*. June 06. Accessed March 25, 2023. <https://www.theverge.com/2013/6/6/4403868/nsa-fbi-mine-data-apple-google-facebook-microsoft-others-prism>.
- Sherman, Justin. 2021. "Data Brokers Are a Threat to Democracy." *Wired Magazine*, April 13. <https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy/>.

- Simonite, Tom. 2021. *3 Years After the Project Maven Uproar, Google Cozies to the Pentagon*. November 18. Accessed November 25, 2021. <https://www.wired.com/story/3-years-maven-uproar-google-warms-pentagon/>.
- . 2020. *A Prominent AI Ethics Researcher Says Google Fired Her*. December 03. Accessed April 10, 2022. <https://www.wired.com/story/prominent-ai-ethics-researcher-says-google-fired-her/>.
- Sloan, Robert H., and Richard Warner. 2017. "Relational Privacy: Surveillance, Common Knowledge and Coordination." *University of St. Thomas Journal of Law and Public Policy* 11 (1): 1-25.
- Solomon, John. 2017. *Newly declassified memos detail extent of improper Obama-era NSA spying*. July 25. Accessed March 25, 2023. <https://thehill.com/policy/national-security/343785-newly-declassified-memos-detail-extent-of-improper-obama-era-nsa/>.
- Solove, Daniel J. 2007. "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy." *San Diego Law Review* 44 (745): 745-772.
- Solove, Daniel J., and Danielle Keats Citron. 2021. "Privacy Harms." *George Washington Law Faculty Publications & Other* 63. https://scholarship.law.gwu.edu/faculty_publications/1534.
- Sottek, T.C. 2013. *NSA reportedly intercepting laptops purchased online to install spy malware*. December 29. Accessed March 13, 2022. <https://www.theverge.com/2013/12/29/5253226/nsa-cia-fbi-laptop-usb-plant-spy>.
- Stoler, Mark A. 2000. "Book Review Michael J. Hogan. A Cross of Iron: Harry S. Truman and the Origins of the National Security State, 1945–1954." *The American Historical Review* 105 (1): 244-245. <https://doi-org.proxy3.library.mcgill.ca/10.1086/ahr/105.1.244>.
- Stone, Brad. 2009. "Amazon Erases Orwell Books From Kindle." *The New York Times*, July 18. <https://www.nytimes.com/2009/07/18/technology/companies/18amazon.html>.
- Svirsky, Daniel. 2019. "Why are privacy preferences inconsistent? information avoidance." *John M. Olin Center for Law, Economics, and Business Discussion Paper No. 81*. Cambridge: Harvard Law School, January. 36.
- Tau, Byron. 2020. "IRS Used Cellphone Location Data to Try to Find Suspects." *The Wall Street Journal*, June 19. Accessed September 20, 2021. <https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815>.
- Taube, Dan, Keely Kolmes, and Colette Voge. 2014. *Preliminary Report: Without My Consent Survey of Online Stalking, Harassment and Violations of Privacy*. Survey summary, San Francisco: Without My Consent. https://withoutmyconsent.org/sites/default/files/wmc_prelim_survey_report.pdf.
- The Electronic Frontier Foundation. 2017. *CALEA*. San Francisco: The Electronic Frontier Foundation. Accessed November 24, 2022. <https://www.eff.org/issues/calea>.
- . 2018. *CDA 230: Legislative History*. Accessed 2021. <https://www.eff.org/issues/cda230/legislative-history>.
- The Washington Post. 2013. "NSA slides explain the PRISM data-collection program." *The Washington Post*, June 06. Accessed March 25, 2023. <https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>.
- The White House. 2023. *2003 National Cybersecurity Strategy*. Full Report, Washington, D.C.: United States of America. Accessed March 27, 2023. <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.
- The White House. 2023. *Fact Sheet: Biden-Harris Administration Announces National Cybersecurity Strategy*. Press Release, Washington, D.C.: United States of America. Accessed March 27, 2023. <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/>.

- Tsukayama, Hayley. 2013. "The Circuit: Netflix reaps benefits of VPPA lobbying, turns on social feature." *The Washington Post*, March 13. Accessed March 27, 2023. https://www.washingtonpost.com/blogs/post-tech/post/the-circuit-netflix-reaps-benefits-of-vppa-lobbying-turns-on-social-feature/2013/03/13/71e1df22-8bf4-11e2-b63f-f53fb9f2fcb4_blog.html.
- Turow, Joseph, Michael Hennessy, Nora Draper, Ope Akanbi, and Diami Virgilio. 2018. *Divided We Feel: Partisan Politics Drive Americans' Emotions Regarding Surveillance of Low-Income Populations*. Academic, University of Pennsylvania, Annenberg: Annenberg School for Communication. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3609974.
- Turton, William. 2022. *Apple and Meta Gave User Data to Hackers Who Used Forged Legal Requests*. March 30. Accessed April 13, 2022. <https://www.bloomberg.com/news/articles/2022-03-30/apple-meta-gave-user-data-to-hackers-who-forged-legal-requests>.
- United Nations Special Rapporteur on Counter-Terrorism and Human Rights. 2013. *Drones Inquiry*. New York: SITU Research. <https://situ.nyc/research/projects/unsrct-drones-inquiry>.
- Urban, Jennifer M., and Laura Quilter. 2005. "Efficient Process or Chilling Effects - Takedown Notices under Section 512 of the Digital Millennium Copyright Act." *Santa Clara Computer & High Tech. Law Journal* (HeinOnline) 22: 621-694. <http://scholarship.law.berkeley.edu/facpubs/501>.
- US Congress. 1938. "Wheeler-Lea Act." Washington, D.C. ch. 49, sec. 3, § 5(a), 52 Stat. 111, 111–12.
- Valentino-DeVries. 2019. "Tracking Phones, Google Is a Dragnet for the Police." *The New York Times*, April 13. <https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html>.
- Valentino-DeVries, Jennifer. 2019. "Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works." *The New York Times*, April 13: A19. Accessed April 13, 2019. <https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html>.
- . 2019. "Secret F.B.I. Subpoenas Scoop Up Personal Data From Scores of Companies." *The New York Times*, September 20: Section A, Page 1. Accessed October 01, 2019. <https://www.nytimes.com/2019/09/20/us/data-privacy-fbi.html>.
- Van der Sar, Ernesto. 2013. *Alleged BitTorrent Pirate Sued Three Times For The Same Download*. May 03. Accessed March 25, 2023. <https://torrentfreak.com/alleged-bittorrent-pirate-sued-three-times-for-the-same-download-130502/>.
- . 2006. *The Past and Future of Filesharing*. August 01. Accessed March 25, 2023. <https://torrentfreak.com/the-past-and-future-of-filesharing/>.
- Villas-Boas, Antonio. 2019. *Police departments across the US are using video doorbells from Amazon-owned Ring to create an unofficial surveillance network, a new report says*. June 7. Accessed June 14, 2019. <https://www.businessinsider.com/amazon-ring-video-doorbell-footage-used-by-police-report-2019-6>.
- Viola, Lora Anne, and Pawel Laidler. 2022. *Trust and transparency in an age of surveillance*. New York: Routledge.
- Walton, Reggie B. 2013. *Letter to Senator Grassley*. Letter, Washington D.C.: United States Foreign Intelligence Surveillance Court.
- Warren, Samuel D., and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4 (5): 193-220.
- Welna, David. 2014. "Before Snowden: The Whistleblowers Who Tried To Lift The Veil." *NPR Morning Edition*, July 22. Accessed March 13, 2023. <https://www.npr.org/2014/07/22/333741495/before-snowden-the-whistleblowers-who-tried-to-lift-the-veil>.

- Westin, Alan F., and Louis F. Harris. 1981. *The Dimensions of Privacy*. New York: Garland Publishing.
- Whelan, Glen. 2019. "Trust in Surveillance: A Reply to Etzioni." *Journal of Business Ethics* 156: 15-19. doi:10.1007/s10551-018-3779-4.
- Wikipedia. 2021. *Lane v. Facebook, Inc.* November 3. Accessed January 13, 2022. https://en.wikipedia.org/wiki/Lane_v._Facebook,_Inc.
- Wong, Julia Carrie. 2020. "More than 1,200 Google workers condemn firing of AI scientist Timnit Gebru." *The Guardian*, December 04. Accessed April 10, 2022. <https://www.theguardian.com/technology/2020/dec/04/timnit-gebru-google-ai-fired-diversity-ethics>.
- Wu, Tim. 2016. *The Attention Merchants: the Epic Scramble to Get Inside Our Heads*. New York: Knopf.
- . 2019. "How Capitalism Betrayed Privacy." *The New York Times*, April 10: SR3. Accessed April 14, 2019. <https://www.nytimes.com/2019/04/10/opinion/sunday/privacy-capitalism.html?login=email&auth=login-email>.
- Wyden, Ron. 2021. "20 Years After the Patriot Act, America Must End Secret Law." *Just Security*, October 26. <https://www.justsecurity.org/78766/20-years-after-the-patriot-act-america-must-end-secret-law/>.
- Zetter, Kim. 2016. "Reddit Hints—Without Saying Anything—That It Got a National Security Letter." *Wired*, March 31. Accessed April 13, 2022. <https://www.wired.com/2016/03/reddit-warrant-canary-hints-it-got-a-national-security-letter/>.
- Zhuang, Yan, Elian Peltier, and Alan Feuer. 2021. "The Criminals Thought the Devices Were Secure. But the Seller Was the F.B.I." *The New York Times*, June 08: Section A page 1. Accessed September 20, 2021. <https://www.nytimes.com/2021/06/08/world/australia/operation-trojan-horse-anom.html>.
- Zuboff, Shoshana. 2015. "Big other: surveillance capitalism and the prospects of an information civilization." *Journal of Information Technology* 30: 75-89. doi:10.1057/jit.2015.5.
- . 2019. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: Public Affairs.

Chapter 2 Measuring Privacy Concerns under the Surveillance Complex

Abstract

This chapter introduces and describes my operationalization of the surveillance complex, testing news measures across different policies. Building on Helen Nissenbaum's theory of contextual integrity, I hypothesize that people's attitudes towards deputized surveillance are substantively (and statistically) different from their attitudes towards surveillance in general when it is produced and ensconced by the government and analogously by the market. To test my hypothesis, I surveyed 1,493 throughout August of 2021, asking them whether they strongly disagree, somewhat disagree, somewhat agree, or strongly agree that a range of surveillance policies should be implemented. I explore their opinion preferences using a data-reduction technique called Principal Components Analysis. I find that Americans' responses produce a multi-dimensional space. This finding alone is a contribution to empirical privacy research. The few researchers who work on multiple surveillance sources tend to average out all sorts of practices, whether unattributed (e.g., "I am concerned about my data"), from governments, or companies, into a single index. While the state's own surveillance and the market's own surveillance policies produce two dimensions with some cross-"contamination", deputized surveillance produces a clear and distinct different dimension of around. This bolsters a larger contribution to privacy studies: deputized surveillance is more than the sum of its parts. In contradistinction to previous theorizing about contextual integrity, but supporting Chapter 1's claim that deputized surveillance allows the government to shirk political costs, I find that this distinct dimension of concerns is lower than surveillance capitalism and government surveillance. A deliberate impetus to be holistic but precise is better served by clarity in our language when theorizing and measuring the phenomenon.

Introduction

How do Americans feel about pervasive, ubiquitous mass surveillance techniques? Answering this question depends on whether the entities collecting the data differ from those using it. In this chapter, I describe how I build on previous measures, describe siloes in the literature, and advance new measures, testing the validity of my hypotheses about how surveillance attribution and data flows shape distinctive dimensions of privacy concerns.

According to privacy theorist Helen Nissenbaum, people's concerns over privacy violations reflect context-dependent "norms of appropriateness" that keep data where it is expected to belong (2010). If context informs what we consider appropriate, people's understanding of who is surveilling and what the data is for should influence people's privacy concerns. However, as discussed in chapter

1, uncertainty over who holds what data is a feature of the surveillance complex that enables actors to escape political and legal accountability. Surveillance can come exclusively from state or market forces or corporations deputized by states¹⁰⁴. I use this taxonomy throughout the dissertation. In this chapter, I produce a novel set of measures for each component of the surveillance complex that disentangles American public opinion. I hypothesize that concern for surveillance deputation should be distinct from state-exclusive or market-exclusive surveillance because it violates the contextual integrity boundaries between the party that collects data (markets) from the party that uses it (governments). I conclude from the empirical evidence that that is the case: concerns over deputized surveillance are distinct from the two other forms of surveillance. These different logics of surveillance produce *multiple* dimensions of privacy concerns based on the monitoring sources. They cannot be “averaged out” into a single measure; responses to policies that have no surveillant attribution (what I call baseline measures) are also distinct, so they cannot be used as “catch-all” substitutes. Thus, measures on attitudes towards deputized surveillance should not be “folded” into any of the other forms of surveillance attitude measures.

A concern in this dissertation is that the surveillance complex obscures and creates uncertainty in how information is extracted and aggregated. If deputation exacerbates data flow obscurity from companies to states, the incentives to regulate and wean off low-cost data are minimal. This would produce a conflict in democratic governance—artificially obscuring the supply of surveillance data, making it hard for citizens to be informed of the policies that govern them. The lowered political costs make any remaining citizen demand for privacy easier to ignore. In other words, the embedded opacity of responsibility makes attribution of surveillance—and subsequent accountability for it—near-

¹⁰⁴ “Peer to peer” surveillance between individuals are mediated by market availability (e.g., commercial stalkerware). In democracies they are not institutionalized (compared to countries with strong morality cultures that reward citizen deputation), and thus defined by inter-personal, even intimate, motivations. I measure concerns and experiences with this type of surveillance and control for it in my models, but I do not analyze them as an outcome.

impossible. That, in turn, jeopardizes claims of meaningful citizen-cum-user consent. As I argue in chapter 1, this seems to be a feature, not a bug. Democratic governments have piggybacked on technological innovations driven by market forces' own profit motives using various legal and technical tools and economic incentives, which I detailed in chapter 1. Understanding patterns of differences in people's opinions between government-operated surveillance, market consumer surveillance, and the growing intersection (deputized surveillance) can help explain why consumer data markets remain deregulated despite on-paper privacy rights and the individual security harms derived from proliferating surveillance.

According to privacy theorist Helen Nissenbaum, people's concerns over privacy violations reflect context-dependent "norms of appropriateness" (2010). If context informs what is appropriate, people's understanding of who is surveilling and their motivations should shape their privacy concerns. But information about privacy violations, and the context in which it occurs, is not always readily available¹⁰⁵. The surveillance complex produces different legal, political, and economic regimes and contexts that sustain surveillance practices with varying levels of visibility/transparency for people as consumers vs. citizens. Most information about surveillance practices has come from whistleblowers, security researchers, and journalists, *despite* the wishes of those who operate or make use of the data. This produces a patchwork of information where "blockbuster" revelations that reach a broad audience are the exception (i.e., Snowden and Cambridge Analytica). Where attention is placed is unsteady. At times, media and public attention are focused on government-operated surveillance (e.g., police use of drones and Stingray), and at other times it is focused on surveillance capitalism (e.g., the ubiquity of Facebook pixels on websites). Once in a while, attention is paid to their

¹⁰⁵ Recently, communications scholar Joseph Turow has argued that, when it comes to companies' use of their data, because Americans "don't understand it, say they're helpless to control it, and believe they are harmed when firms use their data—mak[es] what companies do illegitimate" (Turow 2023).

intersection, what I have dubbed deputized surveillance (e.g., Dropbox's agreement to give NSA access to its network).

In the theory section, I discuss the underlying assumptions of contextual integrity found in government-exclusive and market-exclusive surveillance attitude studies and exemplify how these assumptions have been operationalized in previous studies. I am motivated by conceptual and measurement oversights detailed below. This chapter highlights a gap in the literature produced from studying attitudes towards state surveillance isolated from market surveillance; in doing so, I construct an interdisciplinary critique of previous privacy concern measurements and identify the absent measurement of attitudes towards how the state accesses market surveillance for its own purposes. Doing so requires disentangling overlapping panopticons.

I hypothesize that, following Nissenbaum's theory, people's privacy concerns will differ by surveillance purposes. Surveillance deputation blurs data collection's attribution against who is making use of collected data. Thus, I hypothesize that surveillance deputation responses will differ from those where data collection and data use is consistently ensconced in the same sphere (government/market use of data collected by the government/market). This chapter presents a novel test of Nissenbaum's theory using survey data from a nationally representative sample of Americans.

I use an original, nationally representative survey of Americans ($n=1,493$) conducted in August 2021 (see also technical chapter 5). In the Methods and Data section, I describe the question wording of my survey of Americans' privacy concerns. I propose alternative measurements to disentangle explicitly the contexts in which mass online surveillance is carried out. I measure attitudes toward "state-exclusive" policies (where the government conducts surveillance for public policy purposes), "market-exclusive" surveillance (portrayed as customer monitoring and data use for profit-making purposes within a capitalist logic, following Zuboff's 'surveillance capitalism'), and, crucially, government's deputation of corporations, as well as non-attributable generalized data collection. I

build on two large-n comparative surveillance surveys (Hampson and Jardine 2016, Zureik, Harling Stalker and Smith, et al. 2010, respectively) and other smaller surveys. I measure opinions on a wide range of surveillance policies and use a statistical tool called Principal Components Analysis to test my hypothesis. I analyze the uniqueness and correlation of responses. If, as Nissenbaum posits, context integrity of data collection and retention matters, people’s understanding of who is surveilling and (purportedly) what for ought to map onto distinct dimensions. Further, deputization’s violation of context integrity should produce a particular dimension.

I find supporting evidence for my hypothesis (see Results) that attitudes toward deputized surveillance differ from the sum of its parts (government-exclusive and market-exclusive surveillance). People have multi-dimensional privacy concerns that should not be collapsed into a single measurement, which has been the custom in previous studies. This finding holds even when a surveillance tactic extracts the same information (e.g., location)—attitudes towards deputized surveillance remain distinct from government-exclusive and market-exclusive versions. My measures are a novel contribution that articulates a more clear-eyed test of attitudes on how surveillance factually works¹⁰⁶ in advanced capitalist democracies, where governments have codified privacy protections but systematically circumvent them.

Beyond the distinct attitudes towards deputized surveillance, where contextual integrity expectations are violated, I also find compelling evidence that attitudes towards some forms of government-exclusive surveillance differ from attitudes towards market-exclusive surveillance. In other words, even when contextual integrity norms of privacy are intact, there is variation in the acceptability of practices depending on who is carrying them out. The observed differences substantiate my critique that the findings from state-centric and market-centric fields of study are

¹⁰⁶ See for example the Electronic Frontier Foundation’s 30 year anniversary discussion with Edward Snowden on “fiduciary responsibility” (Cohn, et al. 2021) and contrast to the framing around governmental “increased liability” use of responsibilities (Schmon and Pedersen 2022).

disjointed. Crucially, they should not be ‘averaged out’ into a unidimensional measure as this obscures important differences in public opinion derived from heterogeneity in legitimacy and information. Consolidating disparate forms and sources of surveillance without theoretically sound reasons and empirically proving they are compatible erases the different contexts that shape surveillance public opinion.

Explicitly systematizing the source of surveillance when measuring attitudes is a valuable intervention Political Science can make to privacy studies. This work is especially needed in advanced democracies, where surveillance policies are not meant to be a visible top-down show of state force in contrast to autocratic regimes. This endeavor follows Adcock and Collier’s opinion that a “consequence of ... provid[ing] a fleshed out account may be the recognition that the concept needs to be disaggregated” (Adcock and Collier 2001, 534).

Explaining surveillance deputation attitudes has become increasingly urgent in light of COVID-19. Public health agencies relied on private health surveillance partnerships that required active citizen engagement. One study in the early stage of the pandemic found that an absence of explicit privacy guarantees made citizens reluctant to use technologies that monitor health, physical location, and social interactions (Zhang, Kreps and McMurry 2020). These partnerships further disarray the implicit presumption that surveillance spheres are distinct. The privatized nature of the American healthcare system and low levels of consumer choice make the coercive character of deputized surveillance salient. The Dobbs decision, which does away with interpreting a Constitutional “penumbra of privacy” since *Roe versus Wade*, has increased public scrutiny of companies tracking healthcare information and location data. Companies selling that data for ad sales (Cox 2022, Feathers, et al. 2022) might be coerced into turning over that data to governments that want to enforce bans on abortion-seeking proactively (Kalish 2022, Vagianos 2022), incentivized to do so directly through bulk data purchases, or unknowingly collaborate if their data is resold by a third-party.

Theory

According to Nissenbaum, four components in the appropriate norm establish whether “contextual integrity” remains or has been shattered: contexts, actors, attributes, and transmission principles (e.g., consent). In more plain terms,

“What information do you have? From where did you get it? To whom do you give it, for what purposes, and under what conditions? Clear answers to these and other questions seem important to judgments whether privacy is threatened or violated; yet they are often not offered, and more often not offered clearly” (2010, 50).

However, getting clear answers about how data is collected or what is done to it is not easy. By some accounts, even data Goliaths have no exhaustive knowledge of who has access to its data or where it is stored (Biddle 2022) because they “built systems with open borders” (Franceschi-Bicchierai 2022). Attributing surveillance is increasingly ambiguous and opaque. If contextual integrity cannot be assured, privacy threats proliferate. Certainty is an implicit, under-measured factor in shaping privacy concerns. Previous privacy concerns studies have unwittingly contributed by obfuscating surveillance’s context certainty in several ways.

For example, they may attribute untheorized but unique known objectives to surveillance by using survey wording such as “for criminal investigations”, “for national security”, “for ad targeting”, etc. This way of conceptualizing surveillance capabilities is a remnant of when (pre-digital) data was siloed (Citron and Gray, Addressing the Harm of Total Surveillance: a Reply to Professor Neil Richards 2013). Surveillance used to take place in constrained spaces, and databases across organizations were not customarily merged. For a time, a single controlling institution would monitor individuals, so the objective of monitoring could be derived from a single source. The artificially siloed assumption is widespread in government-exclusive studies. It also occurs in market-exclusive surveillance studies even though cross-website cookies¹⁰⁷ have been discussed since at least a decade

¹⁰⁷ Facebook tracks people’s online behavior outside its website including capturing sensitive data from hospital appointment websites (Chan 2022).

ago (Reitman 2011). The classic Foucaultian analysis of *the* (emphasis on a single) panopticon is one in which the monitored subject was physically in an observation space. One is either in prison or not, in school or not, at work or not, at the asylum or not; monitoring of compliance and subsequent internalization of the location's rules happens at the hands of one institution at a time (Foucault 1995).

However, the nature of online communications allows for overlapping panopticons that erode clarity on who is surveilling (sometimes called “liquid surveillance” (Bauman and Lyon 2012)). This affordance has given way to an unregulated industry of data brokers and aggregators (e.g., Palantir). Digital data is a non-exclusive good that can be reproduced ad infinitum, bounded only by storage limits. Data's non-exclusivity incentivizes what economic theory calls “economies of scope” (Goldhar and Jelinek 1983). An economy of scope enables the same surveillance data to be recycled to produce/run multiple ‘products’ (e.g., in training data for algorithms, predictive policing, and ad sales).

The second way surveys might muddle what respondents understand about mass surveillance is if they echo government claims that *only* criminals are targeted (Solove 2011). A similar version of this ilk includes punitive narratives, such as the unproven assertion that proactive monitoring curbs future crimes (Tunney 2019, Canadian Cultural Mosaic Foundation 2020). Examples of this kind of phrasing, with my emphasis in bold, are: “law enforcement should be free to search a property without a warrant **solely on the suspicion that a crime or a terrorist act is being planned there**” (Davis and Silver 2004), “Some people say that government should be allowed to record telephone calls and monitor email **in order to prevent people from planning terrorist or criminal acts**. Others say that people's conversations and email are private and should be protected by the constitution” (idem), and “Here are some increased powers of investigation that law enforcement agencies **might** use when **dealing with people suspected of terrorist activity**, which would also affect our civil liberties. For each, please say if you would favor or oppose it” (Westin 2003, Taylor 2001).

Questions like these reproduce a false sense of protection *from* mass surveillance because they re-frame the policies as ultimately producing targeted results, which allows readers to interpret them as targeted surveillance. They are meant to insulate policies that affect everyone from scrutiny. John Zaller warns that:

“the most fundamental question” about frames of reference is whether the public is given any choice about them— whether, that is, it is permitted to choose between alternative visions of what the issue is. For in the absence of such choice, the public can do little more than follow the elite consensus on what should be done” (1992, 8).

Questions like the aforementioned misrepresent the policies’ true monitoring scope, capabilities, how they are deployed even without articulated legal reasoning, and lack of oversight. The example questions above reproduce distorted representations of technologically impossible mass surveillance policies purporting to be targeted. In Chapter 3, I examine whether law-and-order frames that tap into an assertion that criminals are the only ones harmed by mass surveillance increase mass surveillance acceptance. In Chapter 4 I test the tradeoff between privacy and security preferences in the EU.

The current (known) practice for American communications surveillance requests phone records for “three-hops” or 3 levels of daisy chain data (Gellman 2020). Three hops are three degrees of separation from an investigation’s surveillance target: a target’s communications (A), all the communications target (A)’s contacts made (B ... Z) with others (B’ ... Z’) and the communications of everyone *they* made (B”... Z”). Gathering this scope of data makes it statistically likely that all Americans’ data has been collected via three-hop wiretaps.

Questions using national security frames to measure attitudes might introduce measurement errors. They are likely measuring people’s belief that the government can only use the data as promised: on specifically targeted subjects for a predefined end. That differs from measuring attitudes towards the policy means themselves: mass data capture for retroactively defined ends. Some respondents may

find surveillance policy frames implausible in other ways, impacting the conclusions drawn from security-framed measures. How can the government know what data does not involve criminal activity unless they check all of it? Mass surveillance is like asking everyone to continuously turn their pockets over to prove they have not and are not planning on robbing someone in the room—more fishing expedition than targeted policing acting on falsifiable evidence. In the words of the former director of the National Security Agency, “[y]ou need the haystack to find the needle” (Gellman 2020, 300). It is economically cheaper and computationally more efficient to collect and analyze everyone’s data¹⁰⁸ (Schneier 2018). For all the reasons described above, targeted government-exclusive surveillance frames are technologically implausible.

The impulse to reframe government-exclusive mass surveillance as a policy that produces selective outcomes might be caused by a comparative process. Relative minimization of mass data *collection* against data *use* leads many to consider the latter invasive and the former less so by comparison, creating a measurement problem. Preferences over targeted surveillance are conflated as preferences over mass surveillance when the means and ends become muddled. I have highlighted how this logic has seeped into government-exclusive surveillance but Chapter 3 addresses this issue in depth.

Kerr et al.’s typology of surveillance exemplifies a recurring binary classification logic. Passive data collection (i.e., only monitoring) is juxtaposed to active surveillance practices, where data collection leads to additional (i.e., escalating) activity, such as notifying or even mobilizing authorities in reaction to the collected data. They suggest surveillance should be categorized as “soft” when only data collection occurs. After all, it is *perceived* to be less intrusive in its outcomes because it is a less visible practice (2009). Data collection that leads to a secondary outcome with visible institutional interaction (e.g., arrests, censorship, lawsuits) is thus, comparatively, “hard” surveillance (Kerr, et al.

¹⁰⁸ This is the logic behind much artificial intelligence.

2009). Hard surveillance is perceived to be more intrusive because as more institutions interact with the data to put it to use, the surveillance practices become more visible/tangible.

I postulate that these distinctions produce distorted representations of surveillance because they rely on making harm a necessary component¹⁰⁹. The act of monitoring becomes tacitly erased from the definition of surveillance when such distinctions are used in media frames, policy discussions, and academic research. A thought exercise illustrates the distortion. Imagine a police officer who follows someone on the street on foot for blocks. This behavior is called surveillance. The police officer may hide their surveillance by staying out of eyesight or make their surveillance known (i.e., visible) to the person being followed. Whether visibility comes from contact with the person during questioning, a physical inspection, or even an arrest is irrelevant to the fact that police surveilled a person on the street. Likewise, whether the police officer records any of their observations, creates a dossier in a database, checks for priors, etc., is largely irrelevant to the fact that surveillance occurred. For some reason, distinguishing whether monitoring is done physically or via digital communications matters to our understanding of whether surveillance occurred or did not. Passive data monitoring tends to be minimized against any subsequent active surveillance practices (soft/hard). Minimizing monitoring as soft surveillance has drawn academic attention away from mass surveillance practices toward policies that produce subsequent policing targeted at individuals or groups (Turow, Hennessy, et al. 2018, Ziller and Helbling 2020, Zureik, Harling Stalker and Smith, et al. 2010).

Lastly, certainty can often be conflated with trust. In summary, this perspective holds that institutions are trusted to do the right thing, either engaging in surveillance or treating the produced data acceptably (Westin 1967). Alan Westin, a researcher who studied post-war privacy preferences of medical, financial, and human resources/labor data, theorized that people's rejection of digital

¹⁰⁹ American legal scholars are also scrutinizing the effects of the current harms-based approach of American privacy law, arguing that meeting the current harm threshold excludes many types of harms and likewise excludes many forms of surveillance from being legally challenged and remedied (Solove and Citron 2021).

surveillance could be traced back to distrust in the technologies themselves by way of a lack of knowledge of how they worked. He hypothesized that as workplace-monitoring technology became ubiquitous in the future, people would realize there was nothing to distrust about computers and would become increasingly accepting with time (1967). His theory is one of normalization: increased exposure will increase trust in technologies and the authorities/institutions that use them¹¹⁰. If that were the case, public opinion concern over surveillance would be tamped down with the increased adoption of digital technology and the passing of time. Westin's hypothesis has not been borne out even when circumscribed to workplace surveillance. Research suggests that normalization has not occurred despite increasingly ubiquitous workplace surveillance and increasingly aware workers. Fettered by labor coordination issues, workers have had difficulty organizing their opposition until recently (Teamsters 2022). This vacuum of public opinion has allowed technologists who profit from surveillance to claim "privacy is dead. Get over it" (H. A. Popkin 2010). However, one 2022 survey found that even among technology workers (n=750), half declared they would quit if facial recognition, audio, or other workplace monitoring were implemented (Morning Consult 2022).

As explained in chapter 1, the surveillance complex exploits uncertainty to ensure its continuation. It shields government institutions from transparency and prevents public accountability. Without knowledge of wrongdoing, there are minimal reasons for citizens to distrust institutions; thus little reason for citizens to demand government regulation of the corporate data collection and distribution practices which would choke off mass state surveillance. This chapter measures privacy concerns that can disentangle multi-dimensional surveillance sources by reducing respondent uncertainty.

¹¹⁰ His industry-friendly policy advocacy explains how he reached this conclusion. Normalization neglects the role of informed consent. As American workers have no say in their labor conditions, the issue of consent can be brushed away. His expectation also requires that there be nothing reprehensible about surveillance. Both issues have not worked out that way.

After 9/11 and the subsequent passage of the Patriot Act 45 days after, the Political Science field produced a limited amount of work researching acceptance of government surveillance (online or offline), focusing on citizen emotions and support for the legislative *fait accompli*. These studies compared surveillance policy outcomes between external shocks like international terrorism (i.e., external threats from immigrants or people whose “Americanness” (i.e., non-whiteness) was scrutinized). A survey conducted on the heels of the 9/11 attack concluded that Americans were willing to trade off civil liberties for policies framed as increasing personal protection (Davis and Silver 2004, 32). However, as the War on Terrorism drags on, we cannot expect shock to 9/11 to explain supporting attitudes towards the *pervasive* institutionalized surveillance techniques decades after.

Corporate technologies and consumer adoption patterns drive advanced democracy surveillance, not overt state-directed coercion¹¹¹. However, measurements about concerns over market surveillance have been absent in Political Science. This omission might be due to state-centric blinders in the field. Companies based in advanced democracies design, operate, market, and otherwise develop technologies to defeat privacy and data integrity¹¹² (Hao 2020).

Significant changes in market surveillance practices shaped the limits to scholars’ research questions, their ability to formulate them, and gather data to test them promptly. The early literature viewed privacy concerns around commercial data as an obstacle to transaction intentions¹¹³. The

¹¹¹ Although chapter 1 provided evidence of how the American “invisible hand” shapes technological supply through government funding, non-regulation and forbearance, and military-intelligence contracts.

¹¹² America’s Cisco, Canada’s Nortel Networks, and Finland’s Nokia collaborated on the first national Chinese database of adults that integrated physical and digital surveillance, called “Golden Shield” and the “Great Firewall” internet filtering project that has restricted information flows into China.

¹¹³ Intention to transact was measured by four questions, all of which mentioned disclosing financial data: To what extent are you willing to use the Internet to do the following? 1 Purchase goods (e.g., books, CDs) or services (e.g., airline tickets, hotel reservations) from Web sites that require me to submit accurate and identifiable information (i.e., credit card information). 2 Retrieve information from Web sites that require me to submit accurate and identifiable registration information, possibly including credit card information (e.g., using sites that provide personalized stock quotes, insurance rates, or loan rates; or using sexual or gambling Web sites). 3 Conduct sales transactions at e-commerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software). 4 Retrieve highly personal and password-protected financial information (e.g., using Web sites that allow me to access my bank account or credit card account).

literature studying market surveillance comes mostly from economics, business, and management. These fields first studied lowering *consumer* barriers to sharing financial data to develop digital commerce (McDonald and Cranor 2010). I highlight consumers here because the shift from focusing on citizens to consumers comes with a change from rights to contract law, impacting how the courts define consent¹¹⁴. The role of consent, exacerbated by the illusion of privacy control settings, makes comparisons between corporate and state surveillance difficult, as corporate-exclusive surveillance is assumed to be devoid of coercion (see below).

The early 2000s “new internet” Web 2.0 services were defined by their reliance on user-generated content (O'Reilly 2005). As the Web 2.0 model of online behavior grew, two questions arose. Why did people post/refuse to post personal information that could be viewed by different audiences (strangers vs. known) in general? Moreover, why did people who said they were concerned about their privacy opt to use these services? These questions focused on willing, active disclosure of personal data: credit card numbers, a blog post on emotional hardships (PostSecrets), routine or mundane behavior (Julie Powell's blog on cooking Julia Child's book), services and experiences reviews (restaurants on Foursquare and Yelp). New, unfamiliar dot-com companies and third-party payment processors would handle credit card information online. Dinev et al. hypothesized that government surveillance of financial transactions reassured users of data safety (Dinev, Belotto, et al. 2006, Dinev and Hart 2005).

At the beginning of mass internet adoption, Americans were opting into services that were alternatives to other commonly used, non-digital services (phonebooks, newspapers, letter-writing,

¹¹⁴ Consent is intimately linked to choice. For example, consent of the governed requires democratic choice. Where there is no democratic choice (e.g., tyranny, authoritarianism, meaningless elections, etc.) there cannot be citizen consent and the social contract is broken. Consent is also important for contract law, as coercion invalidates contracts. People are expected to have the right to choose to contract with the most beneficial terms. However, when there are no market alternatives, can meaningful consent to contract be given? An emerging theory of anti-trust law is that monopolies impact contracting conditions and are thus harmful to consent. If your only option is to hand over the data, or not participate in a digital service, are the choices comparable? And if you are not able to avoid using a digital service, there is no true choice.

and landline calls). The joint availability of digital and analog services initially shaped the question of choice¹¹⁵. Twenty years later, many of these analog services are nonexistent. News outlets have shut down print versions, so all their ad-based funding is produced by individualized ad-tracking systems rooted in surveillance capitalism¹¹⁶ (Fang 2022). The legal privacy protections over physical mail far outweigh email protections (i.e., none), but very few communicate solely via physical letters. The choices available to consumers went from analog vs. digital vs. neither to digital vs. nothing¹¹⁷.

Early work on social network use studied how people (re)defined what was and was not private between online and offline communications. They instead focused on “networked”, person-to-person surveillance (Hargittai and Marwick 2016, 3744). Sharing content was explained by the “fear of being excluded” (Slee 2015). Before Facebook moved on from college campuses (2003-2005), it had operated as a “walled garden” model—a gated community in the online world that required affiliation credentials for membership. Lewis et al. found that even when servicing a relatively homogenous population, “[college] students¹¹⁸ are more likely to have a private profile if their friends and roommates have them; women are more likely to have private profiles than are men; and having a private profile is associated with a higher level of online activity” (2008).

Data access restrictions shaped Lewis et al.’s theoretical expectations of person-to-person privacy concerns. In effect, academics extrapolated (and some continue to) general population conclusions from convenience samples. Facebook’s first users were relatively homogenous networks of well-educated, young, wealthy Americans produced by the company’s walled garden. Another study of American graduates and undergraduates found they envisioned an “imagined community” of fellow

¹¹⁵ Including the use of neither makes three choices: no service, digital version, analog version.

¹¹⁶ One recent example, in 2022 the New York Times bought the Wordle puzzle game, which had no trackers, and filled it with trackers (Wodinsky 2022, Asher Hamilton 2022) despite stating two years before that it was phasing out 3rd party advertising data tracking (Fischer 2020).

¹¹⁷ One might ask, is that much of a choice? If not, can anyone truly consent in a choiceless environment?

¹¹⁸ Their sample came from a northeastern private university, which is very likely Harvard (where Facebook started) given all the authors’ institutional affiliation at the time of writing.

students that was increasingly divergent from reality as non-students joined the network (Acquisti and Gross 2006). In their study comparing privacy attitudes¹¹⁹ to self-reported data and scraped Facebook data Acquisti and Gross found a gender gap in cellphone numbers and sexual orientation disclosure. Other personally identifying data, like birthday, class schedule (location), or political views, was shared at similar rates by gender.

Similar to how much of the empirical government surveillance scholarship has taken at face value the political and media claims that only criminals are targeted by mass surveillance, market surveillance scholarship gave a wide birth of latitude to corporate claims of data use. In my opinion, this has limited the research questions and hypotheses academia has asked about privacy concerns. Partly, this limitation was due to the secretive nature of corporate data collection and use practices. Facebook's first privacy policy stated: "No personal information that you submit to Thefacebook will be available to any user of the Web Site who does not belong to at least one of the groups specified by you in your privacy settings" (Opsahl 2010). But the "sample space" of who "any user" could be was expanding (Acquisti and Gross 2006, Litt and Hargittai 2016). The company decided to enlarge its Ivy-league college walled garden to include high schools and employees of selected companies. At the end of 2006, institutional affiliations were no longer needed, and the walled garden model was torn down¹²⁰. After the 2006 expansion of service, the privacy policy partly read:

"Information set to 'everyone' is publicly available information, may be accessed by everyone on the Internet (including people not logged into Facebook), is subject to indexing by third party search engines, may be associated with you outside of Facebook (such as when you visit

¹¹⁹ The questionnaire was not reported but they cite several framings of a list of issues of which privacy, security and questions related to fear of terrorism were prompted alongside other public opinion issues like same-sex marriage, the economy and economic policy in three ways: "How important do you consider the following issues in the public debate?", to more and more specific (e.g., 'How do you personally value the importance of the following issues for your own life on a day-to-day basis?'), and personal ones (e.g., 'Specifically, how worried would you be if [a certain scenario took place]') (Acquisti and Gross 2006, 8).

¹²⁰ Facebook owned Instagram is still a walled garden in that it is completely off limits to the 'public' internet and requires an account to be viewed.

other sites on the internet), and may be imported and exported by us and others without privacy limitations. The default privacy setting for certain types of information you post on Facebook is set to ‘everyone’ [... (Opsahl 2010)]”.

By 2010 the company had broken up its information types into “50 settings and 170 options” for privacy preferences, while its closest “competitor”¹²¹, MySpace, use was rapidly losing users (Jacobsson 2010).

Corporate infrastructure is so central to monitoring that surveillance studies have sometimes called social network surveillance “institutional privacy violations” (Raynes-Goldie 2010). Indeed, advanced democracies’ most visible point of contact with surveillance is commercial, which imbues surveilling technologies with the veneer that consent took place. A “click to agree” box is ticked, even though not every surveillance practice is disclosed, creating the illusion (delusion) that a consenting decision to be a surveillance subject was actively undertaken. The most palpable surveillance comes from the marketplace. The argument goes that no coercion exists because no one forces you to use any particular service. This circumstance juxtaposes the state’s monopoly on using force, which imposes governance conditions, including surveillance of border crossings, tax payments, etc. This argument ignores the political economy of digital services choice and the deliberate deregulation and un-enforcement of anti-trust, which make alternative services and non-participation unreasonable choices for modern life. Additionally, as discussed in chapter 1, networked communications surveillance limits the capacity of any single individual to control information about themselves. These three elements problematize the classical definition of privacy “achieved only by social withdrawal”¹²² as “this is neither practical nor possible” (Metzger and Suh 2017).

¹²¹ Around the time Facebook was being investigated by the FTC for privacy violations, a Wall Street Journal investigation found that MySpace was also sending personally identifiable information to advertisers (Fowler and Steel 2010) so they were not competitors in the sense of supplying a non-surveillant product, but they were positioning themselves to try to compete in terms of (falsely) marketing themselves as more private (Jacobsson 2010).

¹²² Fundamentally, those who are concerned about privacy cannot and should not be forced into exile and ‘go live in the woods’.

Facebook's practices now set "industry standards"¹²³ of data mining, targeted advertising¹²⁴, cross-site tracking, and merging online to purchased offline behavior (e.g., credit card data). These practices have given way to an industry of unregulated data brokers (Valentino-DeVries and Singer-Vine 2012). The onus is put on users, who have to engage in cognitive and time-consuming practices to manage continuously changing categories of privacy settings—an approach Facebook pioneered. Regulators are now scrutinizing this dynamic in the US and Europe. The US's Federal Trade Commissioner Rohit Chopra has defined "dark pattern[s]" as privacy settings having "design features used to deceive, steer, or manipulate users into behavior that is profitable for an online service, but often harmful to users or contrary to their intent" (Chopra 2020, Brignull 2017). The Federal Trade Commission (FTC) characterized the company's privacy practices as "unfair and deceptive" in 2011 (United States of America 2019, 9). Eight FTC charges of violating users' privacy led to a settlement where Facebook submits to independent audits every two years for the next 20 years¹²⁵.

Some of the company's surveillance practices have come to light outside these audits. New York University's political advertising lab research, lawsuit discovery, whistleblowers like Frances Haugen (Facebook), Christopher Wylie, and Brittany Kaiser (Cambridge Analytica), and Congressional hearing testimony produce vital information about one of the biggest firms' surveillance practices. Without such information, researchers operate under asymmetrical information conditions that benefit Data Goliaths' lucrative narrative that users do not care about privacy.

¹²³ Rains and Brunner have criticized the overwhelming focus on Facebook in social network research. But the outsized role of Facebook communication and advertisement power has justified intense academic scrutiny.

¹²⁴ 25% of US digital ad spending in 2020 from 28.2 billion (Statista Research Department 2021), and 84.2 billion dollars from worldwide advertisement revenue (Statista Research Department 2021).

¹²⁵ The company had made \$55 billion in profits and set aside \$7 billion for the fine. When the fine was announced the stock price went up, signaling that markets were comfortable factoring in sporadic fines as a "cost of business". The two Democratic commissioners' dissent construed the fine as "a substantial undervaluation [...] The fact that Facebook's stock value increased with the disclosure of a potential \$5 billion penalty may suggest that the market believes that a penalty at this level makes a violation profitable" (Feiner and Rodriguez 2019).

Researchers have found that the illusion of privacy controls helps incentivize more disclosures because it creates a false sense of security (Brandimarte, Acquisti and Loewenstein 2012, McDonald and Cranor 2010, Metzger and Suh 2017). Not coincidentally, every time Congress has held hearings on Facebook privacy, Zuckerberg has proposed more privacy settings—but has refused to engage in questions around cross-site and ghost profiles of non-users via tracking cookies (Madrigal 2018, Wagner 2018).

Studies about online behavior tend to silo monitored interactions into particular websites instead of considering the whole digital data collection system (Lewis, Kaufman and Christakis 2008). Empirical research ends up monitoring one-off commercial interactions (Svirsky 2019). This tactic leaves aside the impact of cookies, pixels, ghost profiles, and other technologies tracking users once they “exit” websites (Reitman 2011), behavior across devices, and GPS/Bluetooth technologies used to link online behavior to physical behavior (Kwet 2019) and financial data matching.¹²⁶ Experiments on teenagers’ increased awareness of Facebook cookie-tracking techniques led to decreased purchasing due to heightened ad evaluation skepticism (Zarouali, et al. 2017).

The second question of early corporate surveillance studies became known as the “privacy paradox” (Barnes 2006, Acquisti and Gross 2006). It asked why people who want privacy use services that monitor them. The framing of the problem has had an indelible impact on the field. The privacy paradox literature relied on an untested assumption that revealed preferences occur with perfectly competitive supply-side alternatives (surveilled service vs. privacy service). However, the privacy paradox literature never engaged with the fact that these alternatives essentially do not exist. No one advancing the privacy paradox framework problematized that the Web 2.0 companies’ economic model relied on surveillance capitalism for financing. The initial consumer choice was between

¹²⁶ See, for example, how the measurement of concern for state surveillance is artificially constrained to elicit intrusiveness of “laws aimed at protecting national security” in Zureik et al (2010, 173).

participating in surveilled online vs. non-surveilled offline services and not participating vs. withdrawing, but the former option pair has basically disappeared.

The privacy paradox was conceptualized when evidence of corporate surveillance for ad sales was not publicly known. That created another implicit assumption: people's privacy concerns were limited by considerations towards the companies they were interacting with directly. The Wall Street Journal's "What they Know" series conducted original research on the Facebook app cross-site tracking (Wall Street Journal 2010, Wall Street Journal 2010-2012) and the creation of a government dragnet (Angwin 2012). This increased American awareness of the situation a few years before Snowden's revelations but was limited in its reach, and widespread media scrutiny was not the norm pre-Snowden.

By the time the WSJ series was published, the myth of the privacy paradox had taken hold in econ-leaning surveillance studies. The legacy of the privacy paradox research agenda seems hard to shake off. It is currently spawning a slew of "willingness to pay" experiments for privacy (Svirsky 2019, Dienlin and Trepte 2015, Baek 2014, Motiwalla, Li and Liu 2014, Acquisti, John and Loewenstein 2013, Tsai, et al. 2011). These commercial surveillance attitude studies measure whether consumers would sell their data or pay (money) for services if they refuse to hand over their data (Svirsky 2019, 3). They are an extension of the settings-control framework. This research agenda seeks to prove that consumers can be convinced of surveillance capitalism's monetary benefits by experimenting with more explicit data contracts, "nudging", and short-term financial incentives. The privacy paradox and ensuing willingness to pay for research agenda need to assert that "privacy is governed by free choice"; hence people are freely giving up their right to privacy. This logic is critiqued by legal and critical communications scholars, such as Joseph Turow (2023), and I have echoed these concerns. Svirsky's experiment, for example, relies on a 14% drop in refusal to give data to Facebook by *producing* an environment of ignorance. A majority of respondents (64%) refuse to give their profile

data for 0.50 cents in the “full information” conditions. When they are randomized into an environment that excludes information on “the privacy consequences of their choices” by default and asks respondents to “click to find out” what will happen if they take the money”, ‘only’ 40% refuse to hand over the data. How can consent be legitimized if it is acquired with imperfect information? Furthermore, should the onus of information be placed on individuals or the entities who produce, use, and profit from surveillance?

The dominance of settings-control research has also come at the cost of asking about respondents’ attitudes over secondary data markets and data brokers¹²⁷, which are part of the surveillance complex. Data brokers provide no service to users¹²⁸. Their customers are paying for the data; they are not the users generating data. This dynamic has been fundamentally ignored, and obfuscation between users and data customers is rampant in academic studies, media, and public policy. Here the political science field should converge around the question of the conflict of interest between legislators’ willingness to regulate the data brokers they rely on for their political campaigning regarding fundraising and turnout.

While Dinev et al. first thought government surveillance would incentivize trust and e-commerce, post-Snowden awareness of government surveillance is construed by the field as a threat to e-commerce (Hampson and Jardine 2016). In one of the most extensive cross-national studies on market surveillance, Hampson and Jardine frame privacy concerns as causing distrust in services and reliability. For example, consumers distrust negligent merchants who leave financial data unsecured for hackers or snooping governments to access. The illusion of user choice and the lag in public

¹²⁷ Either actively collaborating, actively refusing to protect it, or passively by repeatedly failing to secure it.

¹²⁸ In a twist, the pervasiveness of selling data to brokers for ads has become so entrenched that Internet Service Providers, which are not free services, successfully argued to Congress that they should also be allowed to do it. They stated that because unpaid services have not been prohibited from selling user data, including metadata and monitored browsing data, the FCC’s rule to make consumers opt-in on ISP data sales produced an uncompetitive burden. The Republican-majority Congress was swayed by the arguments and passed a bill deregulating ISPs ability to monetize browsing internet history (Sottek 2017).

disclosure of market surveillance programs is reflected in privacy concern questions that measure a willingness to give up services where there is no usable un-surveilling alternative. For example, Hampson and Jardine ask: “[Do you know] companies that provide free online services often sell your personal data to governments and other companies” and “[d]oes knowing this cause you to use the internet in different ways than you otherwise would, or does it not cause any change in your internet usage?”. Change for what alternative, one might ask?

As everything becomes digitized (IoT) and financed by surveillance capitalism, the idea that anyone can choose the “right” service or withdraw from online surveillance becomes harder to defend as feasible. Even paid apps use surveillance capitalism to multiply their revenue streams (Han, et al. 2020). The implication is that surveillance *and* privacy have ended up being monetized. This conclusion is reflected in Hampson and Jardine’s other question: “How much would you be willing to pay to continue using your favourite online services to ensure that your data was not sold to governments or other companies?” (2016).

This section highlighted how measuring attitudes towards market-exclusive surveillance falls into the trap of assuming choice under a lack of supply by outlining critical corporate surveillance decisions and survey measures of market surveillance concerns.

No one or everyone? Agentless and deputized surveillance concerns

Nissenbaum argues that norms of appropriateness are also breached when *public* datasets (e.g., census data, education records, phone book data, published tweets), created in perfectly appropriate conditions within their respective spheres, are collated. The aggregated data crosses different social spheres when merged, breaching contextual integrity. Her concern for “the problem of privacy in public” (1998) draws on Walzer’s concept of distributive justice: standing in one social sphere (education, healthcare, politics, etc.) should not negatively affect a person’s standing in another sphere (2010, 80). For example, if being illiterate determined your access to the ballot, that would produce distributive injustice. Contextual integrity is maintained when data from one sphere is siloed from others. Paper files under safekeeping by a single institution made this easy, but digitalization increases the ease with which an individual’s distinct profiles are merged across institutions and social spheres. However, as Chapter 1 discussed, the surveillance complex is rife with incentives and coercive mechanisms that increase data flow between actors in each sphere: online service providers and data brokers, federal and local governments, and between public (government) and private (market) spheres. The surveillance complex’s overlapping panopticons and intra-sphere data flow make violations of contextual integrity inevitable.

Perhaps because surveillance attribution is obfuscated in the surveillance complex of advanced democracies, many studies measure privacy concerns with no attribution. In this dissertation, I call these agentless measures “baseline” measures. Dinev et al.’s comparative survey of Americans and Italians exemplifies the issue of a lack of surveillance source attribution¹²⁹ by asking about general data

¹²⁹ They hypothesize Italians would be less concerned about privacy violations because of “communitarian family structure” leads to the “obliteration of personal space”, individualistic Americans. Undermeasured, broad cultural stereotypes aside, there are a number of methodological issues that make replication of this study hard. For example, they sampled Americans in the Southeast of the country (n = 422) and Northern Italians (n= 889) using non-random convenience sampling of student and tech-company workers.

security concerns without specifying who is the third party accessing commercial surveillance data¹³⁰. Their measurements fail to clarify the surveillant entity, so respondents are unclear about whom to be concerned about, if at all concerned.

In this chapter's section, building on Helen Nissenbaum's theory of contextual integrity, I provided a literature review of disparate perspectives analyzing privacy concerns. I discussed the historical reasons for focusing on state or market surveillance sources as mutually exclusive, and I identified crucial limits to their assumptions and operationalization choices. Deputized surveillance blurs the lines between government and market surveillance, directly impacting public opinion and clarity of context. I hypothesize that attitudes towards surveillance policies will be distinct along the source attribution. In particular, deputized surveillance should produce a dimension of concern distinct from government-exclusive and market-exclusive surveillance practices because it violates expectations of contextual integrity within the two found in the state-exclusive and market-exclusive dimensions of surveillance. In the following section, I provide a battery of survey questions and explain how these allow me to test whether privacy concerns fall along different dimensions (government, corporate, and deputized, as well as non-attributed) when the source and uses of surveillance are made explicit, with a particular focus on when contextual integrity is violated. By measuring opinions of policies from different sources concurrently, I can test how associated or distant each source of surveillance is from one another.

Methods and Data

I hypothesize that attitudes towards surveillance policies will be distinct along the source attribution. In particular, deputized surveillance should produce a distinct dimension because it violates

¹³⁰ I am concerned that the information I submit on the Internet could be misused; I am concerned about submitting information on the Internet, because of what others might do with it; I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee; I am concerned that my private information can show up on the Internet. The authors lack measures on government's ability to use corporate data to prevent financial fraud effectively.

expectations of contextual integrity found in the state-exclusive and market-exclusive dimensions of surveillance. To test this, I conducted a survey of 1,493 respondents Americans, asking them about their attitudes towards different surveillance sources and practices using a 19-item questionnaire¹³¹. The survey was administered between August 9 to 25, 2021; participants were recruited and paid by LUCID Theorem¹³². The average completion time was 17 minutes (median = 11:30 minutes, 3rd quartile = 16:30 minutes). Previous validation exercises have found that LUCID quota samples approximate nationally representative probability samples regarding demographic characteristics and survey experiment effects (Coppock and McClellan 2019). The sample for this survey approximates the marginal distributions of key demographic attributes in terms of age, gender, ethnicity, and region (see Technical chapter documentation). Partisanship is not considered in the recruitment quota. However, analysis of responses shows the sample leans left compared to Gallup polls conducted from August 2 to 17. It does so at the cost of Independents (-10 percentage points compared to Gallup's distribution) since the percent of self-identified Republicans is almost identical to the period's national average (27% in the sample vs. 28% Gallup).

Questions were presented in 4 blocks, randomized within blocks to minimize order effects in the perception of invasiveness severity. I also randomized the presence of two questions in a mutually exclusive way (50% of the sample saw one of the two questions). The two questions describe location data monitoring conducted by the government in public spaces or by companies in their services. These responses are compared to the deputized form to directly assess the role of source and violation of contextual integrity in attitudes towards location data monitoring.

¹³¹ Analysis of the survey does not suggest that respondents stopped answering at any one given question, including the start of the surveillance blocks. However, it is possible that the most anti-surveillance Americans are unwilling to disclose their financial information to a third party to be paid for their opinions, or to have their opinions on issues (surveillance or not) monitored and recorded. This means that if we are systematically omitting the most anti-surveillance Americans, our estimates are conservative.

¹³² The company was bought by CINT in 2022.

The questions were designed with a balanced positive (“should”) and negative (“should not”) phrasing in mind to minimize polarity bias in wording effects, as is standard survey writing practice (Holleman, et al. 2016). The response choices are a 4-point Likert scale: strongly disagree, somewhat disagree, somewhat agree, and strongly agree, and the directionality of the answer for each question is ordered in increasing privacy *concerns*. Respondents unwilling to disclose their preferences can leave responses blank, with no prompts to reconsider picking a choice. I decided not to include a neutral choice. First, the questions capture attitudes towards normative scenarios (should X do Y)¹³³ where something either happens or does not. A fifth neutral option, suggesting “don’t know”, would introduce noise if it incentivizes interpreting a question as one of fact instead of preference. A lack of a neutral option also encourages respondents to engage with the normative question substantively, especially if they are pondering a policy for the first time, preventing me from suggesting to them shirking, although they can leave a response blank. The somewhat options capture weakly held views instead of providing respondents with binary should/should not response options. A discussion of each block’s themes is presented after the literature review.

Design and Question wording

All questions were presented in random order within the survey “blocks” on the Qualtrics website where the survey is answered. An “[R]” at the end of a question implies the answer directionality is reverse-coded to reflect increasing concern response orders. The first battery should capture privacy concerns unattached to any particular policy or source. They replicate common survey questions and serve as a baseline for general privacy concerns (Hargittai and Marwick 2016). I begin with the prompt: We would like to know how you feel about privacy when you are online.

I am concerned about online privacy (Baseline_Concerned).

Information online is used in ways people cannot predict (Baseline_Unpredictability).

¹³³ The only question that *could* be misinterpreted as a “knowledge” question asks respondents about their perception whether news coverage of misused data has increased.

Ultimately, people are responsible for keeping their online data private.

(Baseline_Responsibility) [R].

Reports of misused online data (stolen, leaked, hacked) have been more frequent in the past 12 months (Baseline_Misuse)

The second block's theme is market-exclusive practices that use data for advertising and consumer tracking, recently dubbed "surveillance capitalism" (Zuboff 2019). All respondents saw the first 5 questions, and half the sample was randomized into additionally seeing the question regarding the market location data to gain comparative insight without burdening respondents with two additional, similar questions. I try to prompt people to think about online companies specifically, by starting the prompt with a message that includes general examples, but not specific brands, to avoid tainting responses with feelings towards specific Data Goliaths. It reads (with bold format in survey):

Think about **online commercial services**, like internet providers, search engines, websites, and apps.

Do you agree or disagree that they:

Should not have a legal duty to keep the data they collect from being stolen, hacked or leaked.
(Market_Safety)[R]

Should not make money from selling people's online activity data. (Market_Money)

Should take users' information to provide personalized content. (Market_Content_Change)[R]

Should keep track of what users post and delete it based on "community standards".
(Market_Censor)[R]

Should not show different services and prices based on the information they collect on users.
(Market_Service_Change)

Companies should be allowed to collect location data when visiting private places.
(Market_Geolocation)[R, displayed randomly to 50% sample]

The third block's themes centered around state-exclusive surveillance, broadly bringing in multiple levels and branches of government to reflect the decentralized nature of law enforcement in the US.

Three of the four items shown to everyone explicitly relate to judicial elements (police, judges, investigations). It reads, Thinking about the **government**, do you agree or disagree that:

Federal agencies and state officials should be able to exchange data on citizens.
(Government_Share)[R]

The local police should be able to access anyone's government records without a warrant.
(Government_localAccess) [R]

The government should not have to ask a judge for access to online information about people.
(Government_Warrantless)[R]

Citizens should be notified by the government if their online data has been used in an investigation. (Government_Disclose)

The government should be allowed to collect location data when visiting public places.
(Government_Geolocation)[R, displayed to remaining 50% of sample]

Lastly, I presented practices that require deputation through market-state sharing and collaboration of data monitoring and policing. It builds on the two previous batteries, where people were prompted to think of each actor independently. I prompt them to think of their joint efforts by asking, "Now, think about the **government and commercial online services** like internet service providers, websites and apps. Do you agree or disagree with the following policies?"

Online services should monitor people who break American laws. (Deputized_MMonitor)[R]

Online services should report people who break laws to the government. (Deputized_MReport) [R]

The government should monitor online behavior such as social media posts. (Deputized_GMonitor)[R]

The government should be able to track location data from online services.
(Deputized_GLocation)[R]

Results

Two research questions derived from Nissenbaum's norms of appropriateness theory drive the chapter: Does contextual integrity violation produce different dimensions of privacy concern? The source and purpose of surveillance should structure the dimensions of privacy concerns. Is deputation

a distinct dimension of privacy concern? I hypothesized that because deputation violates contextual integrity of privacy, this should produce a separate privacy concern dimension, different from all the other policies of the surveillance complex. I use Principal Components Analysis (PCA) to answer those questions. This statistical analysis tool uncovers principal components, i.e., new dimensions or “variables” that summarize many responses into groups. All survey questions have their response distributions described in the Technical Chapter of the dissertation. However, in the next subsection I take some space to describe deputized surveillance response distributions and to contrast distributions from other dimensions that might be of particular interest.

Univariate distributions

Lower average scores per dimension (0, 1) reflect disagreement with the surveillance policy while higher scores (2, 3) reflect agreement supporting the policy. I sort the graph by ascending privacy concerns, excluding the baseline measure (placed to the left). The middle point of the scale is highlighted by the red horizontal line.

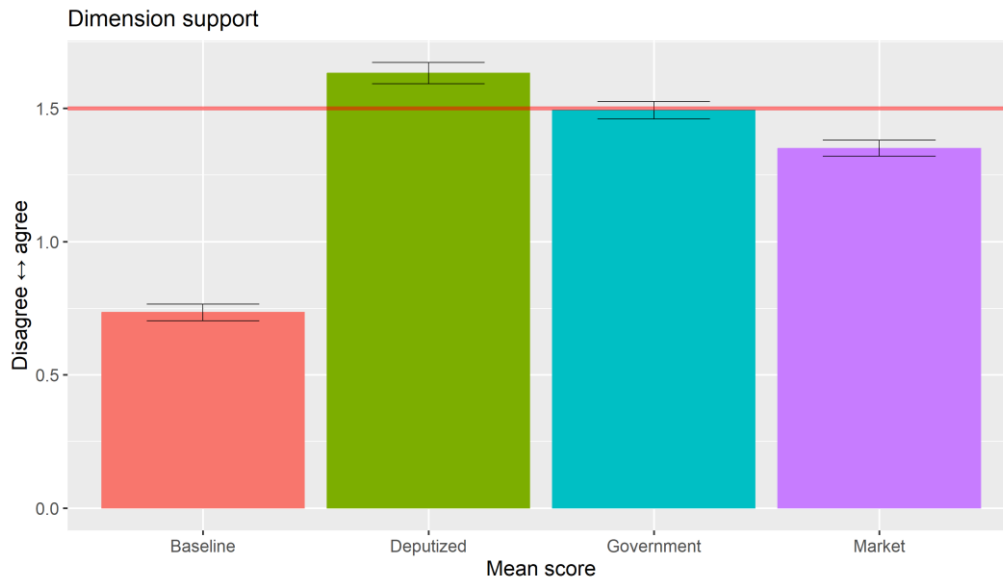


Figure 5 Average concern level per dimension

Figure 5 illustrates the average responses calculated from the four batteries’ responses grouped by source of surveillance. Lower average scores per dimension (0, 1) reflect disagreement with the surveillance policy while higher scores (2, 3) reflect agreement supporting the policy. I sort the graph by ascending privacy

concerns, excluding the baseline measure (placed to the left). The middle point of the scale is highlighted by the red horizontal line.

The average response rates in Figure 1 helps us anticipate several things. First, all the categories have statistically significant differences in means (95% CI)¹³⁴, so average concern levels for the different batteries are distinct. Second, Nissenbaum's theory views contextual integrity violations negatively. This implies that deputized surveillance should be rejected at higher rates because contextual integrity is breached. However, the data shows this is the battery that elicits the least rejection (I discuss the differences in this battery's responses in the next paragraph). This may be the case because deputized surveillance obfuscates who is responsible for surveillance decision-making and data use. The mechanism by which this fosters lower rates of concern, instead of a higher concern echoing normative expectations, encourages further study. The fact that average support for deputation is higher than either of the two dimensions' independent responses justifies my observation that deputized surveillance seems to be more than the sum of its parts.

¹³⁴ Table data y-axis disagree to agree average (0-3)

Battery	Mean	ymin	ymax
Baseline	0.73	0.70	0.765
Deputized	1.63	1.59	1.67
Government	1.49	1.46	1.53
Market	1.35	1.32	1.38

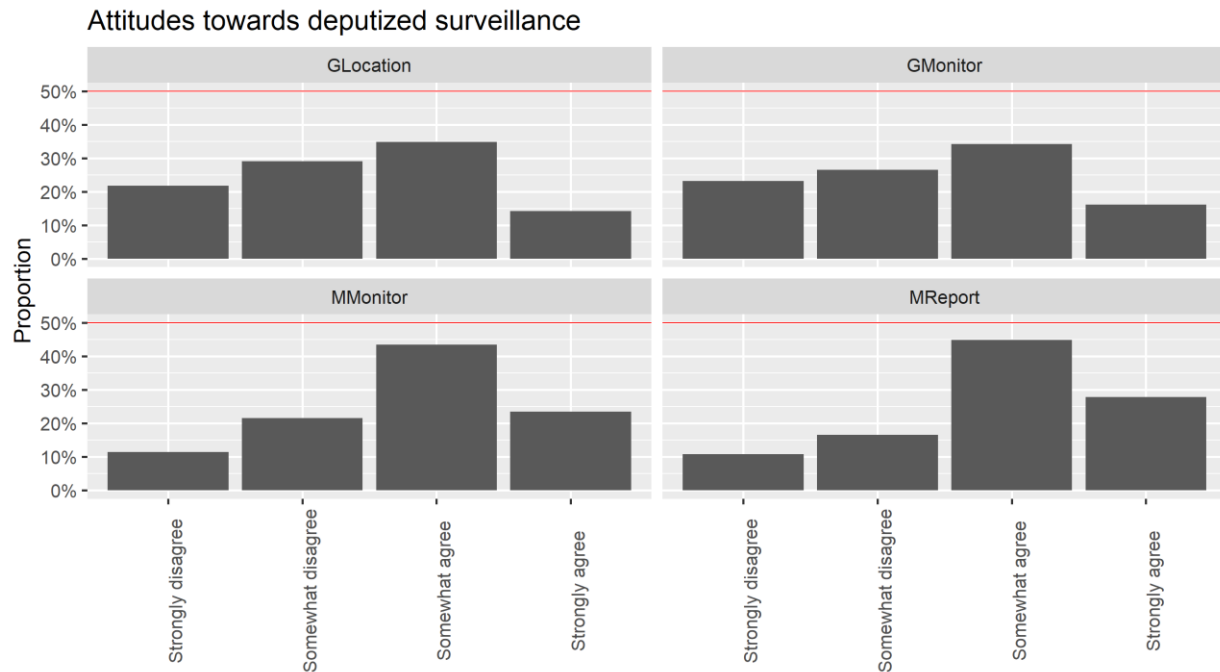


Figure 6 Responses of deputized policies

Figure 6 visualizes the individual response means of deputized policies, the 50% threshold is lined in red. The hard policies that demand more elaborate involvement from online services in surveillance were the most supported. I report the combined response categories of support (strongly and somewhat agree) and rejection (strongly and somewhat disagree) for deputized policies (the technical chapter 5 has all response distributions). A duty for the online services to report to law enforcement violations of the law (MReport) produced the most support (72% agree somewhat or strongly), followed by the deputized mandate to monitor (MMonitor) without a duty to report (66.8%). There is a drastic drop in soft surveillance policies' acceptance (50.7%) when the government is the one monitoring company-collected online data (GMonitor), and agreement (barely) drops below the majority (49.2%) if the government is tracking location data from online services (GLocation)¹³⁵.

¹³⁵ For comparison: the government-exclusive geolocation in public places produced a similar 49.2% agreed to it. Market-exclusive geolocation ("Companies should be allowed to collect location data when visiting private places") produced the least support (38.0%). This is surprising given it is a widespread practice that is used to identify user devices, link online

Figure 8 in the appendix summarizes visually the following data collapsing agree and disagree responses for all variables discussed in this chapter.

Dimensions

In this section I explore the feasibility of creating a single privacy concern measure with the survey responses, compared to a multi-dimensional one. Further, I expect the response dimensions uncovered to be shaped along source attribution: baseline (agentless), government, market, and deputized surveillance. Beyond the literature's 4-way focus' split, I used three empirical tests to conclude that a 4-dimension PCA test produced the most appropriate model. I showcase the PCA analysis in the next paragraph. The preliminary tests that led to a 4-dimension PCA are documented in the Appendix.

The PCA method is advantageous when the variables within the data set are highly correlated, indicating redundancy in the data. The PCA findings are supported by pairwise correlation tests showing higher correlations between the deputized surveillance battery responses and weaker correlations across non-deputized and deputized measures' responses.

A preceding correlation matrix modeling all the survey item associations suggested that 4 dimensions would be appropriate. See the Appendix's Figure 10 and Figure 11 for a visual test of the dyadic correlations and an accompanying discussion. Second, I produced a scree plot (Appendix Figure 9) that helps to establish a minimum number of dimensions. There is no uniformly-accepted way to decide how many principal components are "enough" (Kassambara 2017), but there is consensus that there should be enough dimensions to explain at least 80% of the response variation. The scree plot suggested that at least 3 dimensions would be necessary. Scree plots and PCA results are often used to inform how to aggregate many items into grouped dimensions as a data reduction

searches and offline purchases. This gap is also noteworthy since there is an expectation that Americans are more open to market surveillance than governmental.

method. However, my goal is not to minimize data but to find the response commonalities that form *multiple* discrete dimensions. Thus, the substantive response associations are more important than the specific number of dimensions.

With the first two analyses in mind, I calculated PCA tests for 3 dimensions, 4 dimensions, and 5 dimensions using the psych package in R¹³⁶. I compared how they performed substantively against the theory of contextual integrity, which emphasizes the source and use of data. The hypothesis is that deputized surveillance is a distinct dimension. I also compared each PCA's metrics regarding the distribution of proportion explained by each dimension and cumulatively. Table 1 displays the results of 4-dimension PCA ("nfactors = 4" argument in the function) from the four batteries' responses (18 items¹³⁷), which I considered to be the 'best' performing in the two aforementioned terms. The appendix includes results for 3 dimensions (Table 3).

I facilitate the analysis of the PCA loadings by formatting in bold the elements of each rotated component (RC in the table) that are highly associated¹³⁸. As a robustness check, I also tested alternative hypotheses that 1, 3, and 5 dimensions would be appropriate. The PCA results suggest that 4 dimensions are the most appropriate, although regarding hypotheses 3 and 5, dimensions do not

¹³⁶ The psych package principal function, which uses varimax rotation (Revelle 2021, 298) maximizes the sum of the variance of the squared loadings, i.e. the correlations between variables and factors (Glen 2022).

¹³⁷ Half the survey was randomized into seeing one of two additional location questions: Market location or government location surveillance. I reproduced the PCA with 19 items for each type of location in the appendix. Principal component analysis cannot be run on missing data, as it is estimating the variable combinations that maximize the explained variance in each new dimension (component, variable). So I have to subset respondents who were given the government location question from rest of the respondents, who were shown the market location question. The inclusion of the additional randomized location policy should not affect the number of dimensions of the PCA. It should only moderately impact the estimates and the amount of variation explained. A fourth PCA with 5 factors (18-items) is also presented in the appendix as a robustness check to this claim (Table 6).

¹³⁸ The psych package does not allow for an unspecified nfactors argument. Rencher and Christensen suggest an 80% explained variance cutoff point, which is arrived at with $RC1+RC3+RC2 = 0.82$ in table 1 (2012, 423). Alternatively, the scree plot orders eigenvalues from largest to the smallest. The number of components is determined at the graph's "elbow", the point beyond which the remaining eigenvalues are all relatively small and of such comparable size as to provide little additional value (Jolliffe 2002, Peres-Neto, Jackson, and Somers (2005)). In the appendix, Figure 9 displays a 10-dimension scree plot (10 dimensions is the default for exploratory testing scree plots). It suggests aggregating the items into at least three dimensions as an acceptable data reduction method. My goal is not to minimize data but to find the response commonalities that form *multiple* discrete dimensions, so the substantive response associations are more important than the specific number of dimensions. The elbow encompasses three dimensions, which is consistent with what we would conclude using Rencher and Christensen's guidepost.

change the core finding that the deputized surveillance measures hang together in one cluster and are distinct from all other item responses.

Principal Components Analysis							
Call: psych::principal(r = ., nfactors = 4, rotate = "varimax")							
Standardized loadings (pattern matrix) based upon correlation matrix							
	RC1	RC2: Deputized	RC3: baseline	RC4	h2	u2	com
Baseline_Concerned	0.05	0.01	0.73	0.19	0.57	0.43	1.1
Baseline_Unpredictability	0.04	0	0.74	0.18	0.59	0.41	1.1
Baseline_Responsibility	0.18	-0.15	-0.41	-0.03	0.22	0.78	1.7
Baseline_Misuse	0.07	0.02	0.73	0.16	0.57	0.43	1.1
Market_Safety	0.71	0.09	0.01	-0.07	0.52	0.48	1.1
Market_Money	0.07	0.07	0.24	0.66	0.5	0.5	1.3
Market_Content_Change	0.67	-0.14	0.09	-0.15	0.5	0.5	1.2
Market_Censor	<i>0.54</i>	-0.31	0.1	-0.32	0.5	0.5	2.4
Market_Service_Change	-0.26	-0.03	0.2	0.59	0.46	0.54	1.6
Government_Share	<i>0.44</i>	-0.34	-0.26	0.31	0.47	0.53	3.5
Government_localAccess	0.67	-0.29	-0.11	0.26	0.62	0.38	1.8
Government_Warrantless	0.69	-0.24	-0.03	0.22	0.59	0.41	1.5
Government_Disclose	0.17	0.11	0.24	0.58	0.43	0.57	1.6
Deputized_MMonitor	-0.06	0.84	0.05	0.12	0.72	0.28	1.1
Deputized_MReport	-0.07	0.81	0.08	0.17	0.69	0.31	1.1
Deputized_GMonitor	-0.44	0.65	0.02	-0.06	0.62	0.38	1.8
Deputized_GLocation	-0.47	0.62	0.07	-0.18	0.65	0.35	2.1
	RC1	RC3	RC2	RC4			
SS loadings	2.95	2.58	2.06	1.63			
Proportion Var	0.17	0.15	0.12	0.1			
Cumulative Var	0.17	0.33	0.45	0.54			
Proportion Explained	0.32	0.28	0.22	0.18			
Cumulative Proportion	0.32	0.6	0.82	1			
Mean item complexity = 1.6							
Test of the hypothesis that 4 components are sufficient.							
The root mean square of the residuals (RMSR) is 0.07 with the empirical chi-square 1879.27 with prob < 0							
Fit based upon off-diagonal values = 0.92							

Table 1 18-item Principal Components Analysis

The most important finding from Table 1 is that deputized surveillance attitudes are a distinct dimension. Robustness checks on this conclusion are supported by additional PCAs in the appendix,

with varying nfactor settings, support this conclusion. The elements from RC2 all belong to the deputized surveillance battery of questions. They “hang together”, meaning there is no cross-loading from attitudes toward government-exclusive, market-exclusive, or baseline surveillance responses. The factor loadings for the deputized dimension RC2 range from 0.84 to 0.65, which are strong associations. The response distributions for the deputized surveillance dimension explain nearly 30% of the cumulative 18 items. So, I find evidence for my two hypotheses: there are multiple dimensions of privacy concerns, and importantly, attitudes towards deputation of surveillance are distinct from all other forms of surveillance. These findings support Nissenbaum’s theory that “contextual integrity” boundaries—and their violations— shape privacy concerns (2010).

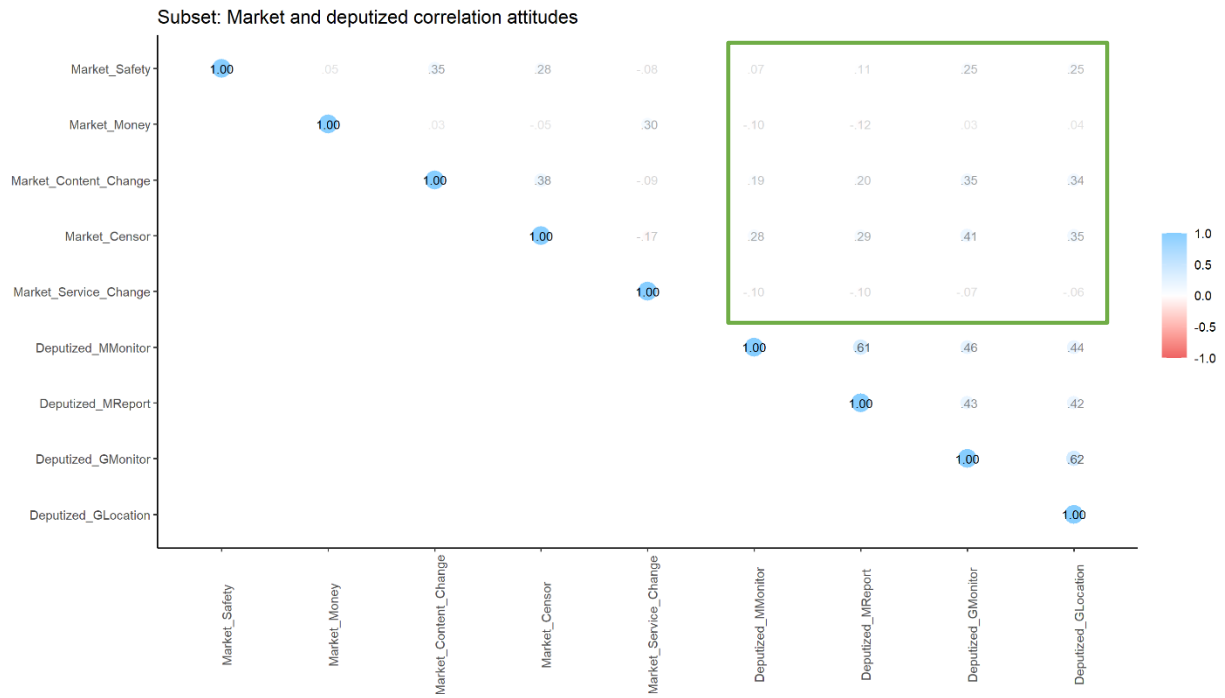
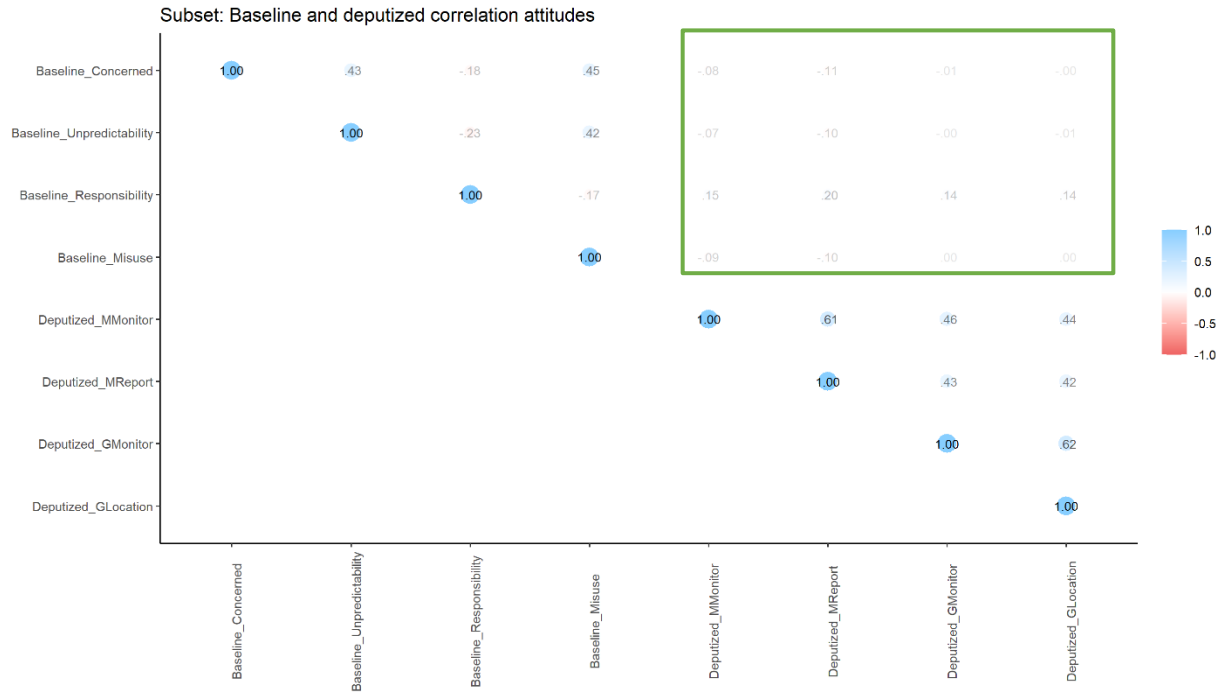
Below, I discuss the PCA results for the other forms of surveillance, as this relates to the literature’s binary between government surveillance and surveillance capitalism. The first dimension explains 32% of the variation. There is some cross-loading between some market-exclusive and government-exclusive attitudes—but importantly, there is no overlap between these and the deputized surveillance attitudes. The questions with cross-loading responses in the first dimension (RC1) are:

Should not have a legal duty to keep the data they collect from being stolen, hacked or leaked.
(Market_Safety)[R]
Should take users’ information to provide personalized content. (Market_Content_Change)[R]
The local police should be able to access anyone’s government records without a warrant.
(Government_localAccess) [R]
The government should not have to ask a judge for access to online information about people.
(Government_Warrantless)[R]

We might ascribe this dimension as one of a legal duty to disclose, but the most explicit deputized duty to report does not load onto this dimension. Also, personalization of content (content_change, which is what fuels surveillance capitalism) also loads into this dimension despite having little relation to a duty to disclose. The cross-loading issue is eliminated if the PCA analysis is set to nfactors=5 (see Table 6 in the appendix). The third dimension (RC3), which I call “baseline”,

has widely used questions that lack surveillance attribution and provides around 20% of the explanation of the 18 items. An individual's responsibility to protect their data from surveillance, drawn from Hargittai and Marwick's work with youth (2016), is very weakly associated with the other three commonly used measures when I conduct paired correlations (concerned -0.18, unpredictability -0.23, misuse -0.17).

To further justify my conclusion that deputized surveillance attitudes are distinct and should not be considered an extension of either government or market surveillance practices, I present dyadic correlations between different batteries. I subset the correlations focusing on comparing the deputized battery to the others and highlight the space where these intersect to draw attention to the combinations of interest. In the Appendix, Table 7, Figure 10, and Figure 11 present data for all the response pair combinations, although the size of the data can be unwieldy.



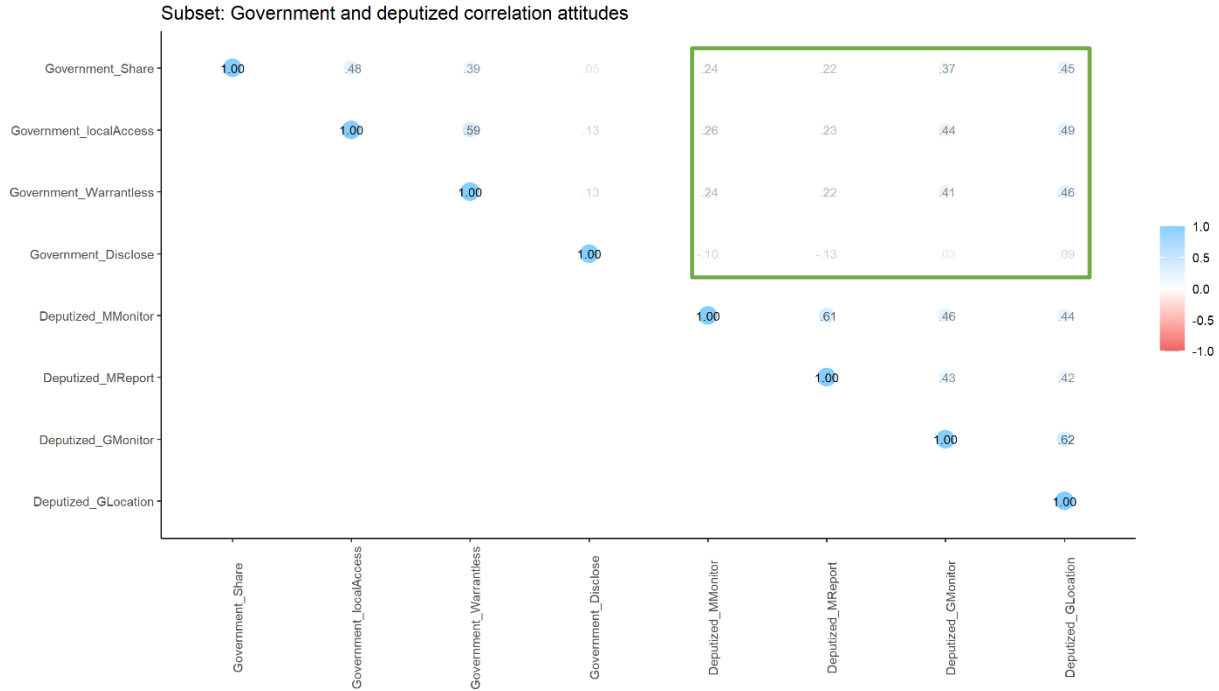


Figure 7 Pairwise subsetting correlational heatmap

Figure 7c which homes in on the correlation between the government battery responses and the deputized surveillance responses has the highest correlations, which are moderately strong (± 0.31 to 0.49) for the two soft deputized surveillance questions. Figures 7b and 7a have the correlations between deputized surveillance and the market, and baseline questions respectively. Their inter-battery paired correlation estimates are weaker and the weakest, respectively. Location access (the government should be able to track location data from online services) has higher correlation dyads to 3/4 government surveillance questions¹³⁹, and the government's monitoring of online behavior such as social media posts has a similar pattern with slightly less strong correlation estimates. However, the deputized surveillance questions still have comparable and higher response correlations, further confirming the PCA warning against subsuming this phenomenon into any other dimension, or creating a single measure.

¹³⁹ Federal agencies and state officials should be able to exchange data on citizens. (Government_Share)[R], The local police should be able to access anyone's government records without a warrant. (Government_localAccess) [R], The government should not have to ask a judge for access to online information about people. (Government_Warrantless)[R].

Discussion and Conclusion

This chapter presented findings from an original and nationally representative survey of Americans' attitudes toward surveillance ($n=1,493$). In line with Nissenbaum's norms of appropriateness theory, I hypothesized that, given the unique context in which deputized surveillance blurs government surveillance by passing it on as commercial surveillance, respondents would manifest a unique dimension of privacy concern towards it, compared to government and market-exclusive surveillance. I hypothesized that deputized surveillance should result in a distinct attitude dimension. I also hypothesized that the remaining surveillance practices would fall into discrete dimensions along the lines of attribution on who collects and uses the data, including a distinct dimension when policies have no evident surveillant agent (baseline).

I produced an original 18-item survey on a representative sample of 1,493 Americans drawing from existing literature and contributing to the empirical gaps in the literature, which I outlined in the Theory section. The policies focused on online monitoring, which updates many of the previous measures of attitudes—particularly around government surveillance—to more current forms of surveillance. The survey also innovates by moving away from government and media frames that only criminals are exposed to surveillance. They emphasize that, technologically and legally, mass monitoring is the status quo. My measures allow me to capture attitudes towards existing, instead of idealized, policies deployed by governments and corporations, on their own and through deputation.

Using Principal Component Analysis of the data, I tested my hypotheses. PCA led me to reject the null hypothesis that all privacy concerns can be collapsed into a single dimension, which is supported by pairwise correlation analysis. The results show there are statistically at least three, although a strong case is made for four, and there are reasons to continue research on whether there might be up to five dimensions. Importantly, regardless of the dimension specification used in the PCA (see Appendix), deputized surveillance attitudes are markedly distinct from the baseline “general”

privacy attitudes and market and government surveillance. The survey analysis supports the hypothesis that measuring “general” privacy attitudes with inexplicit surveillance sources cannot substitute for attitudes toward government-exclusive surveillance, market-exclusive surveillance, or deputized surveillance. Thus, a second takeaway should be a strong warning against collapsing all sorts of surveillance practices into a single averaged index.

In Chapter 3, I take a deep dive into the deputized surveillance dimension and the mechanisms by which attitudes towards these policies either become unstable or remain steadfast. In particular, I put forward two hypotheses about acceptance and rejection of deputized policies, building on the hard/soft theory, and intergroup dynamics. In a pre-registered experiment, I compare attitudes towards the hardest policy (duty to report, MMonitor variable) and softest (government access to online services’ geolocation data, GLocation). These policies ended up eliciting the most and least support within the deputation battery. The chapter considers how the MMonitor variable’s mention of “breaking the law”, a cornerstone of narratives that reframe mass surveillance as producing targeted law enforcement, begs the question whether respondents want to punish some groups more than others for law breaking and how their prior dislike influences acceptance of mass surveillance compared to deputized policies that minimize this dynamic.

Bibliography

- Acquisti, Alessandro, and Ralph Gross. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." *Privacy enhancing technologies*. Berlin: Springer. 429.
- Acquisti, Alessandro, Leslie K. John, and George Loewenstein. 2013. "What Is Privacy Worth?" *Journal of Legal Studies* 42: 249-274. doi:0047-2530/2013/4202-0009.
- Adcock, Robert, and David Collier. 2001. "Measurement Validity: A Shared Standard for Qualitative and Quantitative Research." *The American Political Science Review* 95 (3): 529-546. Accessed November 17, 2019. <https://www.jstor.org/stable/3118231>.
- Albertson, Bethany, and Shana Kushner Gadarian. 2015. *Anxious politics: democratic citizenship in a threatening world*. Cambridge: Cambridge University Press.
- Angwin, Julia. 2012. "U.S. Terrorism Agency to Tap a Vast Database of Citizens." *The Wall Street Journal*, December 13. Accessed January 14, 2022. <https://www.wsj.com/articles/SB10001424127887324478304578171623040640006>.

- Angwin, Julia, Terry Parris Jr., and Surya Mattu. 2016. "Facebook is quietly buying information from data brokers about its users' offline lives." December 30. Accessed December 2017. <http://www.businessinsider.com/facebook-data-brokers-2016-12>.
- Asher Hamilton, Isobel. 2022. *Wordle tracks you more now than The New York Times owns it*. February 18. Accessed March 06, 2022. <https://www.businessinsider.com/wordle-trackers-ads-new-york-times-ownership-2022-2>.
- Baek, Young Min. 2014. "Solving the privacy paradox: A counter-argument experimental approach." *Computers in Human Behavior* 38: 33-42. Accessed March 02, 2019. doi:10.1016/j.chb.2014.05.006.
- Ball, Kirstie, Kevin Haggerty, and David Lyon, . 2012. *Routledge Handbook of Surveillance Studies*. Abingdon, Oxon: Routledge.
- Barnes, Susan B. 2006. "A privacy paradox: Social networking in the United States." *First Monday* 11 (9). https://firstmonday.org/article/view/1394/1312_2.
- Bauman, Zygmunt, and David Lyon. 2012. *Liquid Surveillance: A Conversation*. Cambridge: Polity.
- Biddle, Sam. 2022. "Facebook Engineers: We Have No Idea Where We Keep All Your Personal Data." *The Intercept*, September 07. <https://theintercept.com/2022/09/07/facebook-personal-data-no-accountability/>.
- boyd, danah. 2014. *It's complicated: the social lives of networked teens*. New Haven: Yale University Press.
- Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein. 2012. "Misplaced Confidences: Privacy and the Control Paradox." *Social Psychological and Personality Science* 4 (3): 340-347. doi:10.1177/1948550612455931.
- Brignull, Harry. 2017. April 8. Accessed January 13, 2022. <https://www.darkpatterns.org/types-of-dark-pattern/privacy-zuckering>.
- Byler, Darren. 2022. *In the camps: China's high-tech penal colony*. Durham: Duke University Press.
- Canadian Cultural Mosaic Foundation. 2020. *Why "proactive policing" is counterintuitive*. August 08. Accessed September 14, 2022. <https://www.canadianculturalmosaicfoundation.com/blog/why-proactive-policing-is-counterintuitive>.
- Chan, Anson. 2022. *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*. June 16. Accessed October 3, 2022. <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>.
- Chopra, Rohit. 2020. *Statement of Federal Trade Commissioner Robit Chopra Regarding Dark Patterns in the Matter of Age of Learning, Inc*. Statement, Federal Trade Commission, Washington D.C.: United States of America government. Accessed January 13, 2022. https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abc_mouse_-_rchopra_statement.pdf.
- Citron, Danielle Keats, and David C. Gray. 2013. "Addressing the Harm of Total Surveillance: a Reply to Professor Neil Richards." *Harvard Law Review*, 262-274.
- Cohn, Cindy, Matthew Guariglia, Edward Snowden, and Alexis Hancock. 2021. *EFF30 Fireside Chat: Surveillance, with Edward Snowden*. May 05. Accessed June 16, 2022. https://www.youtube.com/watch?v=jxVpQHTyqKo&ab_channel=EFForg.
- Connors, Elizabeth C., Yanna Krupnikov, and John Barry Ryan. 2019. "How Transparency Affects Survey Responses." *Public Opinion Quarterly* 83: 185–209.
- Coppock, Alexander, and Oliver A. McClellan. 2019. "Validating the demographic, political, psychological, and experimental results obtained from a new source of online survey respondents." *Research & Politics* 6 (1): 1-14. doi:10.1177/2053168018822174.

- Cox, Joseph. 2022. *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*. May 03. Accessed June 20, 2022. <https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood>.
- Davies, Harry. 2015. *Ted Cruz using firm that harvested data on millions of unwitting Facebook users*. December 11. Accessed December 11, 2015. <http://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data>.
- Davis, Darren W., and Brian D. Silver. 2004. "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America." *American Journal of Political Science* 28-46.
- Dienlin, Tobias, and Sabine Trepte. 2015. "Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors." *European Journal of Social Psychology* 285-297. doi:10.1002/ejsp.2049.
- Dinev, Tamara, and Paul Hart. 2005. "Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact." *International Journal of Electronic Commerce* 10 (2): 7-29. doi:10.2753/JEC1086-4415100201.
- Dinev, Tamara, and Paul Hart. 2004. "Internet privacy concerns and their antecedents - measurement validity and a regression model." *Behaviour & Information Technology* 23 (6): 413-422. doi:10.1080/01449290410001715723.
- Dinev, Tamara, Massimo Belotto, Paul Hart, Vincenzo Russo, Ilaria Serra, and Christian Colautti. 2006. "Internet users' privacy concerns and beliefs about government surveillance: An Exploratory Study of Differences Between Italy and the United States." *Journal of Global Information Management* 14 (4): 57-93.
- Fang, Lee. 2022. *Major media outlets that use invasive user tracking are lobbying against regulation*. February 1. <https://theintercept.com/2022/02/01/surveillance-data-collection-ads-news-media/>.
- Feathers, Todd, Simon Fondrie-Teitler, Angie Waller, and Surya Mattu. 2022. *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*. June 16. Accessed June 20, 2022. <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>.
- Federal Trade Commission. 2019. *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*. Press Release, Washington D.C.: United States of America government. <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.
- Federal Trade Commission. 2019. *FTC Sues Cambridge Analytica, Settles with Former CEO and App Developer*. Press Release, Washington D.C.: United States of America government. <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer>.
- Feiner, Lauren, and Salvador Rodriguez. 2019. "FTC slaps Facebook with record \$5 billion fine, orders privacy oversight." *CNBC*, July 24: <https://www.cnn.com/2019/07/24/facebook-to-pay-5-billion-for-privacy-lapses-ftc-announces.html>.
- Fischer, Sara. 2020. *Exclusive: New York Times phasing out all 3rd-party advertising data*. May 19. Accessed March 06, 2022. <https://www.axios.com/new-york-times-advertising-792b3cd6-4bdb-47c3-9817-36601211a79d.html>.
- Foucault, Michel. 1995. *Discipline and Punish: The Birth of the Prison*. Second Edition. Translated by Alan Sheridan. New York: Vintage Books, Random House.
- Fowler, Geoffrey A., and Emily Steel. 2010. "MySpace, Apps Leak User Data." *The Wall Street Journal*, October 23. Accessed January 14, 2022. <https://www.wsj.com/articles/SB10001424052702303738504575568460409331560>.

- Franceschi-Bicchierai, Lorenzo. 2022. "Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document." *Motherboard*, April 26. <https://theintercept.com/2022/09/07/facebook-personal-data-no-accountability/>.
- Friedewald, Michael, Marc Lieshout, Sven Rung, Merel Ooms, and Jelmer Ypma. 2014. "Privacy and Security Perceptions of European Citizens_ A Test of the Trade-Off Model." *9th Privacy and Identity Management for the Future Internet in the Age of Globalisation*. Patras: Springer. 39-53. doi:10.1007/978-3-319-18621-4_4.
- Fuchs, Christian. 2015. "Social media surveillance." In *Handbook of Digital Politics*, edited by Stephen Coleman and Deen Freelon, 395-414. Cheltenham: Edward Elgar Publishing.
- Garcia, Blake E., and Nehemia Geva. 2016. "Security Versus Liberty in the Context." *Terrorism and Political Violence* 48: 30-48. doi:10.1080/09546553.2013.878704.
- Gellman, Barton. 2020. *Dark mirror: Edward Snowden and the American surveillance state*. New York: Penguin Random House.
- . 2020. *Inside the NSA's Secret Tool for Mapping Your Social Network*. May 24. Accessed September 13, 2021. <https://www.wired.com/story/inside-the-nsas-secret-tool-for-mapping-your-social-network/>.
- Glen, Stephanie. 2022. *Varimax Rotation: Definition*. Accessed January 18, 2022. <https://www.statisticshowto.com/varimax-rotation-definition/>.
- Goldhar, Joel D., and Mariann Jelinek. 1983. "Plan for Economies of Scope." *Harvard Business Review*, November. <https://hbr.org/1983/11/plan-for-economies-of-scope>.
- Hampson, Fen Osler, and Eric Jardine. 2016. *Look who's watching: surveillance, treachery, and trust online*. Waterloo: Centre for International Governance Innovation.
- Han, Catherine, Irwin Reyes, Álvaro Feal, Joel Reardon, Primal Wijesekera, Narseo Vallina-Rodriguez, Amit Elazari, Kenneth A. Bamberger, and Serge Egelman. 2020. "The Price is (Not) Right: Comparing Privacy in Free and Paid Apps." *Proceedings on Privacy Enhancing Technologies* 3: 222-242.
- Hao, Karen. 2020. "China's Data Privacy Paradox: Even as the Chinese surveillance state grows more intrusive, the laws protecting consumers' personal data are getting stronger. Can both these things keep happening?" *MIT Technology Review* 123 (5). link.gale.com/apps/doc/A635075110/CDB?u=crepuq_mcgill&sid=bookmark-CDB&xid=29f91480.
- Hargattai, Eszter, and danah boyd. 2010. "Facebook Privacy settings: who cares?" *First Monday*. <https://firstmonday.org/article/view/3086/2589>.
- Hargittai, Eszter. 2010. "Digital Na(t)ives? Variation in Internet Skills and Uses among Members of the "Net Generation"." *Sociological Inquiry* 92-113.
- Hargittai, Eszter. 2005. "Survey Measures of Web-Oriented Digital Literacy Appendix." *Social Science Computer Review*.
- Hargittai, Eszter, and Alice Marwick. 2016. "'What Can I Really Do?' Explaining the Privacy Paradox with Online Apathy." *International Journal of Communication* 10: 3737-3757. doi:10.1002/ijoc.201600005.
- Hargittai, Eszter, and Gina Walejko. 2008. "The participation divide: Content creation and sharing in the digital age." *Information, Communication & Society* 239-256.
- Hayes, Andrew F., Carroll J. Glynn, and James Shanahan. 2005. "Willingness to Self-Censor_ A Construct and Measurement Tool for Public Opinion Research." *International Journal of Public Opinion Research* 298-323.
- Hersh, Eitan. 2015. *Hacking the Electorate: How Campaigns Perceive Voters*. New York: Cambridge University Press.

- Holleman, Bregje, Naomi Kamoen, André Krouwel, Jasper van de Pol, and Claes de Vreese. 2016. "Positive vs. Negative: The Impact of Question Polarity in Voting Advice Applications." *PLOS One* 1-17. doi:10.1371/journal.pone.0164184.
- Huddy, Leonie, Stanley Feldman, Charles Taber, and Gallya Lahav. 2005. "Threat, Anxiety, and Support of Antiterrorism Policies." *American journal of Political Science* 49 (3): 593-608.
- Jacobsson, Sarah. 2010. *MySpace Simplifies Privacy Settings*. May 17. Accessed January 13, 2022. https://www.pcworld.com/article/512822/myspace_privacy.html.
- Kalish, Lil. 2022. *Meet Abortion Bans' New Best Friend—Your Phone*. February 16. Accessed June 20, 2022. <https://www.motherjones.com/politics/2022/02/meet-abortion-bans-new-best-friend-your-phone/>.
- Kassambara, Alboukadel. 2017. *Principal Component Methods in R: Practical Guide*. September 09. Accessed January 18, 2022. <http://www.sthda.com/english/articles/31-principal-component-methods-in-r-practical-guide/112-pca-principal-component-analysis-essentials/>.
- Keefe, Patrick Radden. 2005. *Chatter : dispatches from the secret world of global eavesdropping*. New York: Random House.
- Kerr, Ian, Jennifer Barrigar, Jacquelyn Burkell, and Katie Black. 2009. "Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent." In *Lessons from the identity trail: Anonymity, privacy and identity in a networked society*, edited by Ian Kerr, Valerie M. Steeves and Carole Lucock. Oxford University Press.
- Klar, Samara, and Yanna Krupnikov. 2016. *Independent Politics: How American Disdain for Parties Leads to Political Inaction*. Cambridge: Cambridge University Press.
- Kumaraguru, Ponnurangam, and Lorrie Faith Cranor. 2005. *Privacy Indexes: A Survey of Westin's Studies*. Pittsburgh: Carnegie Mellon University, CyLab, Institute for Software Research International, 22. Accessed October 21, 2018. <http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf>.
- Kwet, Michael. 2019. "In Stores, Secret Surveillance Tracks Your Every Move." *The New York Times*, June 14. <https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html>.
- Lewis, Kevin, Jason Kaufman, and Nicholas Christakis. 2008. "The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network." *Journal of Computer-Mediated Communication* 14: 79-100. doi:10.1111/j.1083-6101.2008.01432.x.
- Litt, Eden, and Eszter Hargittai. 2016. "The Imagined Audience on Social Network Sites." *Social Media + Society* 1-12. doi:10.1177/2056305116633482.
- Lührmann, Anna, and Bryan Rooney. 2020. "Autocratization by Decree: States of Emergency and Democratic Decline." *Comparative Politics* 53 (4): 617-649.
- Lyon, David. 2019. *State and Surveillance*. August. Accessed March 03, 2022. <https://www.cigionline.org/articles/state-and-surveillance/>.
- Madrigal, Alexis C. 2018. "The Most Important Exchange of the Zuckerberg Hearing." *The Atlantic*, April 11. Accessed January 17, 2022. <https://www.theatlantic.com/technology/archive/2018/04/the-most-important-exchange-of-the-zuckerberg-hearing/557795/>.
- Marwick, Alice, Claire Fontaine, and danah boyd. 2017. "Nobody Sees It, Nobody Gets Mad"—Social Media, Privacy, and Personal Responsibility Among Low-SES Youth." *Social Media + Society* 1-14.
- McDonald, Aleecia M., and Lorrie Faith Cranor. 2010. "Americans' Attitudes About Internet Behavioral Advertising Practices." *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society (WPES)*. Chicago: ACM. 63-72. doi:978-1-4503-0096-4/10/10.

- Metzger, Miriam J, and Jennifer Jiyoung Suh. 2017. "Comparative Optimism About Privacy Risks on Facebook." *Journal of Communication* 67 (2): 203-232.
- Morning Consult. 2022. *Many Tech Employees Say They'd Quit Rather Than Be Monitored During Work*. May 31. Accessed February 14, 2023. <https://morningconsult.com/2022/05/31/tech-workers-survey-surveillance/>.
- Motiwalla, Luvai F., Xiaobai (Bob) Li, and Xiaoping Liu. 2014. "Privacy Paradox: Does stated Privacy concerns translate into valuation of personal information?" *Pacific Asia Conference on Information Systems (PACIS) 2014 Proceedings*. Association for Information Systems' Electronic Library (AISeL). 1-17. <https://pdfs.semanticscholar.org/6b22/52fe87c35989f3fe021273eeb636aceff61d.pdf>.
- Newcomb, Alyssa. 2018. *A timeline of Facebook's privacy issues — and its responses*. March 24. Accessed January 13, 2022. <https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651>.
- Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford Law Books.
- Nissenbaum, Helen. 1998. "Protecting Privacy in an Information Age: The Problem of Privacy in Public." *Law and Philosophy* 17 (5/6): 559-596. <https://www.jstor.org/stable/3505189>.
- Opsahl, Kurt. 2010. *Facebook's Eroding Privacy Policy: A Timeline*. April 28. Accessed January 13, 2022. <https://www.eff.org/deeplinks/2010/04/facebook-timeline>.
- O'Reilly, Tim. 2005. *What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*. September 30. Accessed April 20, 2011. <http://oreilly.com/lpt/a/6228>.
- Popkin, Helen A.S. 2010. "Privacy is dead on Facebook. Get over it." *NBC Tech News*, January 13. Accessed March 22, 2023. <https://www.nbcnews.com/id/wbna34825225>.
- Radovanovic, Danica. 2014. *Bridging the Digital Divide: Mobile and Social Media*. January 17. Accessed December 2017. <https://rising.globalvoices.org/blog/2014/01/17/bridging-the-digital-divide-mobile-and-social-media/>.
- Raynes-Goldie, Kate. 2010. "Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook." *First Monday* 15: 1-4. <https://firstmonday.org/ojs/index.php/fm/article/view/2775>.
- Reitman, Rainey. 2011. *Facebook's Hotel California: Cross-Site Tracking and the Potential Impact on Digital Privacy Legislation*. Technical report, San Francisco: Electronic Frontier Foundation.
- Rencher, Alvin C., and William F. Christensen. 2012. *Methods of Multivariate Analysis*. Hoboken: John Wiley & Sons.
- Revelle, William. 2021. *Principal: Principal components analysis (PCA) psych (version 2.1.9)*. September 20. Accessed January 18, 2022. <https://cran.r-project.org/web/packages/psych/psych.pdf>.
- Rueda, David, and Daniel Stegmüller. 2016. "The Externalities of Inequality: Fear of Crime and Preferences for Redistribution in Western Europe." *American Journal of Political Science* 60 (2): 472-489. doi:10.1111/ajps.12212.
- Sander, Thomas H., and Robert D. Putnam. 2010. "Still Bowling Alone? The Post-9/11 Split." *Journal of Democracy* 21 (1): 9-16. http://muse.jhu.edu/journals/journal_of_democracy/v021/21.1.sander.pdf.
- Schlozman, Kay Lehman, Sidney Verba, and Henry E. Brady. 2012. *The Unevenly Chorus: Unequal Political Voice and the Broken Promise of American Democracy*. Princeton: Princeton University Press.
- Schmon, Christoph, and Haley Pedersen. 2022. *Platform Liability Trends Around the Globe: Taxonomy and Tools of Intermediary Liability*. May 25. Accessed June 16, 2022. <https://www.eff.org/deeplinks/2022/05/platform-liability-trends-around-globe-taxonomy-and-tools-intermediary-liability>.

- Schneier, Bruce. 2018. *Click Here to Kill Everybody: security and survival in a hyper-connected world*. New York: W. W. Norton and Company.
- . 2015. *Data and Goliath: the hidden battles to collect your data and control your world*. New York: W.W. Norton & Company.
- Scott, James C. 1998. *Seeing Like a State: how certain schemes to improve the human condition have failed*. New Haven: Yale University Press.
- Siddiq, Fazilat, and Ronny Scherer. 2019. "Is there a gender gap? A meta-analysis of the gender differences in students' ICT literacy." *Educational Research Review* 27: 205-2017.
- Slee, Tom. 2015. *What's Yours Is Mine: Against the Sharing Economy*. New York: OR Books.
- Solove, Daniel J. 2011. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven: Yale University Press.
- Solove, Daniel J., and Danielle Keats Citron. 2021. "Privacy Harms." *George Washington Law Faculty Publications & Other* 63. https://scholarship.law.gwu.edu/faculty_publications/1534.
- Sottek, T.C. 2017. *The 265 members of Congress who sold you out to ISPs, and how much it cost to buy them*. March 29. Accessed January 17, 2022. <https://www.theverge.com/2017/3/29/15100620/congress-fcc-isp-web-browsing-privacy-fire-sale>.
- Statista Research Department. 2021. *Distribution of net digital ad revenue in the United States in 2019 and 2020, by company*. August 06. Accessed January 16, 2022. <https://www.statista.com/statistics/242549/digital-ad-marketFa-share-of-major-ad-selling-companies-in-the-us-by-revenue/#statisticContainer>.
- . 2021. *Facebook's global revenue as of 3rd quarter 2021, by segment*. November 1. Accessed January 16, 2022. <https://www.statista.com/statistics/277963/facebooks-quarterly-global-revenue-by-segment/>.
- Stoycheff, Elizabeth, Juan Liu, Kunto A. Wibowo, and Dominic P. Nanni. 2017. "What have we learned about social media by studying Facebook? A decade in review." *New Media & Society* 19 (6): 968-980. doi:10.1177/1461444817695745.
- Svirsky, Daniel. 2019. "Why are privacy preferences inconsistent? information avoidance." *John M. Olin Center for Law, Economics, and Business Discussion Paper No. 81*. Cambridge: Harvard Law School, January. 36.
- Taylor, Humphrey. 2001. *Overwhelming Public support for increasing surveillance powers in spite of many concerns*. Survey summary, New York : Harris Interactive.
- Teamsters. 2022. "Teamsters Tell FTC It's Time to Crack Down on Mass Surveillance of Workers." Public Statement, Washington D.C. Accessed February 14, 2023. <https://teamster.org/2022/11/teamsters-tell-ftc-its-time-to-crack-down-on-mass-surveillance-of-workers/>.
- Tsai, Janice Y., Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study." *Information Systems Research* 254-268.
- Tunney, Catharine. 2019. "RCMP launches review of its social media monitoring operation." *CBC*, November 05. <https://www.cbc.ca/news/politics/rcmp-social-media-review-1.5346741>.
- Turow, Joseph. 2023. *Americans Can't consent to Companies' use of their Data*. Annenberg School for Communication, University of Pennsylvania. https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf.
- Turow, Joseph, Michael Hennessy, Nora Draper, Ope Akanbi, and Diami Virgilio. 2018. *Divided We Feel: Partisan Politics Drive Americans' Emotions Regarding Surveillance of Low-Income Populations*. Academic, University of Pennsylvania, Annenberg: Annenberg School for Communication.

- United States of America. 2019. *Facebook, Inc.: Complaint for Civil Penalties, Injunction, and Other Relief*. Civil court filing complaint, Washington D.C.: United States District Court for the District of Columbia.
- Vagianos, Alanna. 2022. *Oklahoma Considers Database For Pregnant People As Roe Hangs In The Balance*. February 10. Accessed June 20, 2022. https://www.huffpost.com/entry/oklahoma-considers-database-for-pregnant-people-as-ro-hangs-in-the-balance_n_61fc17dee4b0725faac6d865.
- Valentino-DeVries, Jennifer, and Jeremy Singer-Vine. 2012. "They Know What You're Shopping For; 'You're looking at the premium package, right?' Companies today are increasingly tying people's real-life identities to their online browsing habits." *Wall Street Journal*, December 08. <http://online.wsj.com/article/SB10001424127887324784404578143144132736214.html>.
- Viola, Lora Anne, and Pawel Laidler. 2022. *Trust and transparency in an age of surveillance*. New York: Routledge.
- Wagner, Kurt. 2018. *This is how Facebook collects data on you even if you don't have an account*. April 20. Accessed January 17, 2022. <https://www.vox.com/2018/4/20/17254312/facebook-shadow-profiles-data-collection-non-users-mark-zuckerberg>.
- Wall Street Journal. 2010. "The Journal's Cellphone Testing Methodology." *The Wall Street Journal*, December 18. Accessed January 14, 2022. <https://www.wsj.com/articles/SB10001424052748704034804576025951767626460>.
- . 2010-2012. "What they Know series." *The Wall Street Journal*. <https://www.wsj.com/news/types/what-they-know>.
- Westin, Alan F. 1967. *Privacy and Freedom*. New York: Atheneum.
- Westin, Alan F. 2003. "Social and Political Dimensions of Privacy." *The Society for the Psychological Study of Social Issues* 431-453.
- Whelan, Glen. 2019. "Trust in Surveillance: A Reply to Etzioni." *Journal of Business Ethics* 156: 15-19. doi:10.1007/s10551-018-3779-4.
- Wikipedia. 2021. *Lane v. Facebook, Inc.* November 3. Accessed January 13, 2022. https://en.wikipedia.org/wiki/Lane_v._Facebook,_Inc.
- Wodinsky, Shoshana. 2022. *Wordle Is Watching You*. February 17. <https://gizmodo.com/wordle-ad-trackers-privacy-new-york-times-1848554549>.
- Zaller, John R. 1992. *The Nature and Origins of Mass Opinion*. Cambridge: Cambridge University Press.
- Zarouali, Brahim, Koen Ponnet, Michel Walrave, and Karolien Poels. 2017. "'Do you like cookies?'" Adolescents' skeptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing." *Computers in Human Behavior* 69: 157-165.
- Zhang, Baobao, Sarah Kreps, and Nina McMurry. 2020. "Americans Perception of Privacy and Surveillance in the COVID 19 Pandemic." *Working paper* 1-24.
- Ziller, Conrad, and Marc Helbling. 2020. "Public Support for State Surveillance." *European Journal of Political Research*.
- Zuboff, Shoshana. 2019. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: Public Affairs.
- Zureik, Elia, and Lynda L. Harling Stalker. 2010. "The Cross-Cultural Study of Privacy: Problems and Prospects." Chap. 1 in *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, by Elia Zureik, Lynda L. Harling Stalker, Emily Smith, David Lyon and Yolande E. Chan, 9-30. Montreal: McGill-Queen's University Press.
- Zureik, Elia, Lynda L. Harling Stalker, Emily Smith, David Lyon, and Yolanda E. Chan, . 2010. *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*. Montreal: McGill-Queen's University Press.

Appendix

Distribution and representativeness

Demographic Group	Target %	Current
Age: 18-24:	13	10
Age: 25-34:	20	19
Age: 35-44:	20	19
Age: 45-64:	33	30
Age: 65-99:	14	20
Gender: Male	49	48
Gender: Female	51	52
Race: White (Non-Hispanic)	68	74
Race: Black (Non-Hispanic)	12	9
Race: Hispanic	12	6
Race: Other Ethnicity	10	8% Asian, 3% Other
Region: Midwest	20	NA
Region: West	26	NA
Region: Northeast	20	NA
Region: South	34	NA
OTHER: Education CENSUS data		
Less than complete college	53	42
College	32	42
More than college	12	14
OTHER: PID	Gallup data August 2-17 2021	
Democrat	28	38
Independent	40	30
Other	NA	<1
Republican	28	27
Religion	NA	
Protestant, evangelical		8%
Protestant, non-evangelical		12%
None / Don't have one / Atheist		16%
Other Christian		17%
Catholic		19%
Other		19%
Don't know / Prefer not to answer		8%

Table 2 Sociodemographic survey distributions

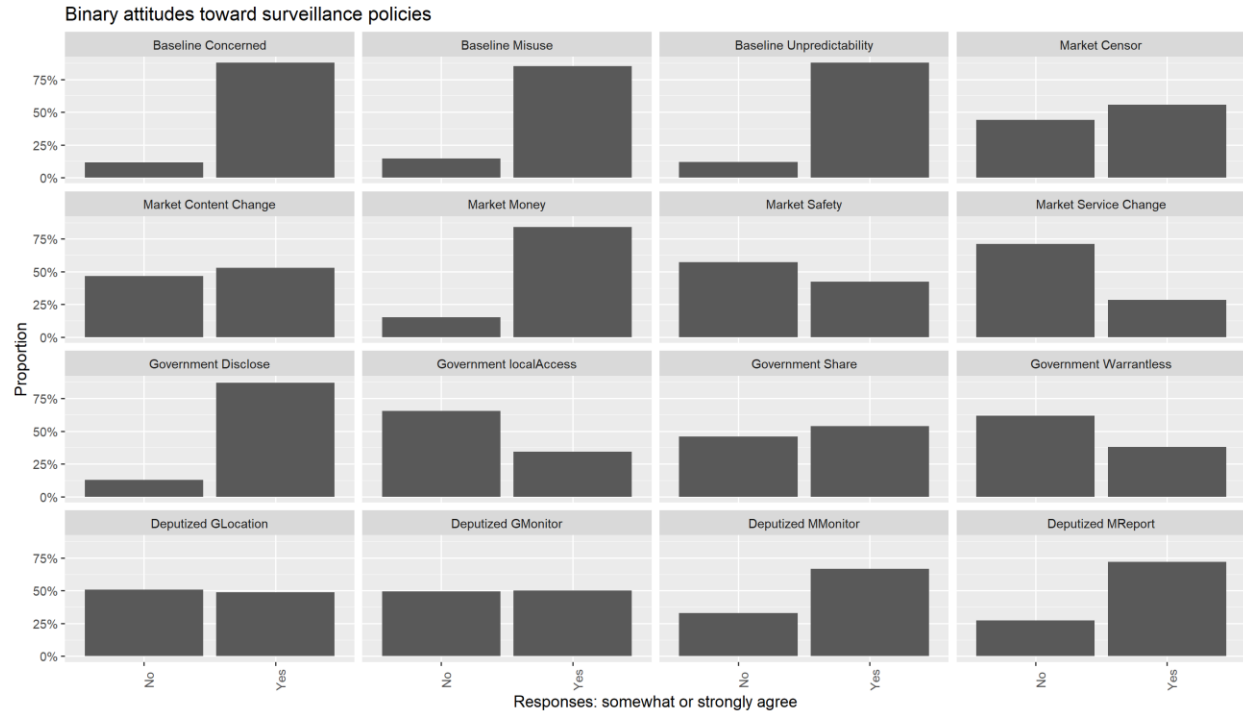


Figure 8 Binary calculation of support for statements

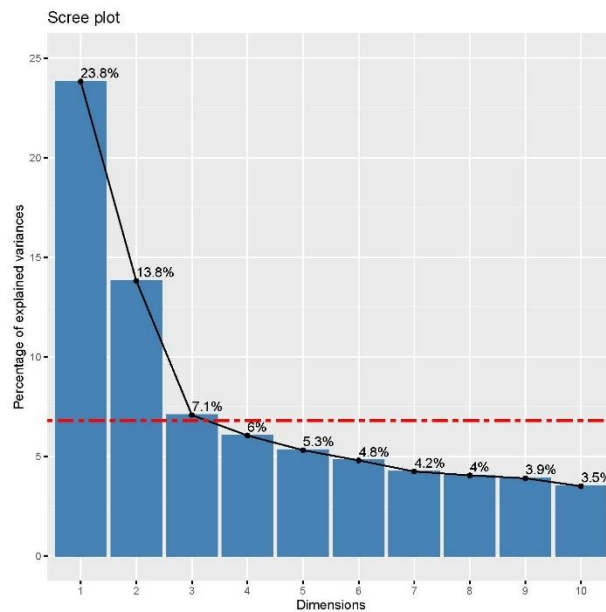


Figure 9 PCA Scree plot

Principal Components Analysis without Market/Gov't Geolocation
 Call: psych::principal(r = ., nfactors = 3, rotate = "varimax")
 Standardized loadings (pattern matrix) based upon correlation matrix

RC1 RC2 RC3

Baseline_Concerned	0	0.71	0.01
Baseline_Unpredictability	-0.01	0.72	0.02
Baseline_Responsibility	0.22	-0.36	0.11
Baseline_Misuse	0.01	0.7	0.01
Market_Safety	0.67	-0.04	-0.15
Market_Money	0.14	0.57	-0.12
Market_Content_Change	0.63	-0.02	0.11
Market_Censor	0.5	-0.1	0.31
Market_Service_Change	-0.17	0.5	0
Government_Share	0.55	-0.05	0.25
Government_localAccess	0.75	0.06	0.19
Government_Warrantless	0.74	0.09	0.15
Government_Disclose	0.23	0.52	-0.18
Deputized_MMonitor	0.13	-0.1	0.83
Deputized_MReport	0.14	-0.16	0.8
Deputized_GMonitor	0.51	0.02	0.59
Deputized_GLocation	0.57	0.04	0.55
	RC1	RC2	RC3
SS loadings	3.28	2.54	2.3
Proportion Var	0.19	0.15	0.14
Cumulative Var	0.19	0.34	0.48
Proportion Explained	0.4	0.31	0.28
Cumulative Proportion	0.4	0.72	1
Mean item complexity = 1.3			
Test of the hypothesis that 3 components are sufficient.			
The root mean square of the residuals (RMSR) is 0.07 (same as nfactors = 4)			
with the empirical chi square 1884.56 with prob < 0			
Fit based upon off diagonal values = 0.92 (same as nfactors = 4)			

Table 3 18-item 3D Principal Components Analysis

To include the 19th item, which is randomized to show either the market or government geolocation item, the PCAs have to be re-run on the respondent subsets based on which policy question they received. Table 2 includes responses to the item “Companies should be allowed to collect location data when visiting private places”. The rank in proportion explained by deputized surveillance is almost split equally between the four dimensions, and market-exclusive attitudes become split off from government-exclusive attitudes. With the PCA subsets those who saw government geolocation (“The government should be allowed to collect location data when visiting public places”), the deputized surveillance dimension explains the most (34%) but the 19th measure weakly cross-loads into that dimension, while the other government attitudes diffuse into no particular dimension or pattern. The fact that neither of these technologically-similar practices loaded onto the deputized

surveillance dimension further supports the hypothesis that deputation produces a dimension of privacy concern different from self-contained government or corporate practices¹⁴⁰.

Principal Components Analysis with Market Geolocation				
Call: psych::principal(r = ., nfactors = 4, rotate = "varimax")				
Standardized loadings (pattern matrix) based upon correlation matrix				
	RC2	RC1	RC3	RC4
Baseline_Concerned	0.76	0.1	0.05	-0.05
Baseline_Unpredictability	0.74	0.11	0.07	-0.13
Baseline_Responsibility	-0.37	0.28	0.15	-0.11
Baseline_Misuse	0.7	0.12	0.07	-0.21
Market_Geolocation	0.08	0.67	0.11	0.33
Market_Safety	0.04	0.72	-0.08	0.1
Market_Money	0.58	-0.09	-0.14	0.32
Market_Content_Change	-0.05	0.69	0.15	0.21
Market_Censor	-0.07	0.62	0.37	0.02
Market_Service_Change	0.5	-0.13	-0.06	0
Government_Share	-0.07	0.13	0.19	0.74
Government_localAccess	0.03	0.4	0.19	0.67
Government_Warrantless	0.07	0.5	0.15	0.54
Government_Disclose	0.55	0.04	-0.17	0.28
Deputized_MMonitor	-0.11	0.06	0.83	0.12
Deputized_MReport	-0.08	0.06	0.84	0.05
Deputized_GMonitor	0.04	0.34	0.61	0.38
Deputized_GLocation	0.03	0.3	0.58	0.5
	RC2	RC1	RC3	RC4
SS loadings	2.7	2.61	2.47	2.13
Proportion Var	0.15	0.14	0.14	0.12
Cumulative Var	0.15	0.29	0.43	0.55
Proportion Explained	0.27	0.26	0.25	0.22
Cumulative Proportion	0.27	0.54	0.78	1
Mean item complexity = 1.6				
Test of the hypothesis that 4 components are sufficient.				
The root mean square of the residuals (RMSR) is 0.06				
with the empirical chi square 796.3 with prob < 4.7e-115				
Fit based upon off diagonal values = 0.94				

Table 4 19-item Market location Principal Components Analysis

¹⁴⁰ A principal components analysis estimated a Cronbach's alpha 0.80 [95% CI: 0.78 to 0.89], further suggesting a distinct dimension of concern over deputized surveillance practices compared to the "exclusive" practices.

Principal Components Analysis with Government Geolocation				
Call: psych::principal(r = ., nfactors = 4, rotate = "varimax")				
Standardized loadings (pattern matrix) based upon correlation matrix				
	RC1	RC3	RC2	RC4
Baseline_Concerned	-0.05	0.07	0.68	0.17
Baseline_Unpredictability	0.03	-0.03	0.73	0.19
Baseline_Responsibility	0.14	0.19	-0.5	0.08
Baseline_Misuse	-0.03	0.15	0.72	0.15
Market_Safety	0.01	0.74	-0.04	-0.02
Market_Money	-0.06	0.11	0.14	0.67
Market_Content_Change	0.2	0.63	0.07	0.01
Market_Censor	0.34	0.5	0.08	-0.29
Market_Service_Change	0.07	-0.4	0.11	0.6
Government_Geolocation	0.58	0.35	-0.07	0.17
Government_Share	0.46	0.31	-0.25	0.26
Government_localAccess	0.46	0.56	-0.07	0.27
Government_Warrantless	0.4	0.6	0	0.21
Government_Disclose	0	0.1	0.19	0.61
Deputized_MMonitor	0.79	-0.06	0	-0.22
Deputized_MReport	0.76	0	-0.13	-0.24
Deputized_GMonitor	0.68	0.34	0.01	0.05
Deputized_GLocation	0.7	0.36	-0.04	0.15
	RC1	RC3	RC2	RC4
SS loadings	3.25	2.59	1.94	1.7
Proportion Var	0.18	0.14	0.11	0.09
Cumulative Var	0.18	0.32	0.43	0.53
Proportion Explained	0.34	0.27	0.2	0.18
Cumulative Proportion	0.34	0.62	0.82	1
Mean item complexity = 1.6				
Test of the hypothesis that 4 components are sufficient.				
The root mean square of the residuals (RMSR) is 0.07				
with the empirical chi square 968 with prob < 9.7e-149				
Fit based upon off diagonal values = 0.91				

Table 5 19-item Government location Principal Components Analysis

The five-dimension PCA does not change the main result that responses to deputized surveillance concerns are a distinct dimension with non-overlapping loadings¹⁴¹. What changes is the variance explained, and deputized surveillance remains the second most powerful dimension (22%, while the first dimension explains 24%, similar to the four-dimension PCA).

Principal Components Analysis without Market/Gov't								
Geolocation								
Call: psych::principal(r = ., nfactors = 5, rotate = "varimax")								
Standardized loadings (pattern matrix) based upon correlation matrix								
	RC1	RC3	RC2	RC5	RC4	h2	u2	com
Baseline_Concerned	0.02	0.01	0.73	0.04	0.19	0.57	0.43	1.2
Baseline_Unpredictability	0.03	0.01	0.74	0.03	0.18	0.59	0.41	1.1
Baseline_Responsibility	0.17	0.25	0.53	0.44	0.27	0.63	0.37	3.2
Baseline_Misuse	0.05	0.01	0.72	0.08	0.18	0.57	0.43	1.2
Market_Safety	0.21	0.08	0.01	0.74	0.04	0.6	0.4	1.2
Market_Money	0.11	-0.1	0.23	0.04	0.7	0.57	0.43	1.3
Market_Content_Change	0.27	0.14	0.09	0.64	-0.09	0.52	0.48	1.6
Market_Censor	0.13	0.35	0.07	0.59	-0.2	0.54	0.46	2.1
Market_Service_Change	0.13	0.05	0.14	0.17	0.72	0.58	0.42	1.3
Government_Share	0.76	0.17	0.12	0	0	0.62	0.38	1.1
Government_localAccess	0.74	0.14	0.01	0.31	0.05	0.67	0.33	1.4
Government_Warrantless	0.66	0.12	0.06	0.39	0.06	0.61	0.39	1.8
Government_Disclose	0.28	-0.2	0.27	0.02	0.49	0.44	0.56	2.6
Deputized_MMonitor	0.17	0.82	0.04	0.02	-0.09	0.72	0.28	1.1
Deputized_MReport	0.1	0.82	-0.1	0.09	-0.08	0.71	0.29	1.1
Deputized_GMonitor	0.45	0.58	0.03	0.27	0.01	0.62	0.38	2.4
Deputized_GLocation	0.59	0.52	0.01	0.2	0.06	0.66	0.34	2.3
	RC1	RC3	RC2	RC5	RC4			
SS loadings	2.42	2.28	2.07	1.92	1.5			
Proportion Var	0.14	0.13	0.12	0.11	0.09			
Cumulative Var	0.14	0.28	0.4	0.51	0.6			

¹⁴¹ The five-dimension PCA disaggregates the explanatory capacity between three market attitudes (market_safety, market_content_change and the addition of Market_censor which was had a weaker eigenvalue (0.54) in the 4-dimension PCA's RC1) from three government attitudes (Government_localAccess, Government_Warrantless and Government_Share) which also had a weak eigenvalue in the 4-dimension PCA RC1 (0.44). Market_censor attitude: Should keep track of what users post and delete it based on "community standards". Government_Share attitude: Federal agencies and state officials should be able to exchange data on citizens.

Proportion Explained	0.24	0.22	0.2	0.19	0.15
Cumulative Proportion	0.24	0.46	0.66	0.85	1

Mean item complexity = 1.6

Test of the hypothesis that 5 components are sufficient.

The root mean square of the residuals (RMSR) is 0.07 (same as nfactors = 4)

with the empirical chi-square 1926.77 with prob < 0

Fit based upon off diagonal values = 0.92 (same as nfactors = 4)

Table 6 18-item 5 dimension PCA

term	Baseline Concerned	Baseline Unpredictability	Baseline Responsibility	Baseline Misuse	Market Geolocation	Market Safety	Market Money	Market Content Change	Market Censor	Market Service Change	Government Geolocation	Government Share	Government localAccess	Government Warrantless	Government Disclose	SComplex MMonitor	SComplex MReport	SComplex GMonitor	SComplex GLocation
Baseline Concerned	1	0.43	-0.18	0.45	0.1	-0.01	0.25	0.05	-0.02	0.21	0.01	-0.02	0.03	0.04	0.24	-0.08	-0.11	-0.01	0
Baseline Unpredictability		1	-0.23	0.42	0.06	0.03	0.25	0.01	-0.03	0.22	-0.03	-0.09	0.02	0.08	0.26	-0.07	-0.1	0	-0.01
Baseline Responsibility			1	-0.17	0.12	0.13	-0.08	0.12	0.16	-0.09	0.15	0.1	0.12	0.1	-0.1	0.15	0.2	0.14	0.14
Baseline Misuse				1	0.07	0.02	0.27	0.03	0	0.18	0.01	-0.05	0.03	0.05	0.23	-0.09	-0.1	0	0
Market Geolocation					1	0.36	0.09	0.54	0.37	-0.01	0*	0.34	0.43	0.43	0.12	0.21	0.15	0.38	0.42
Market Safety						1	0.05	0.35	0.28	-0.08	0.16	0.14	0.33	0.37	0.08	0.07	0.11	0.25	0.25
Market Money							1	0.03	-0.05	0.3	0.05	0.02	0.08	0.1	0.32	-0.1	-0.12	0.03	0.04
Market Content Change								1	0.38	-0.09	0.35	0.26	0.36	0.36	0.02	0.19	0.2	0.35	0.34
Market Censor									1	-0.17	0.29	0.21	0.3	0.31	-0.03	0.28	0.29	0.41	0.35
Market Service Change										1	-0.07	-0.08	-0.08	-0.05	0.18	-0.1	-0.1	-0.07	-0.06
Government Geolocation											1	0.43	0.51	0.38	0.06	0.29	0.35	0.41	0.53
Government Share												1	0.48	0.39	0.05	0.24	0.22	0.37	0.45
Government localAccess													1	0.59	0.13	0.26	0.23	0.44	0.49
Government Warrantless														1	0.13	0.24	0.22	0.41	0.46
Government Disclose															1	-0.1	-0.13	0.03	0.09
SComplex MMonitor																1	0.61	0.46	0.44
SComplex MReport																	1	0.43	0.42
SComplex GMonitor																		1	0.62
SComplex GLocation																			1

Table 7 Correlation matrix estimates

To deal with the volume of combinations, I present two graphical versions of the correlation matrix; the table version is in the appendix (Table 7). The first version is known as a correlation heatmap. All pairwise correlations are noted, with a color background to help visualize patterns of clustering¹⁴².

¹⁴² The color intensity reflects the strength of the correlation, positive correlations are blue, negative correlations are red. The variables are ordered by their appearance in the survey. The diagonal of 1.00's is the correlation of each variable with itself. The correlation of 0.0 between market geolocation and government geolocation was manually inserted because the question was never asked concurrently, but the visualization could not be produced with an NA in the matrix. I also add

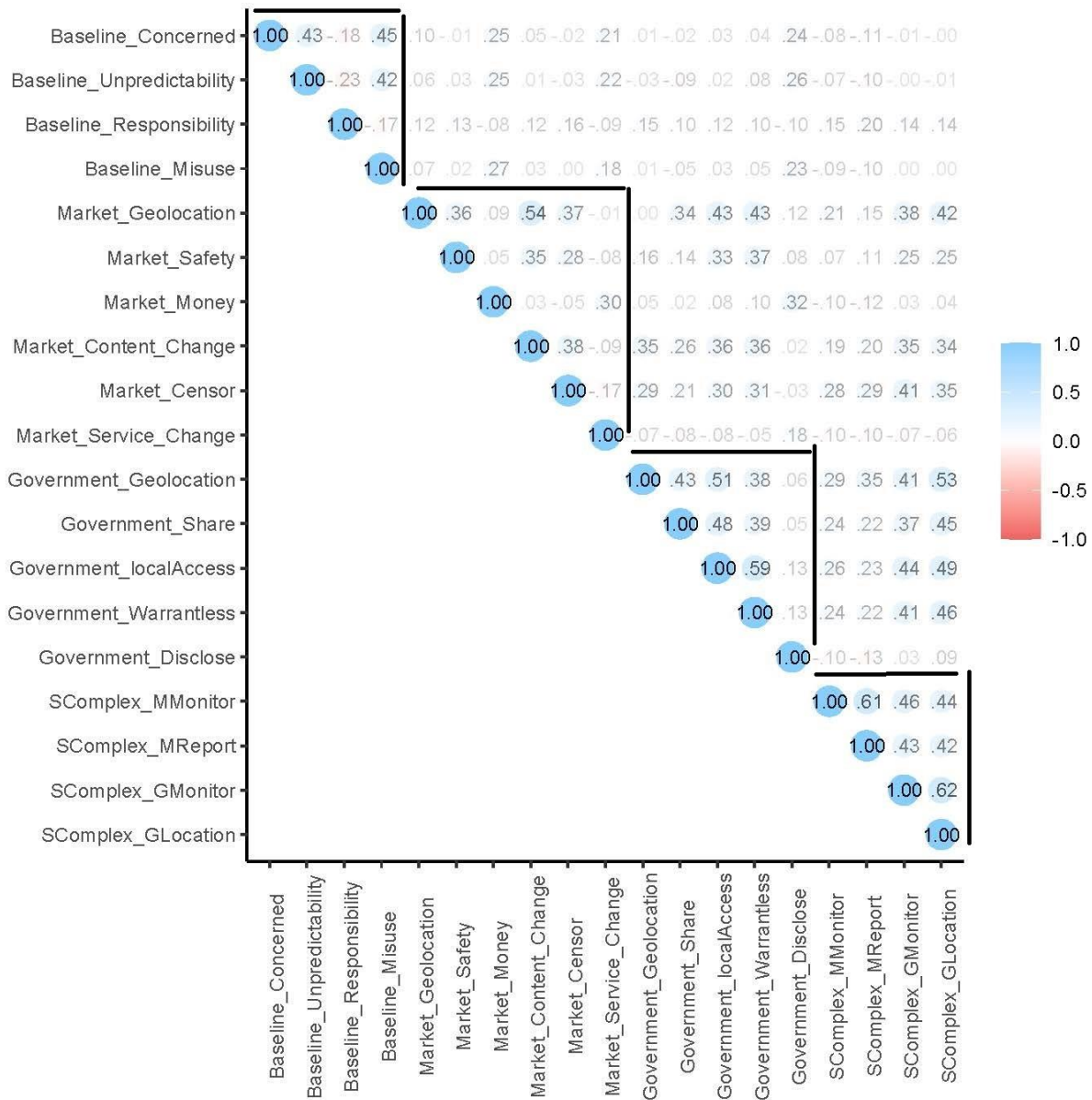


Figure 10 Correlation heatmap

The correlation heatmap suggests strongest clustering between the four deputized surveillance measures. There is also some moderately strong (± 0.31 to 0.49) correlations between the government and deputized surveillance dyads, as well as between government and market. The next figure is a

border lines to demarcate where the survey block dyad groupings are located. The area under the “stairs” demarcates the survey block cluster dyads.

network plot, which represents the strength of the dyad correlations as distances. It is set to plot correlations stronger than ± 0.3 so no dyad below a moderately strong relationship is plotted.



Figure 11 Network plot of dyad correlations

Figure 5 helps us anticipate PCA estimates. Deputized surveillance responses are correlated to themselves and the government location response¹⁴³ (for the half-sample that saw it). Importantly, even though government deputation strongly relies on market surveillance, the relationship between

¹⁴³ The government should be allowed to collect location data when visiting public places.

correlation dyads is not triangular; that is, they are not equally correlated to both market-exclusive surveillance attitudes and government-exclusive surveillance attitudes. Note that the baseline measures are weakly associated with themselves, which was not expected, and not at all close to the rest of the items. A few market and government-exclusive surveillance attitudes are uncorrelated to their block responses.

Chapter 3 Who is mass online surveillance for?

Abstract

Building off chapters 1 and 2, I test the argument that support for mass online surveillance is bolstered by othering frames that make disliked groups more salient. This shift, inadvertently or deliberately, emphasizes a targeted harm effect after data collection that redefines surveillance. Using an experimental factorial vignette design, I test whether reminding people that liked groups are also monitored decreases support for two deputized surveillance policies. Emphasizing competing privacy claims and moving away from self-referential measures of privacy concerns allows me to measure the plasticity of people's opinions, increasing or decreasing depending on their random assignment into treatment or control. This novel experiment also contributes to the field by challenging untested sociodemographic assumptions of privacy concerns, offering an alternative explanation that focuses on how individuals resolve competing claims for privacy and the role of securitized frames offered by those supplying surveillance on demand for these policies.

Introduction

In Chapter 1, I raised the issue of how information about the surveillance complex is managed: prioritizing no information, and if forced into admitting mass surveillance is taking place, emphasizing a targeted group (e.g., criminals broadly or terrorists) and highlighting how the data is put to use after surveillance.

I have argued that this reframing or focus manipulates public perception of the scope of harm. It deemphasizes how all people, including liked groups, must also be monitored because of how mass surveillance works.

Many public opinion studies focus on respondents' attitudes towards their own surveillance ("egotropic"). This leads to an oversight of how intergroup relations (out-group bias *and* in-group favoritism) shape our responses to surveillance. In this chapter, I remediate this ongoing oversight by experimenting with how the presence of disliked and liked group members influences respondents' preferences on surveillance policy implementation. As the dissertation introduction discussed, this point is fundamental to understanding the backsliding process in democratic societies. The use of mass surveillance cannot be compatible with universalistic privacy rights. Even if the evidence

gathered is somehow guaranteed only to be used against targeted groups, mass surveillance still erodes democratic principles. It turns rights afforded to all into privileges for the “right” types of groups. It erodes freedom of speech, freedom of assembly, equal protection under the law, procedural justice (transparent handling of evidence, knowing your accuser, innocent until proven guilty, search and seizure after judicial review), and it erodes republican principles of checks and balances regarding the legislation, execution, and review of the rule of law. Deputation of mass surveillance further erodes democracy by offloading law and order decision-making to private companies, which are shielded from public accountability and legally liable only to shareholder wealth.

In this chapter, I focus on mass surveillance policy frames. Two types of disclosures shape public debate about the surveillance complex: infrequent whistleblowing like the Snowden revelations, which pressure politicians to make public statements or smaller-impact stories written by journalists that produce less public pressure. Journalistic endeavors have yielded important information¹⁴⁴, but these stories have two constraints: they tend to be short-lived in the media cycle¹⁴⁵ and often sourced from law enforcement interactions. The second, in particular, makes media frames of surveillance susceptible to government claims of criminality, the need for technologies to break encryption, and the abuse of surveillance powers as “sporadic” and non-systematic. There are also direct financial incentives for the media to under-report systematic mass surveillance. Newspapers increasingly rely on a web of surveilling technologies to distribute their content (Google and Facebook news feeds), on targeted ads to boost their profit margins and use cookies to paywall articles to non-subscribers

¹⁴⁴ For example, attempts to understand how cellphone and geolocation data is obtained during criminal trials have uncovered a “parallel construction” strategy that introduces laundered evidence that would otherwise be considered “fruit of the tainted tree”. Other journalistic work has revealed how police departments serve Google with para-legal “geofence warrants” identifying all cellphone users in a geographic location that it complies with as a goodwill gesture without court orders and the use of ClearviewAI facial recognition by police departments.

¹⁴⁵ Journalist Patrick Radden Keefe makes the third critique in his pre-Snowden book on NSA digital communications surveillance, *Chatter*. He identifies a “gentleman’s agreement” not to publish stories in the American press (Radden Keefe, 2005, p. 37). The arrangement is exacerbated by an excess of caution from outlets that tend to bury stories when agencies refuse to comment or verify facts, which creates an easy out for both parties (*ibid*, p. 32).

which requires their own (undisclosed) surveilling. Thus, media companies are not neutral observers in reporting complex surveillance stories, which may impact their editorial decisions on this topic (Fang 2022, Wodinsky 2022).

As a result of the three factors above, narratives of mass surveillance tend to be centered on security concerns over *groups* of people instead of the general population. Because law enforcement's contacts with groups comprise the bulk of journalists' sources on surveillance policies, law enforcement's contact with groups is characterized as deviant—criminals or otherwise suspicious of *potential* criminality, quasi-illegal wrongdoing, or general unsavoriness¹⁴⁶. This context leads to framing effects where public opinion of mass monitoring is inextricably linked to attitudes towards specific groups. Seen through a lens where particular groups are the ultimate “aim” of mass surveillance, mass surveillance is de facto winnowed down and reframed as targeted surveillance.

As discussed throughout the dissertation, this way of presenting what the technology does and how surveillant institutions use data has implications for democratic norms of consent and justice: Citizens are incentivized by surveillant entities to believe that groups that are defined by their (known) deviance are the only people monitored, instead of being told everyone is being asked to prove their innocence every second of every day. The subversion of “innocent until proven guilty” into everyone being “guilty until proven innocent” is obfuscated as mass surveillance policies are framed as retroactive and limited to ‘known’ criminals. Citizens’ lack of understanding of this process and its implications, and thus, lack of mobilization against the actual monitoring practices, are taken as explicit consent for the post-9/11 status quo by policy makers and surveillance complex technologists. Because previous surveillance studies have not problematized these issues (as discussed in chapter 2),

¹⁴⁶ Spencer Ackerman argues that the War on Terrorism’s semi-tacit emphasis on suspicion of Muslim “loyalty” to the US, and subsequent surveillance of them, boosted the jingoistic antagonism that was transferred to all immigrants as the war’s failure to stabilize Iraq and Afghanistan became a political quagmire (2021).

we lack a clear sense of people's a) understanding of the multiple dimensions of the surveillance complex and b) the mechanisms by which these are produced/challenged.

In this chapter, I try to understand how people react to the commonly used narratives highlighting the importance of criminal activity to justify surveillance compared to reactions vis-a-vis actual mass surveillance policies and their consequences for non-criminals. I argue that because mass surveillance is more frequently presented as affecting (only) disliked groups, previous measures of support for mass surveillance are more likely to tap support for targeted surveillance. To measure attitudes towards mass surveillance as practiced today in the surveillance complex, respondents must have clarity about how surveillance deputation operates and how many other groups, including liked groups, are subjected to it. Thus, I developed an alternative and novel way of measuring attitudes towards mass surveillance based on the effect of intergroup relations separate from the attitudes towards the particular variation in the invasiveness of the surveillance policies (see Design section).

Theory

Early internet privacy literature was heavily invested in measuring an individual's a) preferences for their privacy and b) personal responsibility, capacity, awareness, and interest in combatting surveillance. Focus on these research questions pursued a *Goffmanian* definition of privacy¹⁴⁷. "Viewed as control of information about the self" (Hann, Hui, Lee, & Png, 2014; Dhir, Torsheim, Pallesen, & Andreassen, 2017), the Goffmanian research agenda assumes a level of autonomy that, in reality, is made impossible by the networked nature of online communications¹⁴⁸. People's concerns over the

¹⁴⁷ Anthropologist Erving Goffman posited that in social interactions, participants take up a *face* that is a personal claim about one's positive social values, an image or personae, and groups of people navigate rules of social interaction collectively, trying to maintain their face or engage in face-saving when "embarrassed" or otherwise out of step with the particular set of practices of a group (1967).

¹⁴⁸ Critics of Data Goliaths argue that large tech firms benefit from discussing privacy in terms of an ego-tropic individual choice, begrudgingly providing minimal settings to operationalize that choice. Data Goliaths benefit from giving little privacy because the more data they have the algorithms can more efficiently sort people into a variety of groups. Algorithms thrive on larger datasets, creating incentives for amassing bigger haystacks (Chushing, 2016). Looking for needles is easier with bigger haystacks when computers, not humans, sort through the data (Radden Keefe, 2005, p. 132).

privacy of others—directly at issue when they engage in digital communications—have been chronically excluded from much of the research. This omission has produced an understandable but narrow focus on measuring attitudes toward one’s own (self-interested) privacy. As discussed throughout the dissertation, especially in the technical explanation of chapter 1¹⁴⁹, online surveillance is networked and affords many points of entry for monitoring even when someone attempts to evade monitoring, mainly via market surveillance. This makes the measurement of attitudes toward others’ surveillance a necessary but absent component (cf. Turow, Hennessy, Draper, Akanbi, & Virgilio, 2018; Whelan, 2019).

Previous public opinion surveys, reflecting public discourse, take at face value government claims that the data gathered from mass online surveillance only affects criminals¹⁵⁰ (Garcia & Geva, 2016; Huddy, Feldman, Taber, & Lahav, 2005; Davis & Silver, 2004; Hampson & Jardine, 2016; Dinev, et al., 2006; Dinev, Hart, & Mullen, 2008; Ziller & Helbling, 2020). This blind spot hints at an answer to why Americans have remained demobilized on mass surveillance, despite revelations from Thomas Drake, Mark Klein, William Binney, Edward Snowden, and others. It helps explain why previous studies are mainly concerned with individuals’ relation to those surveilling them (e.g., ‘are you concerned about your emails being monitored’) instead of mass surveillance as an issue of collective governance.

Mass surveillance is, tautologically, a policy with universalistic effects. Nevertheless, the emphasis on its particularistic effects for certain out-groups (while minimizing the effects on everyone else) may trigger respondents’ beliefs about socially acceptable answers that diminish 1) concerns about their own privacy and 2) concerns about collective in-group privacy. By being asked to consider

¹⁴⁹ See discussion on Goffmanian privacy.

¹⁵⁰ One might also ask how this certainty is produced. If only known criminals are targeted, then why is mass surveillance necessary? This statement implies the evidence to identify criminals already exists, so why does law enforcement need to track everyone else’s communications? This issue has not been systematically raised in the media or in surveys about beliefs/cognitive dissonance of surveillance information.

mass surveillance in terms of out-groups' "others", we are collectively distracted from asking institutions why everyone else's data is collected and justifying why it is needed and effective for policing. Institutions avoid public deliberation over whether democratic principles of justice and free speech need or should be given up through mass surveillance for what is allegedly targeted policing.

An alternative view of mass online surveillance is that its practice relies on an interdependence where everyone is "complicit" in allowing others to be surveilled. The "atomistic self, [viewed as] capable of making perfectly rational and isolated choices" (Kerr & Barrigar, 2012, p. 390), is actually incapable of dealing with mass online surveillance. Such efforts require coordinated collective action based on common knowledge (Sloan & Warner, 2017).

Throughout a range of economic and social policy issues, "[American's] self-interest has had very circumscribed and limited effects" (Huddy, 2013, p. 740) on policy preferences, compared to group interests' effects, which are "often more powerful politically" (idem, 741). In the context of the war on terrorism, religion and country of origin are the main (semi-tacit) groupings of interest, given how their articulation as drivers of (international) terrorism have shaped surveillance intelligence gathering policy and priorities, sustaining the legitimacy of the US invasion of Iraq, Afghanistan, and other Middle East and African interventions, and shaping meta-data analysis for military strike drone operation decision-making over the past 20 years (Jaffer, 2016; Crockford, 2012; United Nations Special Rapporteur on Counter-Terrorism and Human Rights, 2013).

When conservatives tried to make explicit that the war on terrorism's locus was on Muslims by calling it a war on "radical Islamic terrorism", liberals pushed back, seeking to deny anything that might sound like religious persecution¹⁵¹ (Ackerman, 2021). However, the stigma, policy focus, and

¹⁵¹ For example, a decade later, a review of group identity and political cohesion by Huddy states: "When George W. Bush identified Osama bin Laden and al-Qaeda as the enemy after 9/11, he went out of his way to make clear that Muslims and Muslim Americans were not the targets of US military action. His position was generally adopted by Americans". This whitewashing of the pervasive anti-Muslim sentiment extrapolates from a single moment and produces a revisionist take that ignores Bush, and his administration officials', pivot to openly hostile anti-Muslim sentiment, particularly after his second term was secured. The last observation ignores the rise of American hate crimes, how the police and intelligence

military forces' decisions have linked terrorism to populations in Islamic countries bipartisanly. For example, the Department of Homeland security, formed in the wake of 9/11, developed domestic surveillance programs hyper-focused on monitoring Muslim populations at the cost of ignoring growing domestic white nationalist terrorist movements (Pilkington, 2022). Through Homeland's Immigration and Customs Enforcement (ICE) branch, the federal agency expanded deputized surveillance to non-white groups; out-groups are defined by ICE *because* of their "non-Americanness" (i.e., whiteness (Ackerman, 2021; Rana, 2010)e): by their immigration status (Yousef, 2022), blackness, or affinity for protesting left-wing multicultural political causes (Tobias, 2019). This points to institutionalizing a particular, non-neutral definition of terrorism strongly associated with a particular group identity. Agencies like ICE have bypassed Congressional limits on, for example, DMV record sharing by engaging with data brokers (Marcetic, 2022) like right-wing activist Peter Thiel's Palantir in order to get license records¹⁵², creating what an insider has called a "secret undercover army" (Arkin, 21).

"Group identities are central to politics" and are a precursor to group membership (Huddy, 2013, p. 737), producing political effects, such as shared political attitudes and mobilization of electoral behavior around the group-level distribution of political goods. Race, in particular, plays an outsized role in American politics (Hutchings & Valentino, 2004). Social identities like gender and religion are also relatively strong mobilizers (Wilcox, Jelen and Leefe 1993, FitzGerald 2017, Beyerlein and Chaves 2020), while sociodemographics like social class or age produce weaker or sporadic levels of political cohesion in the US. Partisan identity is an increasingly mobilizing group identity (Huddy, Davies, & Sandor, 2020). Turow et al. analyzed how political party identities influence positive or negative

gathering community targeted American Muslims and Muslims abroad, and extensive evidence that the military adopted Christian crusade language following 9/11, which affected military identity in ways hard to ignore after the January 6 insurrection.

¹⁵² Other deputized surveillance firms have been providing ICE with utilities records (Harwell, 2021).

feelings toward surveilling welfare benefit users (2018). Another form of group identity, “politicized collective identity”, has been developed by scholars of collective action and social movement. This group identity is formed around political issues and ideological identities, like “pro-environment, feminist, conservative, right-to-life [which] also generate strong political cohesion and drive commitment to social action” (Huddy, 2013, pp. 737 paraphrasing Simon & Klandermans, 2001).

Social psychologists have researched how sociodemographic traits become part of group identities (Tajfel & Turner, 1986). There is also a recent turn towards investigating how people who hold a sociodemographic trait (e.g., being white) come to identify with groups they do not ‘objectively’ belong to (e.g., blacks), and leading to a politicized collective identity that cannot be assumed from a sociodemographic trait (e.g., allyship like white supporters of Black Lives Matter) (Jardina & Piston, 2019).

This work highlights that group identification requires a subjective, internalized sense of belonging (Huddy, 2013, p. 737). Someone with a weakly held white identity might be more likely to support political causes for racial groups they are not a member of, but this will be unlikelier for someone with a firmly held white identity, although both people would describe themselves as white when asked about their ethnicity. Group identification is also not circumscribed to one identity, “[t]he most strongly identified group member is also the one most likely to take action on behalf of the group and adhere most closely to the beliefs shared among group members” (Huddy, 2017).

Social identity theory postulates that we categorize people into groups, identifying with certain groups and contrasting against others (Tajfel & Turner, 1986). Furthermore, these identifications produce favorable and unfavorable biases towards the groups we identify with (in-groups) and the groups we contrast against (out-groups), respectively (Wilder, 1978). These insights motivate using a most-liked and most-disliked design in my experiment.

Intergroup relations are glaringly absent from surveillance studies. As I discussed before, the prevalent measures of privacy concerns draw strongly from Goffman's perspective of the self and our management of identity. Theoretical and empirical work produces a strange tension: it focuses on attitudes towards one's own privacy, but it describes surveillance as having a 'purpose' that happens to others. The erasure of surveillance as a process of monitoring, of a purpose where the data gathered is mobilized to bring to justice (or harm, depending on the author), a target group 'helps' make this jump in logic. Since the motivation or purpose of surveillance is often presented as happening to others, these two common responses in the general public become implicitly linked: "I have nothing to hide" (Solove 2007), and "only criminals have something to hide". Ergo, unless you are a criminal, you should have no reason for rejecting surveillance/desiring privacy.

In my opinion, this makes a study that brings in intergroup relations a contribution to surveillance studies. Disliked out-group relations matter to the study of concerns about targeted surveillance. However, mass surveillance includes monitoring of liked in-group members. I remediate this ongoing oversight of surveillance public opinion studies by focusing on the role of intergroup relations. I engage respondents in a group categorization exercise instead of focusing on the role of a single identity in intergroup relations (e.g., race) (see the Technical Chapter and Methodology below for details).

Chapter 2 measures concern over one's own privacy, so this perspective is not dismissed in the dissertation. However, considering intergroup relations in the study of privacy concerns allows us to go beyond self-interest, especially since online surveillance technologies 'network' decisions about data and consent (e.g., your email preference settings are independent of the preferences of whomever you are emailing). Disentangling respondents' concerns over their own privacy from concerns over others' privacy—liked *and* disliked groups—gives us a broader sense of how people understand the policies and how frames that emphasize disliked groups might even incentivize minimizing one's own

concerns. The frames I describe in the next section should also produce a more genuine informational context of mass surveillance, leading to more refined measures of public opinion.

I hypothesize that acceptance of surveillance will be highest for disliked groups since I expect privacy concerns to be significantly diminished compared to surveillance of liked groups. I also expect differences based on the surveillance policy, where I vary two by their invasiveness—monitoring only or monitoring and involving law enforcement. I hypothesize that respondents will interpret passive monitoring of location as less invasive and thus more acceptable. The design section formally outlines these hypotheses before the vignettes operationalizing the concepts are displayed.

Design

Framing effects “occur when (often small) changes in the presentation of an issue or an event produce (sometimes large) changes of opinion” (Chong & Druckman, *Framing Theory*, 2007) and are increasingly measured with survey experiments (Chong, 2006). One popular experimental design is to randomize which frame each respondent views and calculate the mean difference in response outcomes between respondents’ frame assignments. Framing effect experiments varying the source of terrorism, from “unexpected” foreign sources to ever-present domestic (American) threats (e.g., mass shootings), find that the former is associated with acceptance of reduced civil liberties, but not the latter (Garcia & Geva, 2016). Another framing experiment randomized factors like mentioning the number of terrorism attacks and testing targeted versus mass surveillance in Germany, Spain, France, and the UK. They found increased support when the number of terrorist attacks is referenced and when the scope is targeted, compared to dragnet and the control frame versions (Ziller & Helbling, 2020).

In contrast to between-respondent framing designs, counter-attitudinal evidence or counterarguments can be used to measure changes or reinforcement of attitudes within-respondents who view at least two frames. Between-respondent counterargument designs are often used when

there is “correct” information and incongruent responses; the researcher wants to understand how people can reach different conclusions from informational changes. This design can also directly measure changes in attitudes or preferences. I discuss how both designs were combined in the vignette experiment design subsection.

In the experiment I describe below, I test how mentioning liked and disliked group members affects a surveillance policy’s acceptability. The experiment and hypotheses are pre-registered online (see <https://aspredicted.org/us9cj.pdf>). I build on the social identity theory of intergroup relations (Tajfel & Turner, 1979, 1986) to explain how framing surveillance of disliked group members influences respondents’ acceptability of the policy. I contrast these opinions to when the mass characterization of surveillance is made salient by explicitly stating that out-groups are not the only ones monitored, exemplified by the liked group. I leverage the counterargument design to measure whether people are willing to change their minds when conflicting groups’ privacy is simultaneously threatened, and if so, how drastically. The factorial design of the experiment also allows me to combine the intergroup dynamics with a test on substantive differences of deputized surveillance policies.

To deepen our understanding of attitudes towards surveillance beyond an interest in one’s own privacy, I analyze the role of intergroup relations. I aim to produce a treatment with and without out-group bias akin to mentioning criminals versus everyone else because such vague terms could produce large error measurements. Instead, I ask people to choose from a list their most liked and least liked group members. The categorization exercise is meant to produce social distancing: othering for the disliked group member is contrasted to a relatively closer “ideological” in-group relative to the respondent and the disliked group.

The decision is based on whom they would want most and least as neighbors, invoking physical proximity to boost a desire for ideological proximity and distance. Multiple experiments have found that in-group bias occurs “even when groups are formed on trivial or random criteria”, such as

flipping a coin (Billig & Tajfel, 1973). Something less trivial, like a sorting exercise reminding respondents of physical proximity and distance, should lead to more powerful effects in metaphorical in-group/out-group transient identities than a random coin flip assignation might. Because the selection comes from a list everyone sees, there is also an implicit ranking between groups which, I hope, translates to buy-in when the group is used for the treatment (see vignette experiment design). Furthermore, in the US, geographical sorting is typical, indicates social status, and has pronounced economic and political effects¹⁵³.

This design also makes it possible for me to explicitly center policy preferences away from personal privacy to mass surveillance because it makes it explicit that most others are monitored, not just oneself or criminals. In fact, because hate speech is protected in the US, none of the groups are ex-ante criminals, nor are they criminals by virtue of their politicized collective identity.

I test opinions of two deputized surveillance policies along the soft/hard lines by randomly assigning individuals to one of them. Gary Marx's typology defines soft surveillance by its invisible or

¹⁵³ In the US geographical sorting, intersecting race and reinforcing income disparities, has been institutionalized through several iterations after the Civil War, exacerbated by infrastructure development, the GI bill's racialized support for white home ownership after World War II, redlining mortgage practices (financially and legally backed by the federal government), that racialized school districts. Although efforts like bussing were pursued in the 1990s to desegregate school districts and foster economic mobility in black students, racial and income segregation is higher now than 30 years ago (Bort, 2016; Jackson, 2021). Geographic sorting, is also carried out on the basis of 'imaginary' or internalized social expectations that are then reinforced, producing real consequences on who people's neighbors are. According to a PEW survey, "seven-in-ten urban dwellers say it's important to them to live in a community that is racially and ethnically diverse, but only 52% of rural Americans express this priority" (Fry & Taylor, 2012). The same report calculates that "six-in-ten rural residents say the values of urban dwellers don't align with theirs; 53% of urban residents say the same about the values of those in rural areas" (ibid). This translates into entrenched low mobility between people who perceive themselves to have different values from the opposite community, which folds geographically with party politics, as urbanites identify more with the Democratic Party and rural residents with Republicans. "[P]eople tend to live, marry, raise children, work, and pass away both physically near their birthplace and *in similar social standing* into which they were born (Davis & Miller, 2022, pp. 3, emphasis mine)". The authors of Not my Neighbor elaborate: "the very center of community tensions lays an almost sentimental attachment to the conventions and mores of a time and place in which community members imagine that social, moral, or economic conditions were more ideal, if not more similar. These imagined, historical standards help to reinforce social expectations for community members. They are not natural in any elemental sense, but are, instead, upheld relationally by people. In turn, the demand for or enforcement of homogeneity causes tensions: heterodoxy, running afoul of, or pushing back against traditional normative standards is often viewed as undesirable to the preservation of a community's status quo" (idem, p.4)

relatively “low visibility” techniques (Marx, 2006, p. 38). Hard surveillance involves coercion and the threat of involuntary compliance (Kerr, Barrigar, Burkell, & Black, 2009, p. 10 summarizing Marx).

One way of interpreting this typology is that hard surveillance’s coercion implies law-enforcement involvement as a representation of the legitimate use of force. In contrast, soft surveillance’s low visibility implies ‘frictionless’ data collection that involves no use of force. It may, however, be argued that these distinctions are lost on people in the context of deputized surveillance. Law enforcement’s coerciveness can be less visible to people through market intermediaries’ participation. Deputizing also blurs hard surveillance’s coerciveness by incentivizing the market’s data collection while barring companies from communicating the coercive elements of its transfer to law enforcement (e.g., a duty to report). Instead, it might be the case that surveillance policies that explicitly invoke law enforcement have a spillover effect on intergroup relations. By making out-groups more salient, people might think it more credible that surveillance would monitor out-groups, and thus more desirable to have such a policy in place.

Understanding how people resolve conflictual information is essential to studying public opinion on surveillance. The design’s ability to combine opposing groups highlights how mass surveillance cannot just target some while protecting the privacy of others. Its experimental component bolsters this: randomization varies the order in which the groups are shown and allows for comparison on a controlled subset where either group is absent. A factorial vignette design lets me isolate how people consider policy differences (hard vs. soft) independent from whatever ‘reframing’ effect spills over by emphasizing liked groups (mass) or disliked groups (targeted) surveillance.

Data

Experimental methods are essential for gathering opinions on sensitive questions and causal inference¹⁵⁴. This chapter analyzes an experimental component of the survey introduced in chapter 2. As a reminder, a total of 1,493 American respondents completed the survey distributed by LUCID Theorem between August 9 to 25, 2021. Chapter 2 and the technical chapter discuss at length how the survey is nationally representative in key demographics. The technical chapter also discusses the external validity of online samples and participation by people sensitive to online tracking in online surveys. I specifically address the idea that people who believe surveillance is never acceptable would be absent from online surveys.

To summarize that discussion, people with these views are present. They are not absent from participating in online surveys while holding these beliefs. Similarly, they are not in self-imposed exile from many other online activities. Indeed, one of the issues this dissertation raises is that even those who wish they could extract themselves from online surveillance have very little ability to do so, short of becoming an off-the-grid hermit.

Vignette experiment design

A factorial experiment design uses descriptions of a situation (policy in this case), called vignettes, to construct a “world in which important factors are built-in experimentally” (Hox, Kreft, & Hermkens, 1991). Respondents read similar text with variations along the issues (factors) of interest (i.e., group and policy). Each factor variation is independent of the other, so assignment into one type of group does not condition the assignment into one type of policy. The particular combination of what respondents read depends on random assignation. In this experiment, respondents are shown two vignettes dealing with deputized surveillance and asked for their support or rejection of these policies.

¹⁵⁴ IRB consent requires much more transparency than the real-world conditions in which online surveillance occurs, and unlike psychology which has embraced more overt forms of deception in experiments, political science, drawing from economics’ preferences for paid participation and some disclosure, snubs deception unless absolutely necessary (Druckman, Green, Kuklinski, & Lupia, 2011, pp. 7-9).

The first vignette has a 2x3 factorial design, meaning respondents were randomly assigned to one of two possible policies and one of three possibilities for the group cue. The policy exemplifies either soft or hard surveillance: “passive” location tracking or “active” reporting of online posts to law enforcement, respectively. The policy differences happen at the between-subjects level, meaning the same person only reads one of the policies throughout the experiment. In the first vignette, respondents are simultaneously randomly assigned to one of three possibilities. A third of the sample is randomly assigned to be the control, reading the policy with no group associated with it; a third of the sample is treated by reading the policy in terms of the disliked group, and the remaining third of the sample is treated by seeing the policy discussed in terms of the liked group.

By mentioning liked and disliked groups affected by surveillance, I hope to achieve two things. First, to avoid the most acute form of social desirability bias—the desirability to falsify or present one’s own preferences in a reputation-shielding way (face-saving, see Goffman). Second, I can compare the usually distorted framing of “mass surveillance for targeted reasons” (e.g., detection of criminal or abhorrent behavior, despised groups’ activities (planning terrorism, human trafficking) to the undistorted framing, where everyone is subjected to mass surveillance to prove their innocence continually.

The wording combinations are made explicit below using bold formatting, footnotes, and square brackets for discussion purposes¹⁵⁵. Respondents read a standard-format text (see technical chapter for disaggregated combinations and response distributions).

“In politics, there are often winners and losers. Imagine your representative in Congress is casting a tie-breaking vote for the following policy: **The government will access anyone’s location data from online services**¹⁵⁶. [OR:] **The government requires online services**

¹⁵⁵ See the technical chapter for each combination of the vignette and its corresponding response distributions displayed sequentially.

¹⁵⁶ Soft policy treatment

monitor and report users who violate any law to enforcement agencies¹⁵⁷. This policy affects (most liked group)¹⁵⁸. [OR:] This policy affects (most disliked group)¹⁵⁹. [OR:] [Blank]¹⁶⁰. How would you like them to vote?"

After recording their preference¹⁶¹, the second vignette is displayed.

In the second vignette, everyone is reminded of the surveillance policy they were randomized to see (hard or soft) to alleviate the cognitive burden of remembering its details. This vignette is a counterargument for the 2/3 sample treated with either the liked or disliked group in the first vignette (n=986). They are asked for their preference (same response options) after being told that the opposite group member from vignette one will “also be affected”¹⁶². The 1/3 respondents (n=507) assigned to the control in the first vignette also read the second vignette. They are randomized into seeing either their liked or disliked group for the first time¹⁶³. Thus, for them, the second vignette is not a “counterfactual” in the same way as it is for those treated in vignette one. The full spectrum of possible group combinations in both vignettes is: liked → disliked, or disliked → like, or none → disliked, or none → liked. Respondents read the following, annotated here once more to highlight randomization procedures:

“A report submitted to the committee identifies that this law on government’s access to location data from online services [OR:] requiring companies monitor and report

¹⁵⁷ Hard policy treatment

¹⁵⁸ Liked group treatment

¹⁵⁹ Disliked group treatment.

¹⁶⁰ Control: sentence with any group being affected is omitted.

¹⁶¹ Definitely should not support the policy, Probably should not support the policy, Don’t care, Probably should support the policy, Definitely should support the policy, see Outcome variables measurement section for discussion of coding

¹⁶² If the 1st vignette mentions the liked group, the second will always bring up the disliked group; if the 1st vignette mentions the disliked group, the second vignette will always mention the liked group, forming a counterargument design.

¹⁶³ Formally, those randomized into the control group have a factorial experiment design of 2x3x2. For those randomized into treatment, the full design is 2x3x1, or just 2x3, because the third factor is pre-determined by what they see in the first vignette’s group.

online violations of the law to enforcement agencies¹⁶⁴ would also affect (**most disliked group**) [OR] (**most liked group**)¹⁶⁵. How would you like them to vote?”

Respondents are given the same response options. Substantively, both vignettes’ group options are populated by the specific liked and disliked group members each respondent selected at the beginning of the survey (fifth and sixth questions). Respondents were prompted first, to:

“pick the **ONE** group you would **MOST LIKE** to have as your neighbor. Even if you like more than one, please pick the group that you would **most prefer** to have as a neighbor.”

The ten options, displayed in random order, but separated here, are:

[Conservative group memberships:] a Second Amendment activist, a climate change skeptic, a member of the Ku Klux Klan, a religious fundamentalist, an anti-vaxxer,
[Liberal group memberships:] a homosexual person, an immigrant, a member of Black Lives Matter, a feminist¹⁶⁶, an atheist.

In the following survey question, they were told:

“We will now show you **a similar** list of groups of people. This time, please pick the **ONE** group you would **NOT LIKE** to have as your neighbor, your **LEAST** preferred group.”

The response option shows the same groups in random order, removing the most liked option picked in the previous prompt. A visual tick  and cross  accompanied the liked and disliked prompts to aid readers’ understanding of the instructions. The 10 groups in randomly listed order were chosen because of their current role in politically charged debates and association with left-right ideology, although they were not identified as such in the survey text. One crucial element to all these groups is that none of these group membership categories are criminal. Even the KKK’s members have

¹⁶⁴ Policy treatment repeats hard or soft assignation from vignette 1

¹⁶⁵ Randomized for those in control assignment for vignette 1, opposite group for those treated in vignette 1.

¹⁶⁶ A feminist is more general than pro-choice but would catch those who prioritize pro/anti-choice issues because abortion support has been closely tied to attitudes towards feminism since the 60s (Williams, 2011).

repeatedly received First Amendment protections from Supreme Court decisions¹⁶⁷, as hate speech is legally protected in the US. I constructed this list following critiques about the emphasis of left-wing groups in the early political tolerance literature (Sullivan, Marcus, Feldman, & Piereson, 1981). The list's 50/50-balanced representation of left-right debates also brings in different salient issues: race, gender, religion, and political issues like climate, guns, immigration, and vaccination. This increases the probability that respondents will pick a group that produces an “emotionally involving” response (Amodio & Devine, 2006).

Information on choice variation can be found in Table 8. However, the substantive answer is not analyzed when testing the response outcomes. The objective is to produce a sorting exercise that produces in-group favoritism and out-group animosity¹⁶⁸. While the groups displayed are “self-selected” in the sense that respondents are responsible for categorizing which is the most liked and the most disliked to them, respondents *are* randomized into treatment assignment (treated or not), and the polarity when treated (liked or disliked in vignette one or two). Thus, the vignettes are expected to: provide readers with a distance between concerns over their own privacy and concerns over everyone else's privacy, to emphasize that mass online surveillance goes beyond reviled groups by highlighting that liked groups are also monitored, and to use personally salient examples as the cherished groups. The exercise is meant to mobilize closer and distant politicized collective identities relative to each other and the groups that are not selected. The breadth of the groups in the list tries to ensure that most people find one member highly appealing and one highly unappealing when the vignettes are read. I build on previous work on intergroup relations to argue that the sorting exercise

¹⁶⁷ *Brandenburg v. Ohio* in 1969, *Capitol Square Review Board v. Pinette* in 1995, and *Virginia v. Black* in 2003 upheld KKK 1st Amendment speech rights.

¹⁶⁸ As with most non-clinical experiments, treatment cannot be fully ensured. It is possible that some respondents pick groups randomly, do not pick the most liked/disliked but just generally liked, or that they try to anticipate why this question is asked and deliberately give opposite responses. These will introduce noise to the measure, but that is accounted for in the measurement error. There is no reason to expect that all or a specific subset of respondents will engage in one of these three systematical mis-reporting strategies, ignoring/sabotaging these questions and thus , impacting the treatment.

produces a relative comparison between disliked and liked groups. While this is not a comprehensive list of politically salient groups, I do not foresee having left out a particular group in a way that makes the most/least choices systematically faulty¹⁶⁹.

To reiterate, the vignette experiment tries to capture people's attention and make explicit mass surveillance by engaging in a social categorization of emotionally involving and politically salient groups. The objective is to make respondents aware of the conflict in policy implementation with mass effects on a broad range of people, compared to the usual framing that mobilizes deviant, disliked groups.

When treated, the liked and disliked group order is randomly assigned to the experiment's manipulations. The sorting process boosts group membership dynamics; it underlies social identity mechanisms that produce bias against an out-group and favor in-groups by comparison (see coin flip experiments). Comparing respondents who see liked and disliked groups is important because mass online surveillance produces *competing* claims. Society cannot simultaneously protect liked groups' privacy while disliked groups are surveilled for three reasons. First, there is no societal consensus on who (from our list) is an out-group. Second, American privacy rights are¹⁷⁰ anchored in a combination of the 4th Amendment's search and seizure interpretation and the 14th Amendment's equal protection clause, which means privacy is not a privilege. Third, the technologies are tautologically designed to collect all networked communications first (haystack), sifting later for targets (needles).

Directing considerations toward collective interests also may avoid social desirability bias in responses to self-interest-based questions. If people perceive that others believe "only criminals have

¹⁶⁹ The breadth of the groups tries to ensure that some people will identify with the politics of the groups. If everyone fails to do so, if I find liked groups lead to rejection of surveillance, the effects are thus conservative. That is, even when the most liked group is held in weak esteem relative to the missing most liked group, there is still some

¹⁷⁰ The Supreme Court's decision on the Mississippi abortion law (Dobbs) reverses *Roe v. Wade* on this specific point ("the penumbra of privacy") and required upending the combination of Amendments into an implicit right. The consequences for the legal interpretation of privacy rights as implicitly rooted in the equal protection clause remain to be seen, but the core argument in the Alito decision is that this basis should be severed.

something to hide”, they might falsify their preferences over their own desire for privacy. They might publicly state accepting more surveillance than they prefer to avoid grouping themselves with the group viewed as wanting privacy, namely criminals and those with something to hide. Introducing a scenario where liked group members are also harmed by more surveillance (or, de facto, benefit from less surveillance) allows people to respond on behalf of in-groups without the stigma of association with out-groups.

Hypotheses

The pre-registered hypotheses are broken up into two different axes. On intergroup relations, I hypothesize that:

- 1) Acceptance of deputized surveillance policies is driven by a willingness to surveil the disliked out-groups. When mass surveillance makes the most disliked group explicit, acceptance will increase (out-group bias) compared to all other group manipulations.
- 2) Deputized surveillance policies are more likely to be rejected when liked groups are explicitly affected (in-group favoritism) compared to all other group manipulations.
- 3) Viewing opposite groups does not produce symmetrical reactions. For respondents who see both groups, liked group surveillance will engender weaker rejection compared to a stronger desire to surveil disliked groups. This is because othering disliked groups produce out-group bias, but the liked group is an imperfect operationalization of a relative ideological in-group.

On the soft/hard dimension of deputized surveillance policies, I hypothesize that:

- 4) Acceptance of surveillance is influenced by its perceived invasiveness:
 - a. “Soft” surveillance, instrumentalized as *only* monitoring and exemplified by the location policy, will be more acceptable because it is less perceptibly obtrusive; whereas,
 - b. “Hard” surveillance, instrumentalized as a policy of monitoring *plus* acting on the data by reporting it to law enforcement, will be less acceptable because this requires an element of state coercion.

In the Appendix, I conduct additional analyses with logistic and multinomial regressions to understand steadfast respondents who do not change their opinion since this is exploratory and outside the pre-registration.

Outcome variables measurement

Both vignettes' response options displayed: Definitely should not support the policy, Probably should not support the policy, Don't care, Probably should support the policy, Definitely should support the policy. When analyzing each vignette outcome independently, the responses are scaled from 0 to 4 in ascending support. To test hypothesis 3, I calculated a change score, taking the difference in opinion for each respondent between the first and second vignette, rescaled from 1 to 5 so the 0 value would not interfere with the subtraction. When the response differs from "Definitely should support the policy" (5) in vignette 1 to "Definitely should not support the policy" (1) in vignette 2, the change score is coded as -4, which is the biggest reduction in acceptance. When the change in direction from vignette 1 to vignette 2 goes from strongly disagreeing to strongly agreeing to support the surveillance policy, the change score is coded as +4, the largest growth in acceptance. When the respondent is steadfast in the response choice between both categories, the answer is coded as 0. All possible combinations and coding are described in this chapter's Annex, Table 10 Change score combinations, coding, and frequencies.

Confounder variables

Random assignment into treatment should make other variables (e.g., sociodemographics) extraneous and thus should not influence the treatment. I also test for balance within treatment groups in both vignettes along several pre-treatment variables that could lead to differential treatment effects or a difference in willingness to complete/submit the survey (P.D.Mehta, 2001). As with sociodemographic characteristics, I find that self-monitoring¹⁷¹, mean deputized surveillance

¹⁷¹ Following Connors, Krupnikov, and Ryan (2019), self-monitoring averages two responses coded as 1 for yes and 0 for no to the statements: "You are often the center of attention" and "You try hard to impress other people" (sample mean 0.28). This measure accounts for individuals' propensity to alter their recorded opinion on surveillance due to intrinsic personality traits. Self-monitoring respondents are "chronically concerned with the appropriateness of their interpersonal behavior. They carefully regulate their self-presentation concerning social norms and contexts. They thus are highly responsive to social and interpersonal cues" (Berinsky & Lavine, 2011, p. 27). In contrast, low self-monitors "manifest consistency between their private attitudes and public actions" (Snyder, 1987), including during survey responses. Those prone to self-monitoring could be subject to heterogeneous treatment effects because they are averse to being seen as punishing a group they think is liked by others with surveillance and willing to display more punishment to a group they

acceptance (chapter 2's measure)¹⁷², mean worries of future personal impact of privacy violations or past experiences with them, mean institutional trust¹⁷³ and knowledge of privacy measures¹⁷⁴ are all balanced between randomized treatment groups in both vignettes.

consider disliked by themselves and others. For example, according to Terkildsen, high racial prejudice respondents with low self-monitoring evaluate dark-skinned candidates more negatively than an identical light-skinned candidate. Still, high-self-monitoring with similar high racial prejudice scores seemed to be aware that they held a minority opinion and compensated much higher support for dark-skinned candidates (1993). A similar dynamic of hiding negative racial views has been documented (Feldman & Huddy, 2005). In research like this, it is essential to check for balance on self-monitoring, because the categorization exercise and treatment will display BLM and KKK members, which tap into racial attitudes. If the treated groups were unbalanced in the proportion of individuals with high-monitoring compared to the control group, their expression of willingness to surveil a disliked group could be impacted by that characteristic. Individuals with low self-monitoring may be more willing to surveil disliked BLM members compared to other low self-monitoring respondents who picked a different disliked group as an outlet of their high racial prejudice. However, this concern is alleviated by the fact that there is no statistically significant difference in the self-monitoring characteristics of the treated and untreated groups.

¹⁷² Pre-treatment attitudes towards deputized surveillance may predetermine the range of the responses a person is willing to entertain when surveillance policies are directed at specific groups, if these attitudes were not balanced between the randomly assigned groups. Along the same lines, concern over one's privacy, also discussed at length in chapter 2, might impact whether respondents are more empathetic to the displayed group's privacy being harmed. Individuals' averaged measure of personal worries about online behavior exposure is also tested for balance, which I find.

¹⁷³ A common alternative hypothesis for the acceptance of surveillance is that trust in institutions (government or corporate) motivates complacency, agreement, or skepticism over demands for data (Hampson & Jardine, 2016; Viola & Laidler, 2022; Radden Keefe, 2005). I test for balance and find no differences in trust between treated and control groups. Still, I conducted a robustness check where I control for individuals' average institutional trust, measured by a battery that asks: "For each item listed, how much confidence do you have in...": The Federal government, the Supreme Court, local government, teachers, police, doctors, preachers, journalists (scale is none at all (0), a bit, some, a lot (3), sample mean 1.62, Cronbach's alpha: 0.81). The effects from intergroup and policy factors in the vignette hold.

¹⁷⁴ Knowledge of surveillance practices might also act as a treatment confounder if the policies' realism is questioned. In particular, people who make use of privacy-enhancing technologies might have systematically different responses to mass surveillance policies because they are aware of the ubiquity in which online surveillance takes place. They may be less willing to accept surveillance in any circumstance, and thus resistant to the intergroup relations treatment. However, this concern is alleviated by the fact that there is no statistically significant difference in knowledge, measured as single average or individually (VPN, cookies, law, and incognito browsers, see Technical Chapter)

Results

The distribution of substantive group choices is presented in the table below before moving onto the hypothesis testing results.

Liked Group		percent	Disliked Group		percent
members of the Ku Klux Klan		1.30%	immigrants		2.40%
anti-vaxxers		2.00%	climate change skeptics		2.90%
climate change skeptics		7.40%	feminists		3.30%
atheists		8.40%	homosexuals		4.30%
feminists		9.10%	anti-vaxxers		4.60%
religious fundamentalists		9.50%	religious fundamentalists		5.50%
immigrants		13.40%	atheists		6.00%
members of Black Lives Matter		13.90%	gun rights advocates		6.20%
homosexuals		16.20%	members of Black Lives Matter		15.80%
gun rights advocates		18.70%	members of the Ku Klux Klan		49.00%
Ideological categorization	Leftwing	61%	Leftwing		32%
	Right-wing	39%	Right-wing		68%

Table 8 Group distribution

Half the sample chose the KKK as the disliked neighbor, which is in line with previous findings that there is waning tolerance for intolerance (Chong, 1993; Nelson, Clawson, & Oxley, 1997; Harell, 2010). There was more thematic diversity among the liked groups. The differences in choices justify my approach, which allows respondents to pick a salient group to exemplify who is impacted by surveillance. The left-skew of groups may partly reflect partisanship since 43% of the sample identify as Democrats, 29% as Independents or other, and 29% as Republicans (the Gallup poll of August 2-17, 2021, had a partisan distribution of 29% Democrats, 40% Independents, and 28% Republicans).

All visual representations of support have the response scale's mid-point demarcated by a red line that translates "don't care" responses numerically (2); the full range of the scale on the y-axis conveys the full spectrum of possible support. I present visual averages of answers concerning the hypothesis and then point out substantively significant heterogeneous effects. I then present the findings from regression analysis.

Overview: Group-based surveillance

All group manipulations from the first vignette (n=1493) are analyzed and discussed throughout this section. However, I focus on the treated respondents (n= 986) when examining the second vignette by subsetting them when discussing hypothesis three's change score test. I do this because people assigned to the control in the first vignette cannot be directly compared to those who received a true counterfactual when analyzing the second vignette¹⁷⁵. Within the control group, the second vignette should emulate the results of the treated group's first vignette: randomization into reading the vignette with the disliked group is associated with higher acceptance of surveillance, while reading it with the liked group is associated with lower surveillance acceptance. The control group's second vignette results are substantively discussed in the Appendix. Their responses are considered a robustness check that intergroup affect manipulation drives the results regardless of either vignette's non-manipulated wording¹⁷⁶.

The second component of the experiment hypothesized that stating disliked groups would be affected by mass surveillance would increase acceptance of a given policy (H1). Clarifying that the policy will impact the liked group is associated with reduced acceptance (H2). In both vignettes, average support¹⁷⁷ for deputized surveillance is lower for the liked group relative to the disliked group frame and below the “don't care” threshold (red line, coded as a “2” in the 0 to 4 scale in Figure 12). In the first vignette, viewing the liked group produces statistically significantly lower levels of support¹⁷⁸ compared to no group mention (means are 1.82 and 1.96, respectively), since the 95% confidence intervals do not overlap¹⁷⁹. Both categories are visibly lower than support for surveillance

¹⁷⁵ The pre-registration explicitly outlines that H3 analyzes treated respondents because only these see both groups.

¹⁷⁶ The results from vignette 2 are practically the same in the full sample and the subset sample.

¹⁷⁷ Pooled support for vignette 1 = 2.05, vignette 2 = 2.17 for the total sample, and 2.196 when restricted to the treated subsample.

¹⁷⁸ In fact, since the mean and confidence intervals are below the neutral “don't care”, we should characterize it as statistically significant levels of rejection of surveillance.

¹⁷⁹ The maximum estimated average for liked group surveillance is 1.88 support, and the minimum estimated for the control assignment is 1.90.

of disliked groups (mean = 2.36). Excluding the untreated from the second vignette from analysis leads to virtually no difference in average support for the second vignette (Liked = 1.95, Disliked = 2.45, n = 986) compared to their inclusion (Liked = 1.92, Disliked = 2.43, n = 1493).

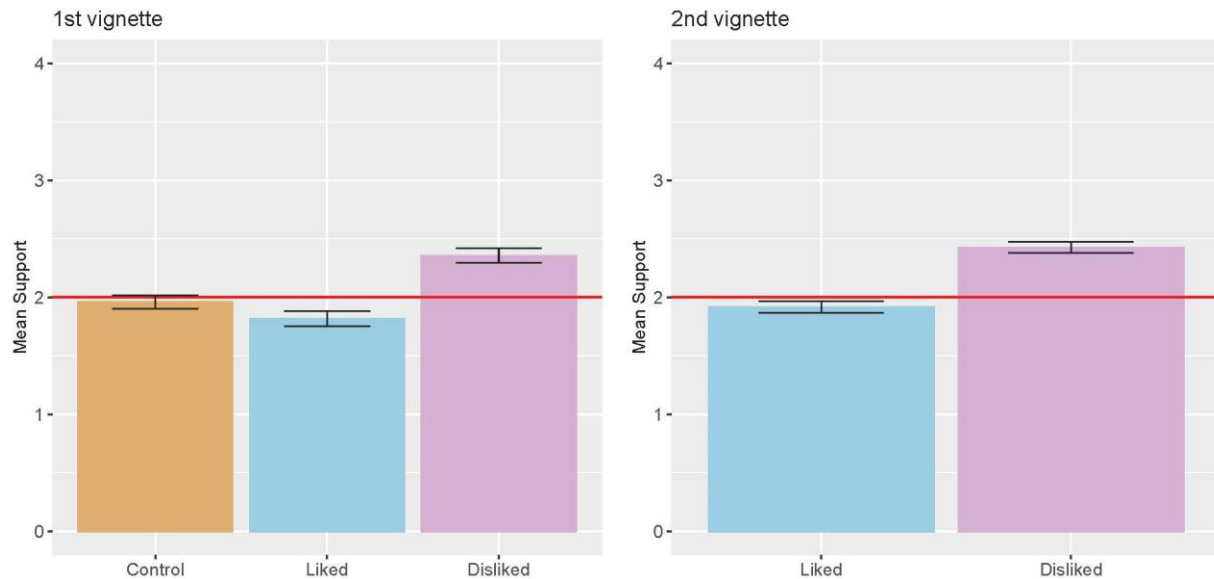


Figure 12 Average response to group

To test hypothesis (3) that disliked group bias is more potent than liked group favoritism, I restrict the sample to the 986 respondents who saw both groups (treated in vignette 1) and analyze the order in which the group polarity was presented, comparing liked → disliked to disliked → liked vignette sequences¹⁸⁰. The expectation is that it will be harder for people to reject surveillance when the liked group frame is presented after the disliked group. This means that each group frame doesn't produce a response of similar magnitude, but in opposite directions, they are weighted differently in people's consideration of what policies should apply collectively. The change in opinion among those who saw the liked → disliked sequence should be a bigger acceptance of surveillance compared to a smaller rejection of surveillance among those who saw the disliked → sequence¹⁸¹. Viewing the disliked group

¹⁸⁰ The findings discussed below hold for untreated respondents; see annex Figure 16.

¹⁸¹ Another way of interpreting this is that it is easier to change a person's opinion from the position of considering a liked group first, and then a disliked group than it is when the order of groups presented is reversed.

first should contribute to a hawkish attitude towards accepting surveillance that is harder to sway with appeals toward liked groups. Viewing the liked group first should produce a dovish attitude towards rejecting surveillance, which is more easily countered by appeals to surveilling out-groups.

To understand how people react to new and conflicting information, comparing both sequences, I calculate a change score that ranges from -4 to 4 (see Outcome variables measurement and Table 10 in Appendix). Within the treated sample, 47.57% of respondents changed their opinion between both vignettes, while 52.43% remained steadfast in the experiment responses. The Appendix's Sankey (Figure 18) visualized the subsample's path in opinion change, including the relevant policy response from the surveillance complex battery discussed in the previous chapter.

The average change in opinion (visualized in Figure 13) was more noticeable when the second vignette revealed the disliked group (0.63 [CI 0.57, 0.693]) compared to when the liked group was shown after the disliked group (-0.40 [CI -0.34, -0.461]). In absolute terms, the size of the opinion change is statistically significantly different between sequence orders (see appendix Figure 17 for absolute size of change visualization). I conclude that despite knowing the policy would harm a liked group, awareness that a disliked group would also be surveilled made it easier for people to a) change their minds and b) change it by becoming more accepting of surveillance. Relevant to the 3rd hypothesis, this finding supports the argument that the motivation for acceptance of surveillance is out-group bias. In-group favoritism can curtail this impulse but cannot equally overcome the desire

to surveil disliked people. In other words, the willingness to surveil disliked groups can override any caution from an awareness that liked groups suffer, so they get thrown under the bus.

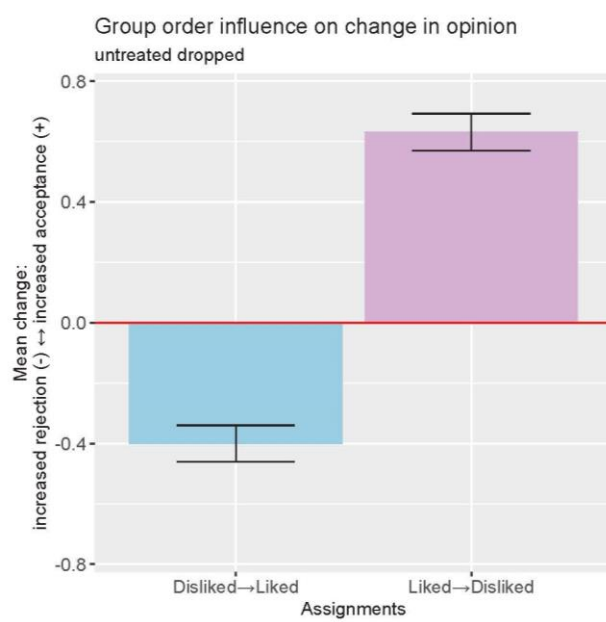


Figure 13 Average change in response given group sequence

Overview: Soft or hard surveillance policy

1,493 respondents were randomly assigned to view one of the two policies throughout the experiment¹⁸². The policy distribution for geolocation was $n = 747$, and for report for, $n = 746$. In contrast to the hypotheses (4a and 4b) that soft surveillance (location) would be more supported than hard surveillance (reporting), average support for acceptance of government use of corporate location surveillance data is markedly lower than support for online services monitoring and reporting users to law enforcement. Relative to each other, the mean differences are statistically significant (1.7 and 2.39, respectively), as conveyed by the lack of overlap in 95% confidence intervals and below and above the indifference (“don’t care”) red line in Figure 14. Those reading the geolocation policy become

¹⁸² The policy is randomized between-respondents but constant within-respondents. As the vignette design section explained, the second vignette reminds the respondent that the [same] policy they considered in the 1st vignette will also affect X group.

slightly more accepting in the second vignette (1.90 compared to 2.44 for reporting), but that increase is still lower than support for monitoring posts and reporting unlawful ones. This is consistent with acceptance rates in the deputized surveillance battery discussed in chapter 2, from which the policies are drawn¹⁸³.

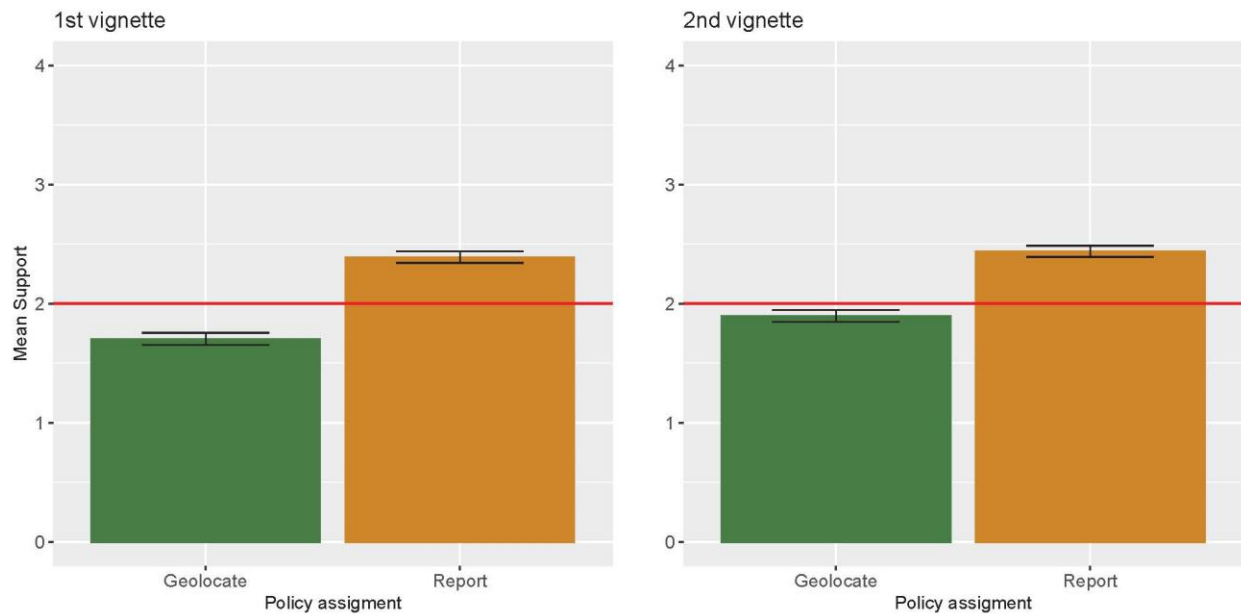


Figure 14 Average response to policy

This finding went against the mechanism theorized by Marx and echoed by Kerr et al., who expect an increase in coercion regarding how data is obtained to increase resistance to it. The statistically significant difference in mean support in the vignettes that described soft surveillance (anyone's geographic data being collected) compared to the hard surveillance policy (monitoring for law-breaking and reporting those posts to police) subverts their expectation that mass collection of data which operates in the background elicits less resistance compared to mechanisms that involve the state's coercive power.

¹⁸³ As a reminder of Chapter 2 findings, government access to monitored corporate geolocation data, the softest of the four policies in the deputized battery, drew the smallest support: strong or somewhat accepting totaled 50.7%. Meanwhile, the deputized reporting policy, the "hardest" surveillance policy currently only in effect in Germany (NetGD law), produced the most support, with 72% agreeing somewhat or strongly with it.

Location monitoring is ubiquitous in commercial online interactions and is one of the pieces of information the government has routinely categorized as “metadata”, seeking to exempt from any privacy protections. Although geolocation is widely used, it is not widely supported. It may be the case that the geolocation frame emphasizes the universality of surveillance by mentioning accessing “anyone’s location”, while the alternative frame emphasizes “report[ing] users who violate the law”. Even though both require monitoring everyone’s data, the cue focusing on law-breaking may reinforce the idea of a criminal association. It may be the case that people perceive geolocation surveillance to be more coercive *because* universal data collection is not ‘mitigated’ by subsequent use of the data that is post-facto justified once criminal behavior is identified.

Despite many governments’ attempts to normalize the use of deputized location data from apps during the pandemic, scrutiny over the government’s access to commercial data has increased where anti-choice states seek to access or buy the data to enforce post-Dobbs restrictions on abortion. These mean differences show that the theory behind the typology is not as settled or clear-cut as expected. Perhaps, rethinking how people conceptualize what makes a policy invasive, coercive, or frictionless and how this intersects with their acceptability warrants further mixed-methods research.

Regression analysis

The mean differences of both manipulation conditions suggest that I can reject the null hypotheses of *no* policy or group effects, but the mean differences do not account for the treatment effect of each manipulation simultaneously. As discussed in the confounder variables section of the Methodology, the assumption that average treatment effects are homogenous on several variables relevant to surveillance acceptance, such as self-monitoring, worries over the fallout of online participation, institutional trust, etc., can be put aside as these variables are balanced between the treated and

controlled (see Appendix for robustness check regression where I include these regardless¹⁸⁴, ¹⁸⁵).

Using OLS regression, I only model the experiment conditions' responses for vignettes one, two, and the change between both vignette responses. Results are presented in Table 9 and graphically visualized in Figure 15.

OLS regression results

Vignette:	Models		
	1st	2nd, only Treated	change score (-4 to 4)
(Intercept)	1.62*** (0.07)	1.68*** (0.07)	-0.39*** (0.07)
Liked (ref Control)	-0.14 (0.08)		
Disliked	0.40*** (ref Control) (0.08)	0.50*** (ref Liked) (0.08)	
Policy: Report (ref Geolocate)	0.69*** (0.07)	0.55*** (0.08)	-0.01 (0.09)
Liked then disliked (ref Disliked then liked)			1.03*** (0.09)
R ²	0.09	0.07	0.13
Adj. R ²	0.09	0.07	0.12
Num. obs.	1493	985	985

*** p < 0.001; ** p < 0.01; * p < 0.05

Table 9 vignette 1, 2 and change score OLS results

Hypotheses 1 and 2 led to the expectation that a given deputized policy is accepted when the targeted group is disliked. However, when the policy is shown to target liked groups, deputized surveillance policy gets less support. Models for vignettes 1 and 2 confirm a statistically significant effect on acceptance (positive sign) when the group is disliked, whether the reference group is the control version (vignette 1, 9.75% increase on the 0 to 4 scale) or the liked group (vignette 2, 11.75% increase

¹⁸⁴ Despite being balanced and not affecting the substantive effects, the goodness of fit of the first and second vignette models is improved with their inclusion (0.28 for both) but the adjusted R² is also 0.12 for the change score model.

¹⁸⁵ Sociodemographic variables are statistically and substantively irrelevant to differences in responses and have no effect on model fit.

on the scale). Vignette 1's reference category is control. This lets me estimate how a frame involving mass online surveillance targeting various groups, including liked groups, shapes its acceptance. The introduction of a liked group in the vignette is associated with waning support for the policy at a statistically significant level, as hypothesis 2 outlined.

In vignette 1, the substantive effect of targeting the most-liked group (-0.18 or a 4.5% decrease on the 4-point scale) is relatively smaller than the least-liked group effect, as expected in hypothesis 3. The 3rd hypothesis can be further analyzed by looking at the aggregate impact of the sequence in which arguments are presented. Results for vignettes 1 and 2 are restricted to respondents who saw both groups. In the third model, the size of the change in opinion score is calculated on a -4 to +4 scale that measures *increased rejection* to *increased acceptance*. Respondents increased their approval on the 8-point change score scale by 13% when presented with surveillance of the disliked group *after* becoming aware the policy will surveil the liked group, compared to when the vignette revealed the liked group *after* the disliked group. Respondents are generally conscious that liked groups will be surveilled and are even willing to change their minds to become less cautious. However, they are willing to throw their liked groups under the bus when out-group bias is triggered.

The statistically significant difference in sequence tells us that targeting the most liked group does not produce a similar effect when the sequence is reversed. People are less willing to change their minds about rejecting surveillance when the liked group is brought up after bringing the disliked group into focus. In other words, when people are confronted with the fact that mass surveillance does not just target disliked groups, people accommodate liked groups' surveillance. This is an essential insight towards explaining why revelations of mass surveillance did not produce the fierce, sustained indignation required to end these programs. The cumulative process I identify is vital because, as explained in chapter 1 and this chapter's introduction, all actors publicly justify the surveillance complex in terms of security (national safety, economic fraud, etc.) in ways that require complicit

tradeoffs of our own and everyone else's privacy to "go after bad guys". The two vignettes, analyzed individually and collectively, show that the mechanism at work relies on out-group bias.

My expectations for hypotheses 4a and 4b, categorizing geolocation as soft surveillance that would elicit lower rejection compared to hard surveillance reporting posts, would require the signs of the regression to be reversed. If the randomly assigned policy is post surveillance with law enforcement reporting, respondents are 16.25% (on the 4-point scale) more accepting in the first vignette and 12.75% in the second vignette, independent of intergroup relation dynamics. Policy differences play no statistically significant or substantive role when analyzing the change of opinions (model 3). This suggests that people's contextual references are more sensitive to intergroup dynamics than the scope of surveillance becoming more or less constrained/clear. As a robustness check, I modeled the factors as interactions. The independent effects are robust to this specification across the three models, and there was no statistically significant effect in the interactions.

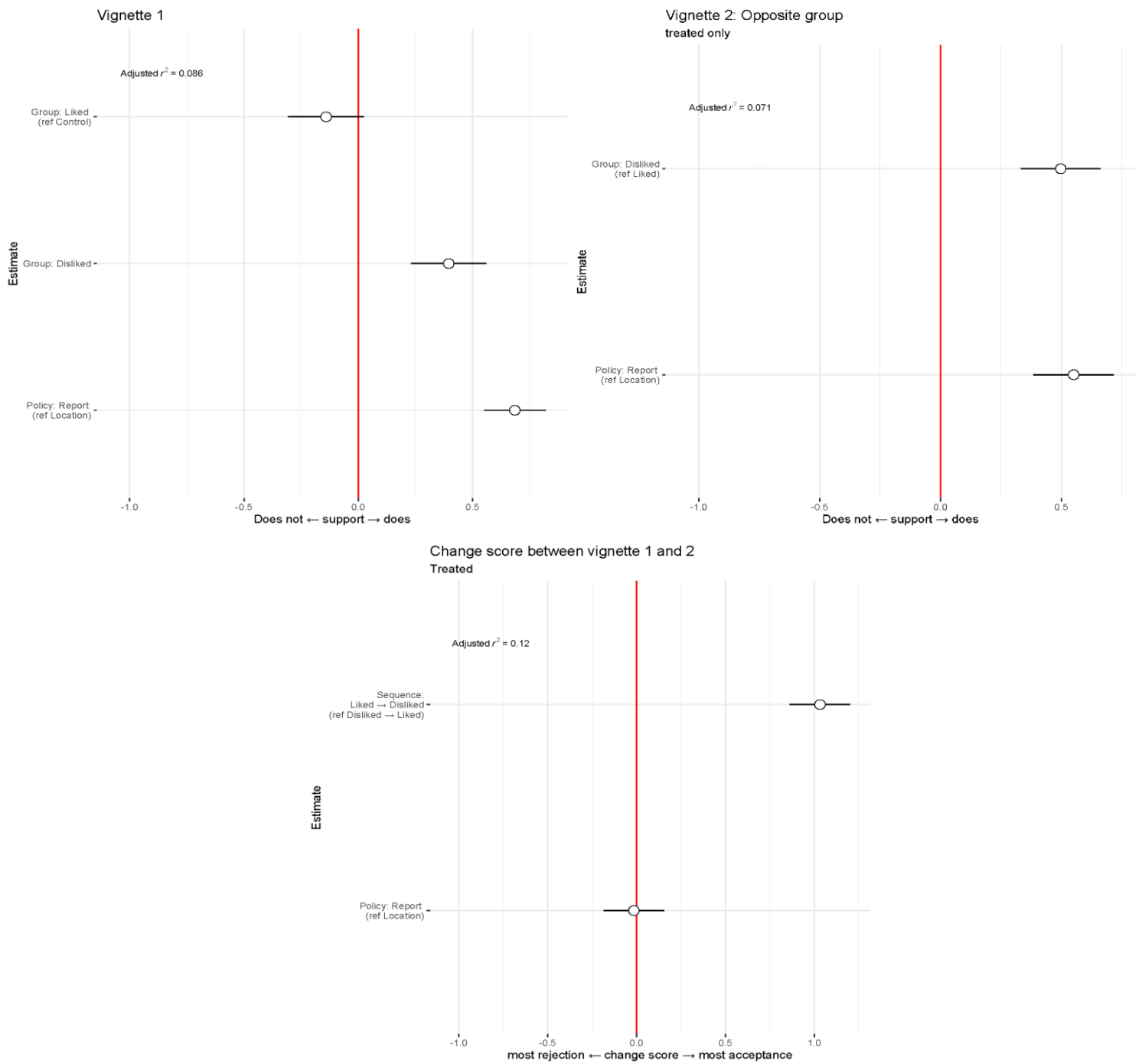


Figure 15 Visual representation of coefficient estimate effects per model

Conclusion

In this chapter, I identified an important gap in the literature on privacy attitudes: the role of surveillance of *others*, and I tested this influence. Comparisons of respondents who see liked and disliked groups are important because mass online surveillance produces *competing* claims. As I argued in the design section, society cannot simultaneously protect liked groups' privacy while disliked groups are surveilled.

I hypothesized that beyond concerns over one's own privacy, acceptance and rejection of surveillance are partly influenced by competing intergroup relation dynamics of favoritism towards liked group members and bias against disliked group members. I also hypothesized that differences in policy invasiveness would influence respondents' willingness to subject liked or disliked groups to surveillance. I proposed to test how attitudes toward others shape acceptance of mass surveillance with a factorial vignette design that provides a path forward for practitioners.

These hypotheses tease out how understandings of surveillance's purposes are shaped by frames that come from media, politicians, and law enforcement. Different policies implicitly, "incidentally", and deliberately make salient a multitude of groups with competing claims to privacy, producing heterogeneous support or rejection across American society. Over the past twenty years, when discussion of mass online surveillance becomes unavoidable, governments and corporations engaged in deputized surveillance have shifted focus toward the subsequent data use on disliked groups—vaguely described as criminals or terrorists.

Using an original survey with experimental features, I simultaneously manipulated group and policy factors to estimate responses toward each element independent of other variables. The particularities of the design allowed me to compare the differences between subjects randomly assigned to different groups and policies at the same vignette stage (1 or 2). Using regression analysis, I found support for the hypothesis that at statistically significant levels of difference, when mass

surveillance policies explicitly framed a group as being affected, responses would vary in their support or rejection in a systematic direction. Support for surveillance was higher when respondents were explicitly told disliked groups would be affected compared to when respondents were shown the same surveillance policy but no group (vignette 1). In contrast, reticent attitudes towards the same surveillance policy were manifest when the frame made explicit that liked groups would be surveilled compared to no group (vignette 1, substantively but not statistically different) or disliked groups (vignettes 1 and 2). These hypotheses were supported by the analysis of between-respondent (models 1 and 2) and within-respondent (model 3) answers.

There is more consistency in attitude along policy lines. Respondents' attitudes on two deputized surveillance methods carried over from the normative policy preferences asked before the experiment discussed in chapter 2. Based on previous theoretical work, I expected respondents would reject a mandated duty to monitor and report to law enforcement at higher rates. This practice is considered to be more invasive, actively requiring decision-making, more visible, and producing friction. Thus, surveillance scholars expect this policy to be less acceptable to the public. The reality of location data gathering practices complicates the hard/soft typology. Apps and websites ubiquitously collect location data¹⁸⁶ in the background (metadata, Bluetooth, GPS, cell tower pings), but permissions requests and services that make this feature central (from Uber to proximity-based dating apps) enhance the visibility of this data collection. However, its routineness has not resulted in its normalization in absolute terms (mean support tended towards rejection in both vignettes) or relative terms (substantively lower acceptance than reporting).

The more burdensome and novel policy, which could be characterized as government over-reach because of its mandate on private companies to conduct active policing duties, was more acceptable to respondents, independently of the group displayed. The only government to require

¹⁸⁶ And routinely obtained by law enforcement, even if the surveillance complex obscures this element.

online services to monitor and report users who violate hate-speech laws to enforcement agencies in Germany, which has one of the most stringent and proactive hate-speech regimes in Western democracies. This suggests a range of policies that might be considered ‘too extreme’ or too heavy-handed might, in reality, be acceptable to Americans if disliked groups, amorphously criminalized, are made salient.

Future research should research the distribution of preferences over a broader range of techniques, opinion plasticity/rigidity, and rigorously test whether the soft/hard dimensions are heuristics people rely on or whether the acceptability of specific techniques hinges on some other technological or institutional characteristic. The precise mechanism by which people regard a particular surveillance policy as permissible needs to be researched in-depth with a focus on more policy variation and wording to identify what people understand and emphasize from a range of possible policies. This also highlights the dynamism between policy supply and demand—studying opinions without the context of why a certain supply of policies and their justifications are available makes it hard to understand how demand is mobilized or immobilized.

The OLS models had goodness-of-fit statistics aligning with or surpassing previously published experimental studies on European government surveillance acceptance (Ziller & Helbling, 2020), while introducing a novel perspective to explaining attitudes towards deputized mass surveillance (intergroup relations). In contrast to some small-sample research on non-representative American attitudes towards government and market surveillance, sociodemographic characteristics intrinsic to respondents play no role in the surveillance vignettes’ responses. Lastly, a proportion of respondents randomly assigned to treatment failed to be swayed by the conditions of the experiment. I produced an exploratory analysis in the Appendix, outside of the pre-registration plan, to understand these respondents’ response choices. The results suggest that public opinion volatility is not as absolute, but that marginalization from politics (institutional trust and disinterest) plays a more

significant role in recalcitrant opinions. This is an encouraging space where political science can contribute to interdisciplinary surveillance studies.

The experiment's liked and disliked response variation exemplifies how there is no societal consensus on who is an out-group; half the sample did not pick the KKK. After the Dobbs decision, American privacy rights seem to be undergoing judicial and political revision. A fundamental tension seems to be whether privacy will remain a right or a privilege. Technologically, however, networked communications are designed to monitor all communications first (haystack) and retroactively sift for targets (needles). One person's decision not to secure their communications puts others' privacy at risk, creating a collective action problem, where we become complicit in others' surveillance when each person decides 'I have nothing to hide'.

Explicitly shifting the conversation towards collective privacy interests may also help us avoid tapping into a social desirability bias, in contrast to self-interested privacy questions. If people perceive that others believe "only criminals have something to hide", they might falsify their preferences over their own desire for privacy. People might publicly state accepting more surveillance than they actually prefer to avoid grouping themselves with the group viewed as wanting privacy, namely criminals and those with something to hide. Introducing a scenario where liked group members are also harmed by more surveillance (or, de facto, benefit from less surveillance) allows people to respond on behalf of in-groups without the stigma of association with out-groups. However, the experiment shows the limits of sympathetic frames. Americans seem willing to reconsider their opinion of mass surveillance and throw under the bus liked groups in order to surveil disliked groups. If people do not accommodate the privacy rights of diverse liked groups to the same extent as they accommodate for surveillance of disliked groups, we end up in a situation where everyone has a reason for accepting mass surveillance, or at the very least, a reason for not mobilizing against it.

Bibliography

- Ackerman, S. (2021). *Reign of Terror: How the 9/11 Era Destabilized America and Produced Trump*. New York: Penguin Publishing Group.
- Amodio, D. M., & Devine, P. G. (2006). Stereotyping and evaluation in implicit race bias: Evidence for independent constructs and unique effects on behavior. *Journal of Personality and Social Psychology*, 652–661.
- Arkin, W. M. (21, May 17). Exclusive: Inside the Military's Secret Undercover Army. *Newsweek*. Retrieved from <https://www.newsweek.com/exclusive-inside-militarys-secret-undercover-army-1591881>
- Berinsky, A. J., & Huber, G. A. (2012). Evaluating Online Labor Markets for Experimental Research: Amazon.com's Mechanical Turk. *Political Analysis*, 351–368.
- Berinsky, A. J., Margolis, M. F., & Sances, M. W. (2016). Can We Turn Shirkers into Workers? *Journal of Experimental Social Psychology*, 20–28.
- Berinsky, A., & Lavine, H. (2011). Self-Monitoring and Political Attitudes. In J. H. Aldrich, & K. M. McGraw (Eds.), *Improving Public Opinion Surveys* (pp. 27–45). Princeton: Princeton University Press.
- Beyerlein, K., & Chaves, M. (2020). The Political Mobilization of America's Congregations. *Journal for the Scientific Study of Religion*, 59(4), 663–674. Retrieved from https://csrs.nd.edu/assets/403171/political_mobilization_of_congregations_for_posting.pdf
- Billig, M., & Tajfel, H. (1973). Social categorization and similarity in intergroup behaviour. *European Journal of Social Psychology*, 27–52.
- Bort, R. (2016, October 31). *John Oliver Explains the Dangers of School Segregation, Which Is on the Rise*. Retrieved April 4, 2023, from Newsweek: <https://www.newsweek.com/john-oliver-last-week-tonight-school-segregation-515289>
- Chong, D. (1993). How People Think, Reason, and Feel about Rights and Liberties. *American Journal of Political Science*, 867–899.
- Chong, D. (2006). Free Speech and Multiculturalism In and Out of the Academy. *Political Psychology*, 27(1), 29–54.
- Chong, D., & Druckman, J. N. (2007). Framing Theory. *Annual Review of Political Science*, 103–126.
- Chushing, T. (2016, February 10). *Intelligence Director James Clapper Warmly Welcomes The Internet Of Things To The NSA's Haystacks*. Retrieved June 15, 2021, from <https://www.techdirt.com/articles/20160209/11432533562/intelligence-director-james-clapper-warmly-welcomes-internet-things-to-nsas-haystacks.shtml>
- Connors, E. C., Krupnikov, Y., & Ryan, J. B. (2019). How Transparency Affects Survey Responses. *Public Opinion Quarterly*, 83, 185–209.
- Coppock, A., & McClellan, O. A. (2019). Validating the demographic, political, psychological, and experimental results obtained from a new source of online survey respondents. *Research & Politics*, 6(1), 1–14. doi:10.1177/2053168018822174
- Crockford, K. (2012, December 04). *Is the Obama administration's drone war legal? Why should we be concerned?* Retrieved April 14, 2022, from American Civil Liberties Union: <https://www.aclu.org/blog/national-security/targeted-killing/obama-administrations-drone-war-legal-why-should-we-be>
- Davis, D. W., & Silver, B. D. (2004). Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America. *American Journal of Political Science*, 28–46.

- Davis, N., & Miller, S. V. (2022). Not my neighbor: Social prejudice and support for democracy. *PsyArXiv*, 17.
- Dhir, A., Torsheim, T., Pallesen, S., & Andreassen, C. S. (2017). Do Online Privacy Concerns Predict Selfie Behavior among Adolescents, Young Adults and Adults? *Frontiers in Psychology*(8), 815. doi:10.3389/fpsyg.2017.00815
- Dinev, T., Belotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006, October-December). Internet users' privacy concerns and beliefs about government surveillance: An Exploratory Study of Differences Between Italy and the United States. *Journal of Global Information Management*, 14(4), 57-93.
- Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance – An empirical investigation. *Journal of Strategic Information Systems*(17), 214-233. doi:10.1016/j.jsis.2007.09.002
- Druckman, J. N., Green, D. P., Kuklinski, J. H., & Lupia, A. (Eds.). (2011). *Cambridge handbook of experimental political science*. Cambridge: Cambridge University Press.
- Fang, L. (2022, February 1). *Major media outlets that use invasive user tracking are lobbying against regulation*. Retrieved from The Intercept: <https://theintercept.com/2022/02/01/surveillance-data-collection-ads-news-media/>
- Feldman, S., & Huddy, L. (2005). Racial Resentment and White Opposition to Race-Conscious Programs: Principles or Prejudice? *American Journal of Political Science*, 168-183.
- FitzGerald, F. (2017). *The Evangelicals: the struggle to shape America*. New York: Simon & Schuster.
- Fry, R., & Taylor, P. (2012). *The Rise of Residential Segregation by Income*. Washington, D.C.: Pew Research Center. Retrieved from <https://www.pewresearch.org/social-trends/2012/08/01/the-rise-of-residential-segregation-by-income/>
- Garcia, B. E., & Geva, N. (2016). Security Versus Liberty in the Context. *Terrorism and Political Violence*, 48, 30-48. doi:10.1080/09546553.2013.878704
- Goffman, E. (1967). *Interaction Ritual: Essays on Face-to-Face Behavior*. Chicago: Aldine Publishing Company.
- Hampson, F. O., & Jardine, E. (2016). *Look who's watching: surveillance, treachery, and trust online*. Waterloo: Centre for International Governance Innovation.
- Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. (2014). Overcoming Online Information Privacy Concerns An Information Processing Theory Approach. *Journal of Management Information Systems*, 24(2), 13-42. doi:10.2753/MIS0742-122240202
- Harell, A. (2010). The Limits of Tolerance in Diverse Societies: Hate Speech and Political Tolerance Norms Among Youth. *Canadian Journal of Political Science*, 43(2), 407-432. doi:10.1017/S0008423910000107
- Harwell, D. (2021, February 26). ICE investigators used a private utility database covering millions to pursue immigration violations. *The Washington Post*. Retrieved March 30, 2023, from <https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data/>
- Haskins, C. (2022, February 02). *A popular workshop for police encouraged cops to use face scans to ID people they pull over at traffic stops*. Retrieved from Business Insider: <https://www.businessinsider.com/police-workshop-street-cop-training-podcast-facial-recognition-traffic-stops-2022-2?r=US&IR=T>
- Hox, J. J., Kreft, I. G., & Hermkens, P. L. (1991). The Analysis of Factorial Surveys. *Sociological Methods & Research*, 19(4), 493-510.
- Huddy, L. (2013). From group identity to political cohesion and commitment. In L. Huddy (Ed.), *The Oxford Handbook of political psychology*. Oxford: Oxford University Press.
- Huddy, L. (2017). Identity Politics. In F. M. Moghaddam (Ed.), *The SAGE Encyclopedia of Political Behavior* (pp. 373-375). Thousand Oaks: SAGE.

- Huddy, L., Davies, C., & Sandor, J. (2020). Measuring the direction and strength of partisan. In G. H. Ekengren Oscarsson, & S. Holmberg (Eds.), *Research Handbook on Political Partisanship* (pp. 103-122). Northampton: Edward Elgar Publishing.
- Huddy, L., Feldman, S., Taber, C., & Lahav, G. (2005). Threat, Anxiety, and Support of Antiterrorism Policies. *American journal of Political Science*, 49(3), 593-608.
- Hutchings, V. L., & Valentino, N. A. (2004). The Centrality of Race in American Politics. *Annual Review of Political Science*, 7, 383-408. Retrieved from <https://www.annualreviews.org/doi/pdf/10.1146/annurev.polisci.7.012003.104859>
- Jackson, C. (2021, August 17). What Is Redlining? *The New York Times*, pp. Section RE, Page 9. Retrieved April 08, 2023, from <https://www.nytimes.com/2021/08/17/realestate/what-is-redlining.html>
- Jaffer, J. (2016). *The Drone Memos: targeted killing, secrecy, and the law*. New York: The New Press.
- Jardina, A., & Piston, S. (2019, May). Racial Prejudice, Racial Identity, and Attitudes in Political Decision Making. *Oxford Research Encyclopedia of Politics*. doi:10.1093/acrefore/9780190228637.013.966
- Kerr, I., & Barrigar, J. (2012). Privacy, Identity and Anonymity. In K. Ball, K. Haggerty, & D. Lyon (Eds.), *Routledge Handbook of Surveillance Studies* (pp. 386-394). Abingdon, Oxon: Routledge.
- Kerr, I., Barrigar, J., Burkell, J., & Black, K. (2009). Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent. In I. Kerr, V. M. Steeves, & C. Lucock (Eds.), *Lessons from the identity trail: Anonymity, privacy and identity in a networked society*. Oxford University Press.
- Kim, M. (2021). Facebook News Sharing, Hostile Perceptions of News Content, and Political Participation. *Social Media + Society*, 1-10. doi:10.1177/20563051211044239
- Marcetic, B. (2022, May 16). ICE Is Tracking Your Every Move. *Jacobin Magazine*. Retrieved from Jacobin Magazine: <https://jacobin.com/2022/05/ice-surveillance-data-dmvs-immigration-citizens-palantir>
- Marx, G. T. (2006). Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information—"Hey Buddy Can You Spare a DNA?". In T. Monahan (Ed.), *Surveillance and security: technological politics and power in everyday life*. New York City: Routledge.
- Nelson, T. E., Clawson, R. A., & Oxley, Z. M. (1997). Media Framing of a Civil Liberties Conflict and Its Effect on Tolerance. *American Political Science Review*, 91(3), 567-583. doi:10.2307/2952075
- P.D.Mehta. (2001). Control Variable in Research. In *International Encyclopedia of the Social & Behavioral Sciences* (pp. 2727-2730). doi:10.1016/B0-08-043076-7/00734-8
- Pilkington, E. (2022, May 20). FBI failing to address white supremacist violence, warns former special agent. *The Guardian*. Retrieved April 3, 2023, from <https://www.theguardian.com/us-news/2022/may/20/fbi-white-supremacist-violence-michael-german>
- Radden Keefe, P. (2005). *Chatter: dispatches from the secret world of global eavesdropping*. New York: Random House.
- Rana, A. (2010). *The Two Faces of American Freedom*. Cambridge: Harvard University Press.
- Simon, B., & Klandermans, B. (2001, April). Politicized Collective Identity. *American Psychologist*, 56(4), 319-331. doi:10.1037//0003-066X.56.4.319
- Sloan, R. H., & Warner, R. (2017). Relational Privacy: Surveillance, Common Knowledge and Coordination. *University of St. Thomas Journal of Law and Public Policy*, 11(1), 1-25.
- Snyder, M. (1987). *Public Appearances, Private Realities: The Psychology of Self-Monitoring*. New York: Freeman.
- Sullivan, J. L., Marcus, G. E., Feldman, S., & Piereson, J. E. (1981). The Sources of Political Tolerance: A Multivariate Analysis. *The American Political Science Review*, 75(1), 92-106.

- Svirsky, D. (2019, January). Why are privacy preferences inconsistent? information avoidance. *John M. Olin Center for Law, Economics, and Business Discussion Paper No. 81*, 36. Cambridge: Harvard Law School.
- Tajfel, H., & Turner, J. C. (1986). The Social Identity Theory Intergroup Behavior. In W. S., & W. Austin (Eds.), *Psychology of Intergroup Relations* (pp. 7-24). Chicago.
- Terkildsen, N. (1993). When White Voters Evaluate Black Candidates: The Processing Implications of Candidate Skin Color, Prejudice, and Self-Monitoring. *American Journal of Political Science*, 1032-1053.
- Tobias, J. (2019, March 6). Exclusive: ICE Has Kept Tabs on 'Anti-Trump' Protesters in New York City. *The Nation*. Retrieved October 21, 2022, from <https://www.thenation.com/article/archive/ice-immigration-protest-spreadsheet-tracking/>
- Turow, J., Hennessy, M., Draper, N., Akanbi, O., & Virgilio, D. (2018). *Divided We Feel: Partisan Politics Drive Americans' Emotions Regarding Surveillance of Low-Income Populations*. University of Pennsylvania. Annenberg: Annenberg School for Communication. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3609974
- United Nations Special Rapporteur on Counter-Terrorism and Human Rights. (2013). *Drones Inquiry*. New York: SITU Research. Retrieved from <https://situ.nyc/research/projects/unsrct-drones-inquiry>
- Viola, L. A., & Laidler, P. (2022). *Trust and transparency in an age of surveillance*. New York: Routledge.
- Whelan, G. (2019). Trust in Surveillance: A Reply to Etzioni. *Journal of Business Ethics*, 156, 15-19. doi:10.1007/s10551-018-3779-4
- Wilcox, C., Jelen, T. G., & Leefe, D. C. (1993). Religious Group Identifications: Toward a Cognitive Theory of Religious Mobilization. In D. C. Legee, & L. A. Kellstedt, *Rediscovering the Religious Factor in American Politics* (pp. 72-99). Armonk: Sharpe.
- Wilder, D. A. (1978). Perceiving persons as a group: Effect on attributions of causality and beliefs. *Social Psychology*, 12-23.
- Williams, D. K. (2011). The GOP's Abortion Strategy: Why Pro-choice Republicans became Pro-life in the 1970s. *The Journal of Policy History*, 513-539. doi:10.1017/S0898030611000285
- Wodinsky, S. (2022, February 17). *Wordle Is Watching You*. Retrieved from Gizmodo: <https://gizmodo.com/wordle-ad-trackers-privacy-new-york-times-1848554549>
- Yousef, O. (2022, May 17). The 'great replacement' conspiracy theory isn't fringe anymore, it's mainstream. *NPR*. Retrieved from <https://www.npr.org/2022/05/17/1099233034/the-great-replacement-conspiracy-theory-isnt-fringe-anymore-its-mainstream>
- Ziller, C., & Helbling, M. (2020). Public Support for State Surveillance. *European Journal of Political Research*.

Appendix

First vignette 2x3:

Manipulation type	Text viewed by all	Text viewed or not depending on randomized assignment
In politics, there are often winners and losers. Imagine your representative in Congress is casting a tie-breaking vote for the following policy:		

<i>Policy manipulation (between respondent randomized):</i>	The government will access anyone’s location data from online services.		The government requires online services monitor and report users who violate any law to enforcement agencies.	
<i>Group manipulation:</i>	This policy affects [most liked group]	This policy affects [most disliked group]	Nothing if control	
How would you like them to vote? Definitely should not support the policy, Probably should not support the policy, Don’t care, Probably should support the policy, Definitely should support the policy.				

Second vignette:

Manipulation type	Text viewed by all	Text viewed <i>or not</i> depending on randomized assignment
A report submitted to the committee identifies that this law		
Policy (repeated from vignette 1 assignment):	on government's access to location data from online services	requiring companies to monitor and report online violations of the law to enforcement agencies
would also affect		
Group: Opposite of vignette 1 treatment randomized if vignette 1 = control	most disliked group	most liked group
How would you like your representative in Congress to cast their tie-breaking vote? Definitely should not support the policy, Probably should not support the policy, Don't care, Probably should support the policy, Definitely should support the policy.		

1st vignette	1st vignette recode	2nd vignette	2nd vignette recode	Change score	Percent full sample	Percent treated subset
Definitely should not support the policy	0	Definitely should support the policy	4	4	1.88	2.23
Probably should not support the policy	1	Definitely should support the policy	4	3	1.47	1.83
Definitely should not support the policy	0	Probably should support the policy	3	3	2.55	2.64
Probably should not support the policy	1	Probably should support the policy	3	2	3.88	3.55
Definitely should not support the policy	0	Don't care	2	2	2.01	2.23
Don't care	2	Definitely should support the policy	4	2	1.21	1.42
Probably should not support the policy	1	Don't care	2	1	2.14	2.03
Don't care	2	Probably should support the policy	3	1	3.08	3.14
Probably should support the policy	3	Definitely should support the policy	4	1	4.55	4.36
Definitely should not support the policy	0	Probably should not support the policy	1	1	2.88	3.04
Don't care	2	Don't care	2	0	10.98	10.14
Definitely should support the policy	4	Definitely should support the policy	4	0	9.44	10.65
Probably should support the policy	3	Probably should support the policy	3	0	16.21	14.71
Definitely should not support the policy	0	Definitely should not support the policy	0	0	10.18	9.94
Probably should not support the policy	1	Probably should not support the policy	1	0	8.04	7.00
Definitely should support the policy	4	Probably should support the policy	3	-1	3.55	4.06
Don't care	2	Probably should not support the policy	1	-1	1.81	1.72
Probably should support the policy	3	Don't care	2	-1	2.34	2.54
Probably should not support the policy	1	Definitely should not support the policy	0	-1	2.81	2.33
Probably should support the policy	3	Probably should not support the policy	1	-2	2.68	3.14
Definitely should support the policy	4	Don't care	2	-2	1.34	1.32
Don't care	2	Definitely should not support the policy	0	-2	0.67	0.81
Probably should support the policy	3	Definitely should not support the policy	0	-3	1.00	1.01
Definitely should support the policy	4	Probably should not support the policy	1	-3	1.54	1.72
Definitely should support the policy	4	Definitely should not support the policy	0	-4	1.67	2.33

Table 10 Change score combinations, coding, and frequencies

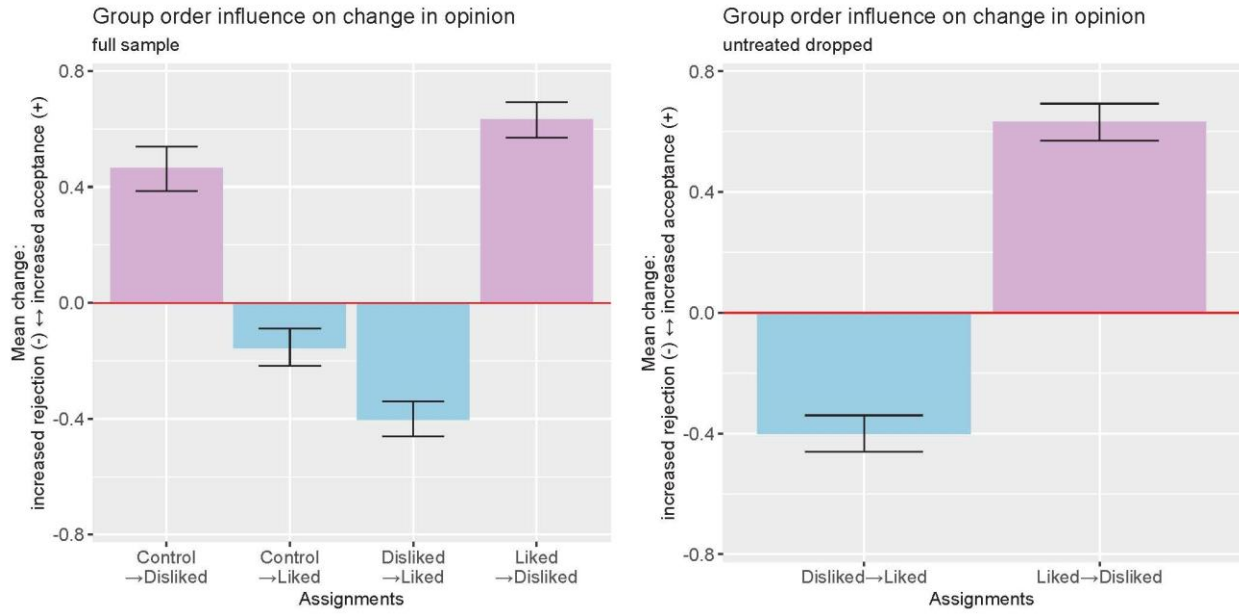


Figure 16 Full sample and treated sample average change in opinion

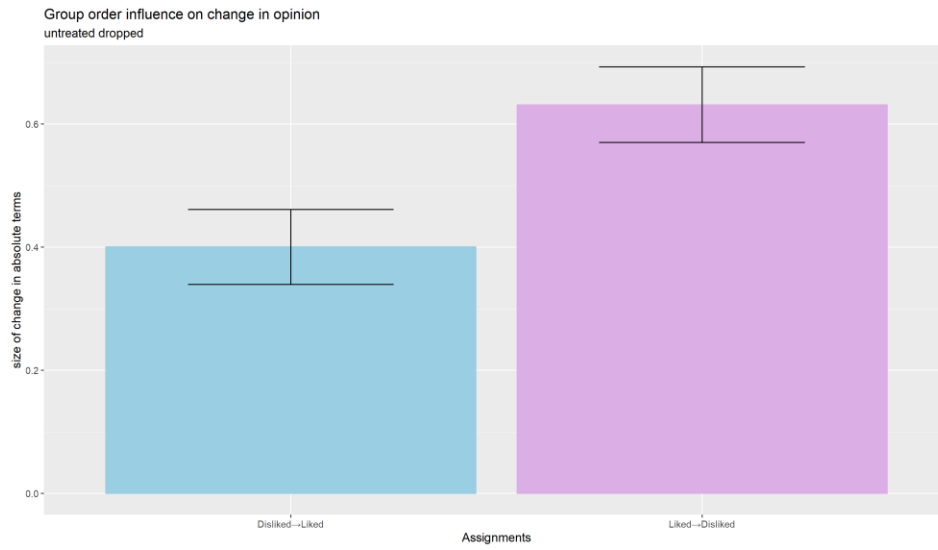


Figure 17 Size of opinion change (absolute values)

vignette:	Statistical models			
	1st	2nd, all	2nd, only Treated	change score (-4 to 4)
(Intercept)	1.62*** (0.07)	1.65*** (0.06)	1.68*** (0.07)	-0.39*** (0.07)
Liked (ref Control)	-0.14 (0.08)			
Disliked	0.40*** (ref control) (0.08)	0.51*** (ref Liked) (0.07)	0.50*** (ref Liked) (0.08)	
Policy: Report (ref (Geolocate)	0.69*** (0.07)	0.54*** (0.07)	0.55*** (0.08)	-0.01 (0.09)
Liked then disliked (ref Disliked then liked)				1.03*** (0.09)
R ²	0.09	0.07	0.07	0.13
Adj. R ²	0.09	0.07	0.07	0.12
Num. obs.	1493	1492	985	985

*** p < 0.001; ** p < 0.01; * p < 0.05

Table 11 Full sample vignette 2 OLS results

	Models		
	1 st vignette	2 nd vignette 0 to 4 scale	change score -4 to 4 scale
(Intercept)	0.31** (0.12)	0.37** (0.14)	-0.31 (0.16)
Group: Liked (ref Control)	-0.18* (0.08)		
Group: Disliked (ref Control)	0.39*** (0.07)		
Group: Disliked (ref Liked)		0.47*** (0.07)	
Sequence: Liked then Disliked (ref Disliked then Liked)			1.04*** (0.09)
Report (ref Geolocate)	0.65*** (0.06)	0.51*** (0.07)	-0.02 (0.09)
Self-monitoring	0.19* (0.09)	0.37** (0.11)	0.09 (0.13)
Mean deputized surveillance acceptance	0.65***	0.70***	0.08

	Models		
	1 st vignette	2 nd vignette	change score
	0 to 4 scale		-4 to 4 scale
Mean worries	(0.04) 0.03	(0.05) -0.03	(0.06) -0.09
Mean institutional trust	(0.04) 0.21***	(0.05) 0.14*	(0.06) -0.11
Mean privacy knowledge	(0.05) -0.45***	(0.06) -0.31*	(0.07) 0.10
R ²	(0.12) 0.28	(0.14) 0.29	(0.16) 0.13
Adj. R ²	0.28	0.28	0.12
Num. obs.	1491	985	985

*** p < 0.001; ** p < 0.01; * p < 0.05

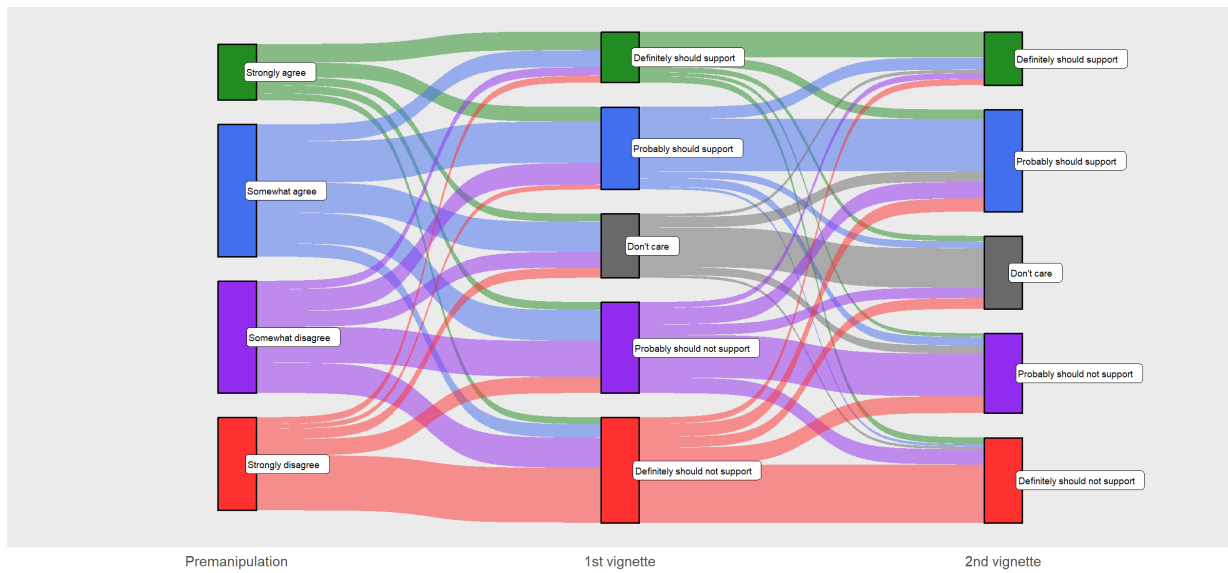
Table 12 Pre-treatment variable models, robustness check

Steadfast respondents

Do previous choices on the relevant policy bound the vignette responses? A Sankey visualization of the frequency of response paths taken provides one way of understanding response instability and steadfastness¹⁸⁷. The Sankey identifies which policy (geolocation or reporting) a respondent was randomized into in the experiment and the response to that particular policy in the four-item pre-treatment deputized battery.

¹⁸⁷ Ten respondents did not answer a battery's policy question but were later randomized into seeing it in the vignette. Because I lack their initial response, I take the average from the remaining three questions and label whether they rejected or accepted the remaining battery items.

Change in opinion
Geolocation policy & vignettes



Change in opinion
Reporting policy & vignettes

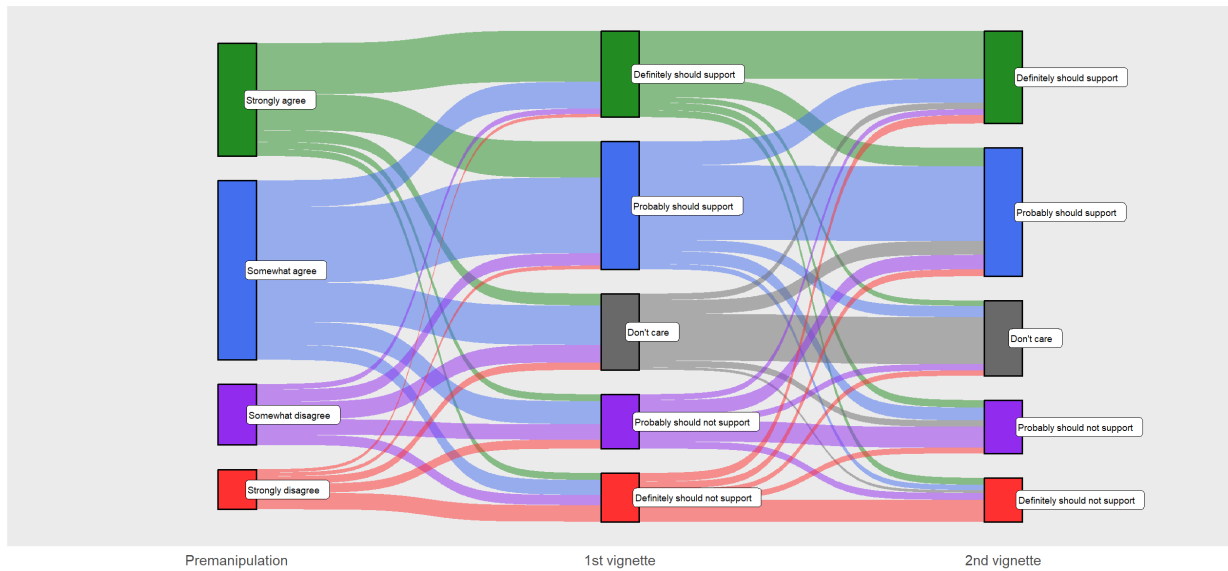


Figure 18 Change in opinions from deputized battery to vignette experiments

Figure 18 indicates the most notable proportion of steadfast respondents—those assigned to treatment but refused to change opinions are dominated by those who respond “probably should support”. Out of these, the majority shared an also-lukewarm agreement (“somewhat agree”) of deputized reporting requirements when they were asked about the four-item deputized surveillance

battery that included a version of the policy they would later be randomized into. The four-item battery, discussed at length in Chapter 2, had no neutral response by design to capture normative attitudes towards the deployment of the listed policies. In the experiment, which is couched as a tie-breaking vote, I included a neutral response to accommodate for the real-world absenteeism. The steadfast “don’t care” respondents mostly come from people who answered “somewhat agree” with the geolocation or reporting policy in the four-item battery.

Logit and Multinomial results on steadfast respondents

At this point in the results, the analysis follows an exploratory spirit outside pre-registration to understand who the steadfast respondents are. Using the same model parameters, I present two relevant findings from the confounder variables using a logit model where the responses ($n = 986$, only those treated with both groups) are recoded as volatile if they changed opinions between vignettes (0, $n = 469$) or steadfast (1, $n = 517$). From the steadfast respondents treated with both groups ($n = 517$), I show three findings using a multinomial logit model, where the outcome is the five substantive response choices.

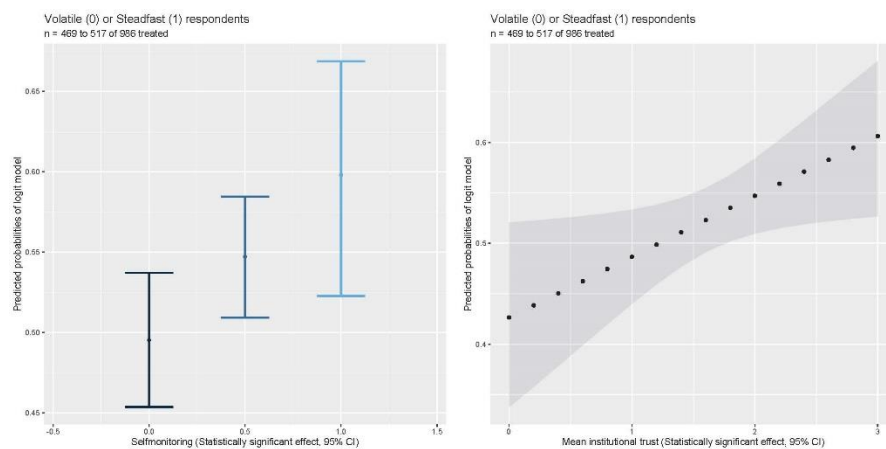


Figure 19 Selected predicted probabilities from the logit model

Because one cannot directly analyze logit and multinomial regression data, I calculate and graph the predicted probabilities for both models. All predicted probabilities are calculated with full model variables from the OLS regression. Figure 19 shows the predicted probabilities of two variables with statistically significant effects, calculated from the logit model where the outcome is responses recoded

as showing some change between vignettes (volatile = 0) and steadfast (coded as 1). The left-hand panel shows the predicted probability of an increase in self-monitoring responses (scale is 0, 0.5, and 1). Respondents who self-monitor more have a higher predicted probability of not changing their responses. That aligns with the theoretical expectation that these types of people are more self-aware and even self-censoring in their opinions and thus would be resistant to changing their response after viewing the opposite group member, independent of the group order or policy they are randomly assigned to. On the right-hand side panel, the upward-sloping line graphs the predicted probability of respondents' increased mean institutional trust. More trusting respondents are anticipated to retain their initial preference choice even when the second vignette shows the opposite group member being affected by the randomly assigned policy. One way of interpreting this is that people who trust institutions more might be more confident or more willing to minimize doubts about surveillance abuses, as others have theorized (Viola & Laidler, 2022).

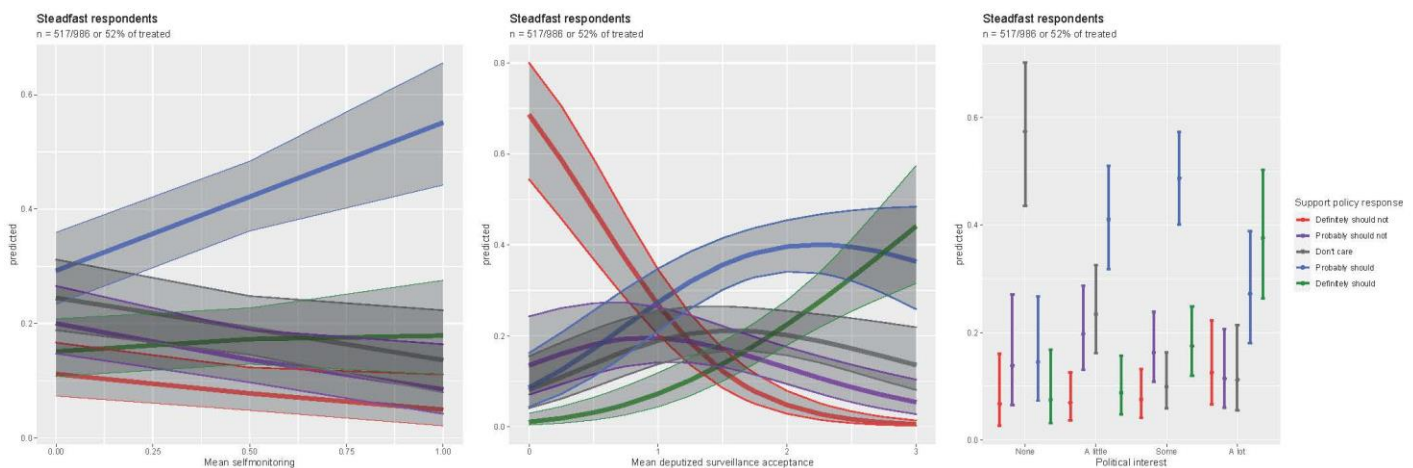


Figure 20 Selected predicted probabilities from multinomial model

Figure 20 shows three other variables of interest—including political interest, which is not in the OLS model. The predicted probabilities of the multinomial model are color-coded in the same pattern to display the steadfast choice made by the 517 respondents (who are part of those treated in vignette 1). In this subset, increasingly self-monitoring respondents (left-hand panel) had a higher probability of choosing the “probably should support the policy” response independent of the order of the groups

shown. The middle panel calculates the predicted probabilities given respondents' mean acceptance of the deputized surveillance battery. Of note are the dramatically crisscrossing slopes from the two most extreme responses: "definitely should not" responses in red and "definitely should" in green. Intuitively, the predicted probability of choosing and sticking with the maximalist rejection of a given surveillance policy, regardless of the group shown, decreases dramatically as the pre-experiment mean acceptance of the deputized surveillance increases.

In contrast, the opposite occurs for the most accepting experiment response choice. We again see the second-most accepting response choice following a similar pattern, rapidly increasing, reaching its zenith in the 2-average. The right-hand panel highlights political interest. The variable plays little to no role in any other model but is included here because it sheds light on the substantively apathetic steadfast respondents who chose "don't care" in both vignettes. The highest predicted probability for these respondents, with a substantive effect and statistically significant from 95% confidence intervals, is having no political interest. In contrast, highly politically interested people have a high predicted probability of being very accepting of the surveillance policies for both groups, independent of which policy is randomly assigned. Moderately politically interested respondents have a high probability of choosing the relatively accepting choice (probably should) in both group conditions.

Chapter 4 European attitudes towards privacy and security as a policy tradeoff

Abstract

Scholars generally assume citizens treat security as a valence issue and accept increased government monitoring as a tradeoff. However, these assumptions have not been systematically or comparatively studied, so American preference studies drive the tradeoff narrative in the context of terrorism (Garcia and Geva 2016, Huddy, et al. 2005). In the wake of increased scrutiny over commercial privacy practices, the past years' debate in Europe has shifted towards regulating the corporate handling of personal information. Using the 2014 and 2019 European Election Voter Study, this chapter pivots back to countries' regulating their own data collection. I argue that juxtaposing two valence issues (security and privacy) creates a policy preference issue. What, if anything, explains Europeans' privacy/security policy preferences? I use variables from six plausible voting behavior theories to explain voters' policy preferences (Lipset and Rokkan's frozen cleavage theory, Inglehart's value change theory, vote choice, ideological preferences over state economic interventionism, individuals' relation to their domestic government institutions, European Union transnationalism), the survey year, and sociodemographic (age, class, education), and news consumption controls. The models include country-fixed effects to account for omitted variable bias. Using a logit fixed effect model, I also model these relationships by focusing on the substantive differences between those who make a tradeoff and those who do not.

Introduction

The 2013 revelations of Edward Snowden did not just affect American politics. They revealed that the United States government was engaging in mass surveillance of European citizens, that European governments were cooperating in surveilling other European governments,¹⁸⁸ and that European telecommunications companies and online services did not secure their data as the 1995 directive mandated. Unlike in the US, the European Union's experience with totalitarian and fascist regimes has shaped citizens' expectations of the limits to government regarding privacy. Nevertheless, like in the US, experiences with terrorism have incentivized governments to campaign and govern with visible domestic security policies and to increase international cooperation between the national police forces.

¹⁸⁸ The US engages in asymmetric data sharing and uses intelligence alliances to ask some countries to surveil others on their behalf. See footnote 194.

Like Americans, Europeans also face competing claims about the degree to which they should surrender privacy rights to face security crises (Lührmann and Rooney 2020). At the same time, data insecurity has also become more prevalent. Russian groups have targeted critical infrastructure in European countries, making the idea that loss of privacy can create more insecurity visible to affected citizens.

In the US, Obama justified the NSA programs because they targeted foreigners. An underexplored perspective is how foreigners felt¹⁸⁹. Europeans are military and intelligence allies and a large consumer market of American technologies. Furthermore, because the use of intelligence is untransparent, the political rewards of cooperating with American intelligence are unknown to Europeans. It is hard to prove surveillance provides security benefits for Europe without data, but harder to imply this in the face of successful terrorist attacks—which Europe experienced. It is worth mentioning that between 2010 and 2021, War on Terror-related terrorism (defined as jihad/religious inspired) was the least frequent version. The greatest proportion was motivated by ethno-nationalist and separatist (i.e., domestic) violence, according to Europol, the EU law enforcement cooperation agency (Council of the EU and the European Council 2021).

Increased threats, whether real or perceived, boost individual support for pro-security measures, which may come at a cost to privacy (Garcia and Geva 2016, Huddy, et al. 2005, Ziller and Helbling 2020, Krueger, Best and Johnson 2020). Yet, little research exists on attitudes at times of low threat. The Snowden revelations made European heads of state unable to sidestep the need for a political response, especially once it came to light that the US was surveilling allied leaders, not just citizens directly or indirectly involved in terrorism.

¹⁸⁹ As a counter example to the American exclusionary reading of privacy rights, in 2022 Germany's court ruled that privacy rights extended to foreigners and that intelligence services could not rely on citizenship status to justify warrantless online surveillance, targeted or bulk (Eddy 2022).

The need for political responses seemed almost personally necessary, if not electorally. In the following subsection, I detail the European political response resulting in a new policy (supply), the 2016 General Data Protection Regulation (GDPR), which, briefly summarized placed privacy rights in the framework of data security, institutionalizing financial penalties for privacy breaches and mishandled data, avenues for citizens to request data, its deletion or launch complains, and mechanisms for national governments to investigate wrongdoing (Laurer and Seidl 2020).

But what did/do European voters want? What do Europeans decide when privacy or security are no longer valence issues but presented (by the media and politicians) as a tradeoff choice? Are other political preferences closely associated with the tradeoff preference? Did the EU's institutionalization of a policy change in privacy rights (data protection) follow an increased voter demand for privacy? Or did attitudes crystallize with the aid of policy supply?

This chapter will examine European Union voter preferences based on a continuous measure of a security-privacy tradeoff recorded in 2014 and 2019. This study aims to analyze the demand for privacy in the face of security concerns outside the United States. I use the European Election Voter Study of 2014 (Schmitt, Popa and Devinger 2015, GESIS ZA5160) and its 2019 follow-up (Popa, et al. 2019). My descriptive data analysis provides further evidence that we should scrutinize the blanket statement, "People don't care about privacy". This study is the first to compare pan-European attitudes before and after the 2016 GDPR passed. This European Union legislation institutionalized penalties for privacy breaches and data mishandling and provided institutional avenues for citizens to lodge complaints to their national government that led to investigations of private companies' practices.

Beyond a descriptive look at the changes in privacy demands, I test whether the privacy-security tradeoff preference (measured as a 0-10 interval variable) is associated with a series of voter preferences of interest to the Political Science literature. This approach tackles a gap in surveillance

studies literature, public opinion and voter choice literatures. The basic question: when it comes to privacy, what do voters want? is hardly ever asked. In part, this is because, as I discussed in Chapter 1, collective privacy rights and the threat posed by mass surveillance is usually not up for democratic debate, either in spaces where oppositional discourse is institutionalized (e.g., legislative bodies), or on the campaign trail and ballot (e.g., left to voters to decide). Companies also prefer not to disclose to consumers (or competitors) the ways in which they use, buy, or sell data, for their own profit or as deputized actors.

The question is also not usually conceived in terms of voters because people are not usually given a political choice in mass online surveillance, intelligence, or regulation of corporate data security practices. Two other reasons incentivize this blind spot. One is the common belief that most people don't care about privacy, which unfortunately begets a circular lack of scrutiny. Even if this were true, what proportion is "most people"? Second is the idea, fostered by political campaign messaging, is that security is a valence issue—privacy is assumed by as policy makers to give way to support for security measures. Often, that assumption is used to justify the use of surveillance. But, if privacy is also a valence issue, what policy preferences do voters hold when the two are explicitly counterposed? A third, slightly cynical reason is that campaigns use voter surveillance to mobilize favorable voters and demobilize antagonistic voters in ways that "result is an unfair system that undermines voter autonomy" (Burkell and Regan 2019), producing what I and others identify as a regulatory conflict of interest (Lavigne 2022).

Fortunately, the European Election Voter Studies asked Europeans to place themselves in an interval scale where on one end they expressed full support for privacy rights even when they hindered the ability to combat crime or, vice versa, fully restricting privacy rights to combat crime. The debate about whether voters would have a policy preference prioritizing one side or the other was of interest because, unlike American institutions' scramble to justify the NSA programs and deputized

surveillance, European politicians—particularly at the European Union level—reignited the debate about mass surveillance’s political economy. For European politicians and observers of EU integration, it became politically relevant to know what preferences people voting in the 2014 and 2019 European Union Parliament elections held when privacy was explicitly juxtaposed to security.

This chapter treats the preferences along the privacy-security tradeoff continuum as the outcome of interest, driven by the dissertation’s overall focus on understanding privacy concerns and policy preferences. Therefore, I treat vote choice, along with a range of other preferences on policy, ideology, values, social standing and demographic placement as variables of interest or controls.

I preview the main findings now. Variables reflecting postmaterial values are strongly associated to privacy preferences. This suggests an intertwining in voters’ minds that privacy is a quality of life issue. Ideological, partisan, and social cleavage factors are moderately associated with respondent preferences. Even though the EU passed GDPR, attitudes toward national governments are more associated with responses than attitudes toward the EU, reflecting the national character of security, surveillance, and privacy enforcement. Gender and age controls are moderately associated with tradeoff responses, but overall sociodemographic variables have the weakest explanatory power. Notably, 2019 responses were statistically significantly more likely to be pro-privacy than 2014, a year after the Snowden revelations.

The sizeable sample ($n = 52,885$) allows me to test these variables related to different voter theories concurrently. Motivated by the descriptive evidence of preferences’ distribution and the modest explanatory power of the model ($<12\%$), I focus on a noticeable proportion of responses that substantively refuse to trade privacy or security. I regroup responses into a binary outcome of interest, separating the refusal to make the tradeoff category from making the tradeoff. As an exploratory analysis, I have no strong priors informing who would refuse to make the tradeoff on the substantive basis of the issue. But, there is likely some overlap with expectations from the public opinion literature

on self-censorship of political preferences (i.e., voice) (Schlozman, Verba and Brady 2012, Berinsky and Lavine 2011, Beauvais 2019).

I make a concerted effort to explore who refuses to make the tradeoff for two reasons. First, doing so resists the temptation to categorize these respondents as having no preference and omitting their choice. As I will show in the result section, treating these responses as essentially a non-preference would be problematic. This response is the most popular, vacillating between 18-20% depending on the survey. Second, given the non-negligible number of respondents who did *not* answer the question (~5%), the respondents who picked “5” distinctly and deliberately chose a response that puts on equal footing security and privacy. It is substantively important to understand these voters because they seem to be unmoved by the premise that privacy and security are zero-sum resources. This is exactly the argument that cybersecurity and encryption experts make: physical and digital privacy provides security, and security ensures privacy (Schneier 2015).

With regards to the GDPR, its passing seems associated to European’s support for strengthened privacy preferences. This trend supports the idea that institutional policies (Europe) can play a role in mobilizing privacy concerns, while a hands-off approach to privacy protections (US) may signal to voters that those concerns are not valid and should be brushed off¹⁹⁰. In 2019 Europeans were less likely to refuse to make the tradeoff than in 2014. Women were more likely to refuse to make the tradeoff compared to men, in line with gendered patterns of political opinion expression. Those who consumed less media during the campaign were more reluctant to pick a tradeoff side. Religious respondents, those who disapprove of same-sex marriage, prefer economic growth to environmental protection were more likely to refuse the tradeoff than their counterparts. Voters of the three right-wing party families (Christian Democrats, Conservatives, and Far Right) were more likely to make the tradeoff than all other non-right parties, although, when considering the interval measure,

¹⁹⁰ See Figure 25 for a comparison of American responses to the question posed to European Union member citizens.

Conservative voters were the statistically significant party choice associated to the tradeoff for security. The association between time and increasing pro-privacy preferences, and party choice and pro-security preferences indicate that attitudes can sharpen on both sides of the tradeoff.

In contrast to the previous empirical chapters studying Americans, I rely on secondary data to analyze Europeans. The question posed by the European Election Voter Study highlights the justification used to motivate surveillance and justify the loss of collective privacy: fighting crime. This chapter's findings deliver several insights. First, Europe provides a sort of counter-factual to the American context. Their policy change in data protection regulations to strengthen citizens' access to privacy, and remediation for its violation, reflected institutional reactions opposite to the American dismissal, minimization, and later reframing of surveillance as targeted and thus justified. What are the attitudes associated with this context difference in information and politics?

The use of secondary data has constraints. The question was asked identically twice, but the survey team dropped other questions in the second wave. I cannot measure deputized surveillance attitudes or test if intergroup relations influence the acceptance of surveillance similarly in Europe. But, the data provides a broad comparative view of European Union citizens' voter preferences in two moments, directly focusing on the interaction of surveillance when justified as a necessity for security. Finally, this data allows me to study how citizens' relationship to their state and its policies is associated with the shape and strength of privacy concerns and how concerns fluctuate, further justifying my perspective that Political Science has a role to play in surveillance studies.

The data suggests the European citizenry is paying attention to the issue and is increasingly concerned with privacy. In the theory section, I motivate the selection of several variables, drawing competing voter models, to test whether/how they help explain people's privacy-security tradeoff choices. I conclude with hypotheses. In the Design section, I discuss the two survey waves and how the variables were measured. In the Results section, I present the findings I have foreshadowed here,

delving deeper into the directionality of interval variables and nuances in categorical variables. I also analyze the time component through the empirical finding that Europeans had higher privacy preferences in 2019. The comparison of survey years suggests that Europeans' attitudes align with their governments' supplying policies with stricter data protection. Future research should investigate if and how parties have become competitive on privacy issues, whether citizens' exposure to data breaches or regulation efforts partly motivates opinion change, and whether the two-point trend continues or reverses.

European surveillance regulation

Disclosures from Edward Snowden (2013) and WikiLeaks (Vault7, 2017) showed that states do not ask for voters' permission when expanding their monitoring capabilities, undermining the legitimacy-through-consent relationship of democratic governments. European states are also entangled in the dynamics of the surveillance complex. Some states have declared that full disclosure of the exact procedures would negate their effectiveness since criminals would devise ways around surveillance techniques (Statewatch 2020, Access Now 2023). In embracing its anti-European Union mandate, the United Kingdom is taking Brexit as an opportunity to undo European privacy regulations and has proposed anti-encryption legislation that may lead services like Signal to leave the country (Milmo 2023).

European individuals find themselves in the same position as their American counterparts: as consumers, many have used digital services that provide access for free but serve targeted ads and monetize their data. Companies can only target ads and extract a price for targeting¹⁹¹ from advertisers if enough information on the user is available to create consumer profiles. The ad market is heavily concentrated between Google and Facebook, whose inordinate access to data and management of ad

¹⁹¹ This is the 'value added' that online companies competing for ad spending against traditional media purport to bring. That's the gist of Zuboff's argument on surveillance capitalism.

services lets them control supply and demand, increasingly fueling calls for audits and anti-trust regulation. Facebook filings to the Securities and Exchange Commission in 2018 stated that American and Canadian users were three times more valuable to advertisers (priced at USD 34.9) than European users and ten times more valuable than Asia-Pacific region users (Fisher 2019). I have conducted the same analysis on additional SEC filings from 2013 and found these regional differences in data value stable (see the end of the appendix).

Not all individuals are at ease with the idea of the government holding vast amounts of personal data and behavioral information¹⁹², even at the cost of security¹⁹³. Analysis of the voter study data shows that a year after Snowden (2014), 31% of respondents wanted some degree of privacy over the ability to fight crime, 41% preferred giving up some degree of privacy for security while 20% expressed a neutral preference and the rest did not know or refused to answer.

Those who forgo privacy for security might do so because they are unaware of the security risks in keeping corporate systems vulnerable to state surveillance, given that criminal organizations can also exploit these digital backdoors. European national governments and the European Union institutions view with skepticism the American Data Goliaths' claims that people do not care about privacy. They might not have technological alternatives. Europeans lobbying for protections questioned whether American Data Goliaths gave citizens a genuine choice over their privacy if comparable alternatives and all the information necessary to make that choice were unavailable.

After the Snowden disclosures, European legislatures, courts, and regulators mobilized a more critical stance against the claims of American technology companies that use and sell citizen data. Their skepticism motivated the most significant change in data protection regulation since the 1990s

¹⁹² The 2014 European Election Voter Study places 31% of respondents as preferring some degree of privacy over the ability to fight crime, while 41% prefer giving up privacy for security; 20% expressed a neutral preference and the rest did not know or refused to answer.

¹⁹³ Prominent security experts like Bruce Schneier make the case that digital privacy *is* security, in the same way that a lock on a door extends both to an individual (2015). For these experts, policy makers are setting up a false dichotomy, or worse, producing the illusion of security with measures that do nothing or undermine it (security theater).

and has helped raise the issue's salience for citizens. In the wake of the Snowden revelations, the political pushback against privacy protections waned. The general scrutinizing environment boosted the European Parliament's negotiations on The General Data Protection Regulation (GDPR) (Laurer and Seidl 2020). The EU Parliament passed the regulation in 2016, and enforcement started in 2018.

This European Union legislation institutionalized penalties for privacy breaches and data mishandling. It also provided institutional avenues for citizens to lodge complaints to their national government with empowered national data protection offices. Complaints lead to investigations of private companies' practices, with a maximum penalty calculated from 4% of global profits. Accompanying rulings like "the right to be forgotten" have strengthened the reality that European data is treated with different privacy and security (data integrity) guarantees than American data (Jones 2018).

On the other hand, the state's ability to track communications through commercial services and to link individuals within its borders and outside of them is now as important an asset for governments' security apparatus. Just as proliferation and denuclearization movements emerged after the Second World War and became part of competing party platforms, data retention and surveillance policies can polarize in a world of increasing technical abilities and globalized criminal/terrorist networks. American allies helped implement the post-9/11 digital surveillance apparatus internationally—specifically the European NATO members, Five Eyes, Nine Eyes, and Fourteen Eyes surveillance partners¹⁹⁴. For 17 years governing European parties across the ideological spectrum have participated in the growth of their surveillance capabilities and collaborated in the transatlantic and domestic securitization of digital communications. This might have left the majority-winning

¹⁹⁴ These are intelligence alliances: the United Kingdom is the only European member of the English-speaking Five Eyes; Denmark, France and the Netherlands joined the Nine Eyes; Belgium, Denmark, Germany, Italy, Spain and Sweden are members of the Fourteen Eyes group.

governments (mostly center-right given the collapse of the center-left) with little credibility on the topic of reigning in foreign or domestic surveillance in the eyes of voters.

Revelations of the secretive arrangements between intelligence agencies are *still* reverberating. In 2021 news emerged of a Danish Defense Intelligence Service that blew the whistle on how Americans used the Danish agency to spy on Danish social institutions, national defense contractors (competing with Americans for bids) and shared allies “France, Germany, the Netherlands, Norway, and Sweden” (Moss 2020). Thus, the news exposes citizens to a slow drip of information regarding companies, states, and malicious actors accessing their data.

Throughout Europe, niche parties like the Pirate Party¹⁹⁵ have made salient how Europeans have few policy choices and technological alternatives. This niche party, which began in Sweden in 2006 as an anti-copyright party and later expanded to digital civil rights issues, has tried increasing the issue salience of privacy¹⁹⁶ but has not increased its national or EU Parliament seats much in more than 15 years (Van der Sar 2006, BBC News 2011, News Limited 2016). Recently, they have even gone below the required vote share to get EU funding for future campaigns. Instead, Green parties have capitalized on their institutionalized position as an increasingly reputable opposition party. They have spearheaded many digital-rights proposals Pirates had advocated for, and in alliance with them, at the national and EU levels (Siewert and König 2019).

On the other hand, Conservative parties have issue-ownership on “law and order” issues in the eyes of voters. If it is juxtaposed with national security, an ideological left/right divide around digital policy might be present¹⁹⁷. However, the growth of online media monopolies has, in practice,

¹⁹⁵ These parties see themselves as the party of digital civil liberties and has made opposition to ubiquitous digital surveillance part of its policy centerpiece.

¹⁹⁶ To deal with lack of electoral gain, this study measures changes in the media’s weekly average coverage of national Pirate Parties a year before the Snowden revelations, between the Snowden revelations and the end of sampling for the 2014 sample (30 May 2014) and the end of sampling for the 2019 survey (14 June 2019).

¹⁹⁷ For example, the center-right EPP ministers in the Council voted against the Civil Liberties, Justice and Home Affairs (LIBE) committee’s report on the ePrivacy directive that was discussed in 2017, which had called out lobbyist’s

moved some moderate and right-wing parties to favor regulating online services on nationalistic terms in ways that intersect with left-wing pro-privacy proposals. European publishers have specifically lobbied governments to regulate Google and Facebook towards a compulsory licensing scheme (Scott and Clark 2015).

At the EU level, privacy and policing *governance* policies have become increasingly Europeanized, creating a tiered effect “comparable, for instance, to US federalism” (Herschinger, Jachtenfuchs and Kraft-Kasack 2011). The General Data Protection Regulation was passed in the EU Parliament with near-unanimous consent, bolstered by the support of national presses who have complained that the data collection of (American) Big Tech creates an uncompetitive ad market. However, the accompanying ePrivacy Directive has stalled under pressure from American firms and US trade representatives’ lobbying of the Council of the EU (Corporate Europe Observatory 2017, Corporate Europe Observatory 2018)¹⁹⁸. Thus, in this respect, privacy can also be a roundabout way of enforcing anti-trust and domestic economic protectionism. This angle to regulation is politically appealing to moderate and anti-globalization parties throughout the nationalist/integrationist dimension (Hooghe and Marks 2018). The monopoly of the legitimate use of physical force is “still in the hands of EU member states”, and operational jurisdiction has not been internationalized. However, the rules and “dispute over their application are settled by an independent court”, increasingly “embedding” national sovereignty decisions into a “larger institutional framework” (Herschinger, Jachtenfuchs and Kraft-Kasack 2011). In sum, this chapter is directing our attention away from the US context to look at support for privacy more comparatively. Political parties, their

“innovation” scare-mongering and recentered the directive along the lines of privacy being a “non-partisan human right” (Corporate Europe Observatory 2017, quoted officials).

¹⁹⁸ The Council of the EU is notoriously more pro-market than the EU Parliament and its deliberations more opaque. Second, the ePrivacy dossier was handled by telecoms officials from member states (via the Telecommunications Working Party) which worried specialized observers in 2017, who concluded it “could imply that positions are more likely to be pro-industry. By contrast, the GDPR was handled by data protection officials” (Corporate Europe Observatory 2017). In fact, GDPR passed and ePrivacy did not, even after much watering down, which was the preferred position of the EU advertiser and American tech groups’ preferred choice.

related cleavages, and policy stances are essential in understanding some focal party-oriented cross-national roots of privacy attitudes.

Theory

Following Liesbet Hooghe and Gary Marks, I compare theories of public opinion to explain the policy preferences trading increased privacy for security or vice versa. The authors “consider the contributions of each theory in its own terms. We neither treat these theories as mutually exclusive nor do we mould them in a composite super-theory” (2019, 1113). In the following paragraphs, I justify why these theories are plausible explanations for voters’ policy preferences. In the Data section, I discuss their operationalization.

Cleavages

Cleavage theory posits that “issues that divide voters are connected in durable dimensions” (Hooghe and Marks 2018, 109 paraphrasing Lipset and Rokkan 1967). Political parties organize around these durable dimensions, creating sticky institutions and commitments that give parties issue ownership. Lipset and Rokkan describe “[a] national revolution that produced a cleavage between the central state and peripheral communities and between the central state and a supranational church; and the industrial revolution that produced an urban/rural cleavage, and later a worker/employer cleavage” (ibid).

The de-industrialization of Europe towards a service and knowledge economy might lead to some reconfiguration of political parties similar to the industrial revolution and the birth of communist, socialist, and social democratic parties. WikiLeaks’ and Edward Snowden’s NSA revelations of the scope of this surveillance may also serve as exogenous shocks that confront the voter with the cost of collective security as a tradeoff for individual privacy. However, it is too early to know if de-alignment is occurring (Dalton and Wattenberg 2000), or whether emerging cleavages are substituting old ones (Marks, et al. 2017). Older, established (mainstream) parties usually have

difficulty adapting and expanding their agenda, opening the way for challenger parties (Meguid 2008, Hagemann, Hobolt and Wratil 2016). I turn to this issue in detail when I discuss party vote choice.

Postmaterialism

Ronald Inglehart posits that a combination of objective external conditions regarding scarcity and subjective interpretations of these conditions at an early age will lead individuals within generational cohorts to have political preferences that reflect a predilection for either economic and physical security (materialist values) or self-expression and autonomy (postmaterialist values) (Inglehart 2007, 223). Postmaterialism emphasizes quality of life, while materialism is concerned with securing life (survival) regardless of its quality. Those who hold postmaterialist values will likely downplay concerns for physical security, anxiety towards crime, and economic security, like inflation. Instead, they are concerned with policies that further: “freedom of speech, giving people more say in important government decisions, more say on the job, and a society where ideas count” (idem, 225). Respondents with consistent postmaterial belief systems will prioritize quality-of-life issues like privacy over physical security.

The postmaterialist theory might explain privacy preferences as part of emerging issues tied to individuals’ ability to and need for self-expression as part of a coherent system of beliefs. Attitudes towards immigration, environmental protection, and sexual identity reflect postmaterialist values since they emphasize quality of life and freedom to express oneself (Inglehart 2007, 225).

In several studies on EU countries, Dalton finds a cohesive cultural belief system around support for gay rights, immigration, and gender equality in Western Europe using principal component analysis (R. Dalton 2020, 7), while Welzel and Inglehart find a strong positive correlation (0.77) between acceptance of homosexuality and postmaterialism (Welzel and Inglehart 2005). Privacy is a value that itself facilitates freedom of expression while surveillance undermines people’s autonomy. Materialists, defined by their concerns about security, are more likely to favor policies that affirm the

status quo and are perceived to build security: demographic status quo, economic stability, and traditional marriage.

Party vote choice and ideology

Individuals' policy preferences are also shaped by a political world organized with sticky institutions. Established parties have longstanding positions on domestic economic and social issues and their country's role in international security. Some parties are so closely associated with a policy stance voters consider them to have 'issue ownership' (Budge and Farlie 1983, Petrocik 1989). Identifying a party's position on an issue or its perceived issue-ownership of a party is an informational shortcut for voters (Lupia 1994, Popkin 1991). I hypothesize that voters who support conservative parties will also support security policies because these parties are more likely to be associated with "law and order" policies than liberal and left-wing parties. Centrist voters, especially center-left voters, likely lack such preferential clarity. This is because mainstream center-left parties try to compete with center-right parties to avoid being labeled as "soft on crime". In the late 1990s, Third Way/ "new labor" parties tried to compete on law and order against conservative parties by taking a harder-line stance on immigration and security (Kriesi, et al. 2008). For example, German Chancellor Schröder and British Prime Minister Blair co-authored *Europe – The Third Way/Die Neue Mitte* in mid-1999, advocating for reforming the welfare state and tying it to domestic security to make themselves competitive with moderate-right voters. Other European center-left governments followed suit (Tham 2001). European parties were further incentivized to run on security when 9-11 bolstered NATO collaboration. Europe's own terrorism events brought the issue home to voters. Moderate left-wing parties have distanced themselves from their international pacifist traditions and domestic critiques of police states (Kriesi, et al. 2008). Thus, center-left parties might have convinced voters that they can be competitive in the security policy space. If so, we should observe a "fuzzy middle" in the partisan breakdown of preferences.

Beyond party vote choice, people's ideological preferences can be expressed by policy preferences. One significant component of ideological preferences reflects people's preferences toward the size of the state. Anthony Downs' spatial model, championed by those who prize parsimony, is used to place individuals in a unidimensional space of left-right politics, focused initially on economic welfare ("how much government intervention in the economy should there be" (1957, 116)). However, the scale has become colloquial shorthand for a broader sorting of political ideology, expanding its use along with its ambiguity (e.g., "In political matters people talk of "the left" and "the right". What is your position? Please use a scale from 0 to 10, where '0' means "left" and '10' means "right".) skepticism about respondents' equivocal understanding of the "left" and "right" and the measurement errors of inferring meaning have plagued the field. Although authors have found the majority of less-knowledgeable respondents held consistent and 'correct' ideas about the "left" and "right" concepts (Lambert, et al. 1986), there is debate about whether a second left-right dimension on social liberalism and conservatism are orthogonal or even reversed from economic liberalism and conservatism (Marks, Attewell, et al. 2021). Thus, economic interventionism is measured separately to account for people's preferences on the size of the state's economic interventionism and preferences on exercising that economic interventionism.

Institutions: trust, approval, political interest

Surveillance scholars have theorized that acceptance of surveillance is associated with higher institutional trust, whether from the government (Viola and Laidler 2022, Radden Keefe 2005) or corporations (Hampson and Jardine 2016). Friedewald et al. found respondents can distinguish between privacy-intrusive practices countering "legitimate interest[s] of EU citizens", such as protests and "actions meant to safeguard the majority of EU citizens" (2016, 28) and that trust in institutions is an essential correlate to acceptance of surveillance. However, Friedewald et al.'s vignettes do not invoke security or privacy explicitly; they test indirect privacy and security preferences independently.

In a study comparing the third and fourth waves of the Values Surveys (1995–2001), Catterberg and Moreno find that Europeans’ trust in parliamentary and civil service institutions is generally associated positively with assessments of government performance, political interest, and external efficacy (the perception that people have a say in government) (2006). Because Parliament is an institution where party affiliation is explicit (unlike civil service institutions, where non-partisanship is expected, especially outside the US), “the relationship between partisanship and trust is dependent on partisan control” and “its influence on trust occurs indirectly through approval of governmental institution” (Gershtenson, Ladewig and Plan 2006).

Emerging cleavages: the European Union and Transnationalism

Hooghe and Marks have produced evidence of an emerging cleavage (“transnational”) organized as a reaction to the “reforms that have weakened national sovereignty, promoted international economic exchange, increased immigration and exacerbated cultural and economic insecurity” derived from globalization and in Europe’s case, the integration process (Hooghe and Marks 2018, 110). The transnational cleavage updates Lipset and Rokkan’s regional center-periphery cleavage. It reflects a tension between “the defense of national political, social and economical ways of life against external actors” (ibid).

Capturing preferences on the emerging transnational cleavage, like the desire for further integration, openness to immigration and trust in the EU Parliament, is relevant to the privacy-security tradeoff on both sides of the question (Marks, Attewell, et al. 2021, 177). Privacy and policing regulations have increasingly become “federalized” (Herschinger, Jachtenfuchs and Kraft-Kasack 2011), meaning that the European Union is increasingly constraining domestic decisions by setting minimum standards, prohibitions, and requirements for domestic regulation. One example that shows how far this consolidation has come, collapsing privacy and security, is the European Union’s recent vote to ban the use of facial recognition in law enforcement (Peets, et al. 2021).

Controls

I control for age, education, gender, and news consumption¹⁹⁹. The digital gap literature invokes demographic variables like age and gender, which are relevant when considering digital surveillance attitudes. There are conflicting expectations about whether women are more pro-security because of their self-perceived vulnerability to physical crime compared to men's, or whether their experiences with harassment online and offline make them more pro-privacy. For the most part, women tend to be more privacy-conscious and feel less secure than men (Tufekci 2021), but this has led to some studies finding gendered "overcorrection" where women are more accepting of invasive surveillance if it promises to create security (Huddy, et al. 2005). The myth that young people do not care about privacy has been debunked (boyd 2014, Hargattai and boyd 2010), but it is unclear whether older generations are privacy-concerned²⁰⁰.

Age and cohorts are also relevant to postmaterialist theory, framed by generational value change in given cohort differences in safety (objective and perceived). I expect awareness and reluctance to trade security for privacy to be more entrenched in the generations of those who have enjoyed economic security growing up. Younger people who grew up in the new information ecology and more frequent internet users are likelier to be more aware of the policy tradeoff as the extent of digital surveillance has become more apparent during a larger portion of their internet use relative to older respondents. I expect the most well-educated to oppose surveillance as they will more likely understand themselves as part of the dragnet. I control for people's exposure to information on crime and the use of surveillance through a measure of news consumption frequency (O. H. Gandy 1995).

¹⁹⁹ The 2014 survey had a longer battery asking how people received their news but the 2019 did not so I cannot distinguish between online and TV news consumption. More respondents got their news from TV than from the internet and TV viewers were more willing to trade security for privacy. Those who read newspapers were more willing to express a concrete policy preference than those who do not. Internet news did not seem to have a substantial effect on its readers' opinions or desire to express them.

²⁰⁰ Studies on older cohort preferences are missing from the literature.

Hypotheses for preferences prioritizing privacy or security

Broadly, I expect a left-right division of the public, where privacy support is associated with left-leaning policy preferences and identities while right-leaning policy preferences and identities are associated with security. Specifically, regarding each theory, I hypothesize the following, categorized by the theories they relate to.

- 1) Cleavages: city-dwellers, upper-class and non-religious respondents lean towards privacy preferences compared to rural, middle and low class, and religious respondents.
- 2) Postmaterialism: pro-privacy preferences are associated with attitudes favoring immigration, environmental protection, and acceptance of homosexual marriage; pro-security preferences are associated with opposing migration, economic growth, and opposition to homosexual marriage.
- 3) Parties and government ideology: Left-wing voters are likelier to pick privacy preferences, and right-wing voters will prefer security. Radical/far-right voters will likely also select security since these parties claim ethnic and religious diversity and immigration are a national security threat (Rydgren 2018).
 - a. I hypothesize a “fuzzy middle” or U-shaped distribution of privacy-security preferences. Sharper security preferences will be associated to more right-wing party voting, and the inverse for more left-wing party voters’ sharper privacy preferences. Voter of center parties (on the left and right) will have less comparative clarity on their parties’ positioning because their parties, which have been in government during the War on Terror, do not highlight the erosion of privacy rights and try to compete on security without fully committing to the hardline outsider/insider or populist language that more right-wing parties introduce.

- b. I hypothesize similar effects when measuring ideology on a 0-10 scale, producing a positive correlation with the tradeoff (a placement most to the left (0) in ideology is likelier to pick the most privacy-oriented preference (0) in the tradeoff question; the most right ideology choice (10) ideology will pick the most security oriented answer (10) in the tradeoff).
 - c. Size of the state: respondents who prefer the state to intervene in economic matters and who want the state to proactively redistribute income will be associated with privacy over security preferences. This reflects a contemporary leftist view of political economy, where the state scrutinizes powerful market actors but safeguards individual's private lives. An opposing political economy preference wants the state to dedicate itself toward ensuring physical security, including policing individuals, but holding *laissez-faire* market attitudes.
- 4) Relation to political institutions: people who trust their domestic political institutions and approve of the government in power will feel more comfortable trading privacy for security. People who disapprove of the government or mistrust domestic political institutions will prefer not to increase the government's surveillance powers. It may be because the latter do not believe their government is capable of acting responsibly or effectively, although I cannot directly test this causal mechanism. Following Catterberg and Moreno, higher political interest should be positively associated with trust and approval (2006), so I hypothesize that increased political interest positively correlates to an increased tradeoff score in favor of more security.
- 5) Transnationalism: privacy regulation is increasingly homogenized, driven explicitly by European Union institutions and its policies. Thus, I hypothesize a negative correlation: individuals supportive of integration and higher trust in the EU Parliament will be more likely to pick privacy over security (lower tradeoff scores), because they are following the data and

privacy protecting position of the EU. Those who do not support EU integration and distrust its Parliament will reject increased privacy for more security because this domain is still mostly (and in voters' mind) in the hands of domestic institutions and because it is juxtaposed to the privacy-maximizing position of the EU.

Refusal to tradeoff versus trading one for the other as a secondary outcome

The debate about non-attitudes has claimed that respondent ambivalence is due to unreliable or haphazard decision-making during survey taking (Converse 1964). A reevaluation of the issue has centered around distinguishing conceptually or operationally ambivalent individuals who may hold both positive and negative attitudes (and, further, highly uncertain when holding *many* considerations on both sides of an issue) from those who are indifferent (none on either side). Pushing back on Converse's views on "vacillation", for Zaller, "individuals possess multiple and often conflicting opinions toward important issues" (1992). Meffert et al. critique Zaller and Feldman's survey response theory for the "conventional ways" of measuring them as "a tradeoff between the polar opposite ends of evaluative scales". They juxtapose it to "qualitatively different reactions" where a person simultaneously holds some positive and negative evaluations of an object, drawing from Cacioppo et al.'s bidimensional evaluative space, where negativity and positivity towards an object are orthogonal (1997). However, Meffert et al.'s critique on the bipolar, unidimensional representation is aimed at "attitudinal ambivalence," i.e., "positive and negative ideas towards a single attitude object" (2018, 66) like abortion, or a presidential candidate, measured independently of whomever else they are running against. They do not discuss tradeoff issues with variation (exemplified by "value conflict" issues like how affirmative action may put egalitarianism and individualism in conflict), which are also different from binary or dependent tradeoff issues (e.g., candidate A implies not candidate B).

These differences are at stake in Friedewald et al.'s study, where they measure single-object attitudes and then conflate the conceptual independence of privacy and security with an absence of

preferences towards a policy tradeoff. Stating they “did not include a question directly addressing whether people think about privacy and security in terms of a tradeoff”, they infer the non-existence of attitudes towards the tradeoff policy choice from the absence of a negative correlation between “general and personal security and privacy” (Friedewald, Lieshout, et al. 2014). Despite their one-sided or independent questions, their descriptive analysis finds that Europeans (40%) are concerned about security²⁰¹. A similarly noticeable proportion of Europeans worry about being personally hacked (32%). However, because the questions are asked independently and no crosstab is reported, it is unclear how many respondents hold both opinions²⁰².

Refusing the tradeoff conveys an equal desire for privacy and security²⁰³. This chapter section seeks to draw out the theoretical background justifying the study of the refusal to trade privacy for security or vice versa. I am motivated by the empirical finding that the modal category in both surveys is the 5 response where security and privacy preferences remain balanced. This section seeks to contextualize the results I will provide later. However, because the analysis is exploratory, no explicit hypotheses are related to the tradeoff theories preceding the examination. Below I detail some plausible expectations from public opinion on neutral positions, and relate it to this chapter’s research question.

Given the primal role physiological insecurity plays in the human psyche (e.g., crime) (Maslow 1954), refusing a tradeoff as a function of indifference seems highly unusual. Given the substantial focus of the question, Zaller’s theory seems more suitable. Respondents might be coming up with an

²⁰¹ This is similar to the collapsed European pro-security ranges I calculated from the Voter Survey data: 41.3% in 2014 and 37.3% in 2019.

²⁰² Additionally, they grouped irregularly spaced responses of frequency of worry (very) with relatively infrequent response choices (“most days”, “at least once a week”, “at least once a month”), and compared these to rarely held worries (“At least once in the last year”, “Not in the last year, and “Never”)

²⁰³ I justify coming to this conclusion in the results section given the distinct proportion of respondents who do not respond (~5%). Thus, I claim that we can take the 5 responses as an explicit refusal to prioritize one at the cost of the other because those who have no opinion or do not know their preference do not answer it. The result section discusses this in detail.

equal amount of positive and negative considerations for both elements of the tradeoff and are unwilling to decide how to weigh them. In a tradeoff where respondents may hold positive and negative attitudes towards privacy and security, the highly ambivalent respondent averages more than in a single object attitude measure because the premise of the question brings to the forefront pros and cons of each polar option.

First, lower levels of political interest are likely correlated with not making a tradeoff decision if the tradeoff is perceived by these voters as a (uninteresting) policy choice. For example, in the experiment of American deputized surveillance preferences, those who reported no political interest were outliers in their discrete and unmoved “don’t care” preferences during both vignette manipulations (see Chapter 3 appendix Figure 9). Relatedly, media consumption should help respondents shape their attitudes. Thus, lack of media consumption about the campaign might lead to a feeling of being unfamiliar with specific security and privacy debates (civil rights, online data protection) and an associated unwillingness to prioritize one for the other. Politically interested people will likely report consuming more news during the election, too. Conservative party identities are the least likely to refuse the tradeoff, as they have clear issue-ownership on the security side of the tradeoff, while Green parties have taken up digital civil liberties platforms from the defunct Pirate Parties. Catch-all moderate party voters should be the least able to pick between the two, thus more likely to refuse the tradeoff²⁰⁴.

Lastly, there is some discussion about the role of class and gender. Insecurity may affect lower-class respondents more, but higher-class respondents may be equally preoccupied because they have “more (wealth) to lose” from crime. Rueda and Stegmueller find that the redistribution preferences of the Western European rich are highly dependent on the macro level of inequality associated with national crime levels, not by egotropic considerations (2016). Second, gendered survey opinion

²⁰⁴ This echoes my U-shaped or fuzzy middle hypothesis for the interval scale version of the outcome.

expression could lead to a gap in refusing the tradeoff, mediated by persistent lower levels of political interest (Fraile and Gomez 2017, Beauvais 2019) or a higher willingness to express moderate opinions. Alternatively, a genuine desire for privacy and security might be driven by higher rates of violence against women, stalking, etc., leading to a gendered perspective that privacy is an element of security (Stolle and Gidengil 2010).

Data and methodology

This study pools the European Election Voter Study 2014 ($n = 30,064$) (Schmitt, Popa and Devinger 2015)) and its 2019 follow-up ($n = 26,538$) (Popa, et al. 2019), carried out as a European Union-wide survey after the European Parliament elections of each year. All 28 countries in the EU were surveyed (before the UK's official exit). Because I wanted to study privacy and security preferences as a policy preference in the framework of an election where the EU Parliament would vote on the matter (GDPR), I removed non-EU citizens from the sample, to constrain the models to European respondents who are eligible to vote. By modeling country-fixed effects, I deal with omitted variation in explaining cross-country differences caused by hard-to-measure country-specific characteristics (culture, history, quality of life, security)^{205, 206}. I account for the survey year in the model. All non-categorical variables use Gelman's recommendation to standardize numeric variables by dividing each by twice its respective standard deviation (2008), to produce estimates that can be compared to categorical variables. Given the number of categorical variables in the model, this standardization should aid the model's interpretation. The regression observation size is $n = 34,482$, after accounting for data missingness in the independent and control variables.

²⁰⁵ Implementing fixed effects for a small n (28 countries) is often done using the country as a factor, which is controlled for in the linear model. Technically, fixed effects are used for panel data, meaning that by controlling for country we are essentially creating fixed effects without relying on dummies to implement the least squares dummy variable (LSDV) model.

²⁰⁶ Economists Joshua D. Angrist and Jörn-Steffen Pischke have warned that fixed effects capture unobserved heterogeneity in a black box, "the exact nature of the unobserved variables typically remains mysterious" (2009, 243). At the urging of a committee member, I explored country-year variation at that level to supplement my findings. I present a reduced model of a larger exploratory project in the appendix.

I run regression models with two versions of the dependent variable: privacy-security tradeoff as a 0 to 10 interval scale and a binary where a no tradeoff response (5 in the scale version) = 1 and tradeoff (all other responses) = 0. This coding separates those who stated *one or the other* policy preference as different from those who expressed no particular policy preference (Lacy 2001). The objective is to assess what/whether certain kinds of people are more likely to refrain from stating a clear policy choice.

Outcome measures: Privacy-security tradeoff interval and binary refusal/tradeoff

The European Voter Study asks respondents about a well-defined and salient objective of surveillance as a policy response to crime²⁰⁷. The question asks respondents to rate the following statement from 0-10 where:

You fully support privacy rights even if they hinder efforts to combat crime (0)
You are fully in favor of restricting privacy rights in order to combat crime (10)

This measure makes explicit the criminalizing motivations of surveillance (see chapters 2 and 3). In contrast to the American studies' measurements, the question does not focus on how or who collects the data but on how security is made salient to justify mass surveillance. In the first part of the results section, I use OLS to estimate the change in preferences measured as an 11-point interval of increasing privacy (0) over security (10). This question explicitly invokes a tradeoff, meaning that as the scale increases in value, the respondent prefers combating crime *at the expense of* privacy (cf. Friedewald, Lieshout, et al. 2014).

In calculating the model, I standardize the outcome variable by dividing observations by two standard deviations (2x3.03), as Andrew Gelman advocates (2008). This procedure centers the standardized variable's mean (originally 5.17) to zero and the new standard deviation to 0.5. In the

²⁰⁷ The last question of study 1 replicates this question as a robustness check to this claim. We can also compare whether fewer respondents give neutral answers to the tradeoff compared to the baseline questions, to validate whether the intensity of privacy concerns is lower when a security tradeoff is primed compared to generic privacy concerns.

second part of the results, I collapse preferences into a categorical unordered variable that groups those who express any privacy preference (0-4) and those who prefer any security (6-10) together, compared against those who do not make a tradeoff (5). I code the refusal to tradeoff as 1 and make the tradeoff as the reference category because the former is the substantive category of interest, and the latter is the modal response (~80%).

Independent variable measures

I replicate the standardization procedure of dividing variables by their respective two standard deviations on all numeric variables (see Appendix Table 15 for summary statistics). The aim of this transformation is twofold: it puts all predictors on a common scale and makes the effect size in a regression comparable to the effects of binary categorical variables.²⁰⁸

Cleavages

The survey asked respondents if they live in a rural area or village, a small or middle size town, or a large town. I keep these response categories. In 2019 they were asked to choose “*one of these five names for your social class, which would you say you belong to - the working class, the lower middle class, the middle class, the upper middle class or the upper class?*”. I grouped them into working, middle or high to match the 2014 response choices. They were asked to describe their religious identity. The reference category is coded as Catholic. The other categories are Protestant, Atheists are grouped with Non believer/Agnostic answers, and the Other response collapses less frequent religion responses in Europe (Jewish, Orthodox, Other Christian, Muslim, Sikh, Buddhist, Hindu) to produce a 4-level variable.

Postmaterialism

The standard way to measure postmaterialism is to ask questions about people’s ranking of most important values for their country, using either 4-item, 10-item, or 12-item factor-loaded indexes

²⁰⁸ Another standardization procedure, subtracting from the observations the mean and dividing by its standard deviation is discussed at length in Gelman 2008.

developed and tested by Ronald Inglehart throughout his academic career²⁰⁹. Materialist response options invoke economic growth, fighting rising prices, maintaining order and respecting authority²¹⁰, and the fight against crime. Postmaterialism is measured by values like freedom of speech, giving people more say in important government decisions, more say on the job, and a desire to live in a society where “ideas count”. The goal is to identify traditional versus secular-rational values and survival versus self-expression values (Welzel and Inglehart 2005).

However, the surveys have three issues in this regard. The 2014 voter survey asked about voters’ “most important issue” in the election but did not draw on Inglehart’s batteries or exhaustively use his values lists. The 2019 study let respondents answer open-ended, complicating response comparisons across surveys. Furthermore, there was more data missingness in 2014 than in 2019; respondents in the first survey who reported not voting (n=12,847 or 42%) were excluded from the most important issue question, but not in 2019.

Due to survey constraints, I cannot replicate Inglehart’s factor-loaded index, so I turn to preferences measuring three other tradeoffs that generally capture post-material and material preferences. Respondents placed themselves on a scale from 0 to 10 whether:

You are fully in favor of same-sex marriage (0)
You are fully opposed to same-sex marriage (10),

whether they are:

fully opposed to a restrictive policy on immigration (reverse coded to 0)
fully in favour of a restrictive policy on immigration (reverse coded to 10),

and if:

Environmental protection should take priority even at the cost of economic growth (0)
Economic growth should take priority even at the cost of environmental protection (10).

²⁰⁹ For a succinct overview of Inglehart’s two-step methodology and question wording see Roser, otherwise see the Eurobarometer codebook.

²¹⁰ I address the issue of endogeneity that this raises below.

Welzel and Inglehart have previously tested if acceptance of homosexuality is strongly correlated with postmaterialism (2005). Attitudes towards homosexuality tap into survival versus self-expression and postmaterialism's traditional versus secular axis. I include the second question because historically, times of economic insecurity (the mechanism for ebbs and flows in material/postmaterial socialization (Inglehart 1977)) tend to generate physical insecurity against out-groups like immigrants. The third question taps into a tradeoff between economic security and quality of life that directly reflects material and postmaterial values. Environmental and immigration-based activism has been met with state surveillance, and there is ample historical evidence of the surveillance of homosexuals until full legal rights were granted in the 21st century. Regardless of the historical record, the current public debate centers around a perception that higher immigration leads to insecurity and rising crime rates.

Vote choice and ideology

I measure survey respondents' national party vote choice. The survey also asked about the EU Parliament vote. A considerable proportion of voters stated a domestic party vote choice (63.7%), but a large minority left the EU party choice unanswered (42.6%). Those who provided both displayed minimal switching between domestic and EU levels (see Appendix Figure 26). I have little reason to believe respondents who demurred from stating an EU vote choice would systematically also be vote-switching, but I use the domestic party preferences to avoid unnecessary data missingness.

I recode the vote choice options classifying each country's parties to the EU Parliament voting bloc affiliation. There are eight parliamentary blocs organized around ideological lines: Parties are classified as belonging to one of the following EU groups Conservative Reformists, Greens/European Free Alliance, Identity and Democracy, People's Party Christian Democrats, Progressive Alliance of Socialists and Democrats, Renew Europe, Nordic Green-Left, Non-attached members, unlisted parties, refused or system-missing responses of national vote choice. The modal and reference category is "Other", aggregating the last three non-substantive/abstaining vote choices.

I use these groupings instead of older categories, given the obsolescence and incomparability of specific categories in the contemporary party taxonomy (e.g., agricultural parties). This method increases comparability in two ways. First, it allows me to compare parties across countries. Small-party and small-country parties are often left out by comparative datasets, prioritizing parsimony in party-family categories (Kitschelt 2018). I expect right-leaning parties to favor security and left-wing party families to favor privacy. Center-right and center-left catch-all parties' voters may rely less on party cues because their parties feel either little pressure to compete on security or lower credibility due to involvement in privacy scandals.

The left-right scale of both survey waves asks:

In political matters people talk of “the left” and “the right”. What is your position? Please use a scale from 0 to 10, where ‘0’ means “left” and ‘10’ means “right”. Which number best describes your position?

The model also uses two variables to capture preferences around the size of the state. Economic interventionism is measured by respondent's preference for state and market relations by asking them to place themselves on a scale:

You are fully in favor of state intervention in the economy (0)

You are fully opposed to state intervention in the economy (10)

The variable capturing preferences for *how* economic interventionism is exercised is a sort of “Robin Hood” redistribution policy:

You fully in favour of redistribution from the rich to the poor in [country] (0)

You fully opposed of redistribution of wealth from the rich to the poor in [country] (10)

Institutions

I reverse-code the answers to “do you trust the [nationality parliament, use proper name for Lower House]” (Yes, totally; yes, somewhat; neither trust or distrust; No, not really; No, not at all) to reflect increasing levels of trust in the national House of Representatives equivalent for each EU country. I measure approval with a binary response question, “Do you approve or disapprove the government's record to date?”. I categorize whether respondents' answer to who they voted for last (national) election matches the party in power at the

time of the survey with a variable called voted for the winner (yes or no). I also reverse code political interest “*To what extent would you say you are interested in politics?*” (*Very, somewhat, a little, or not at all?*) so the variable’s directionality is ascending interest.

EU transnationalism

I reverse-coded the answers to *You trust the European Parliament* (*Yes, totally; yes, somewhat; neither trust or distrust; No, not really; No, not at all*). EU integration support is measured with the question:

Some say European unification should be pushed further. Others say it already has gone too far. What is your opinion? Please indicate your views using a scale from 0 to 10, where 0 means unification ‘has already gone too far’ and 10 means it ‘should be pushed further’. What number on this scale best describes your position?

Control variable measures

I control age (also divided by two standard deviations), education, gender, and news consumption (same standardization procedure). I calculate age from the given birth year to the survey year. Education is a function of reported years in school. People reporting less than 15 years of schooling are labeled “low”; 16-19 years of education is medium, and over 20 years is high. There is also a response category for those who are still studying. The survey did not ask them what stage of studies there were conducting, so I cannot collapse them into the three tiers. Gender is binary because a non-binary response option was missing in 2014; in 2019, only 29 people selected this response²¹¹. There are three response possibilities for 2014’s class question where respondents place themselves in either “the working class of society”, “the middle class of society”, or “The higher class of society”. I collapsed response options from the 2019 question to match the three tiers:

If you were asked to choose one of these five names for your social class, which would you say you belong to - the working class, the lower middle class, the middle class, the upper middle class or the upper class?

Media consumption questions were also asked differently in the two surveys. The 2014 survey asked people how frequently they got their news from different sources (TV, internet, newspapers), while

²¹¹ The responses were dropped.

the 2019 survey asked, “How closely did you follow the campaign ahead of the European Parliament elections in the media or on social media?” providing 0-10 responses. I transformed both into a 0-5 scale for both years to capture ascending news consumption. I then standardized this variable and all other numeric ones, dividing by twice their standard deviation.

Results

	Tradeoff choice	Selected in 2014	Selected in 2019	Difference	Pearson's Chi-squared test
Full support of privacy rights at the cost of security	0	8.21%	11.34%	3.13	157.57***
	1	3.05%	4.46%	1.41	77.782***
	2	5.82%	7.41%	1.59	57.643***
	3	7.64%	8.91%	1.27	29.815***
	4	6.60%	7.28%	0.68	10.143***
	5	20.89%	18.30%	-2.59	59.363***
	6	7.56%	7.66%	0.10	0.18725*
	7	9.34%	8.58%	-0.76	9.9627***
	8	7.86%	6.69%	-1.17	28.336***
	9	3.17%	3.16%	-0.01	0.0010827*
Neither is prioritized/traded	10	13.40%	11.18%	-2.22	64.038***
	No response/DK	6.46%	5.03%	-1.43	52.575***
Fully supports security at the cost of privacy	Total:	100%	100%		
	n = 52,885	n = 30,064	n = 26,538	-3,526	dummying each response of interest vs. all others (d.f. = 1)
	Statistics for All Table Factors: Pearson's Chi-squared test Chi ² = 498.7269, d.f. = 11, p = 5.99224e-100				Statistical significance of Pearson's Chi-squared test with Yeats correction *p<0.1; **p<0.05; ***p<0.01

Table 13 Proportion and difference of outcome responses by year

The tradeoff variable has a pooled mean of 5.17 and a standard deviation of 3.03. The number of respondents in 2019 is on average 89% that of the number in 2014²¹². Table 13 calculates the

²¹² It seems like the sample size was deliberately capped at 1,000 for almost all countries in 2019 except for Cyprus, Luxemburg, and Malta (capped around 500 2019). The biggest drop is Germany, which has a 61% sample size in 2019 compared to 1,648 in 2014, and the UK which has a 70% sample size compared to 1,421 in 2014. The other 26 countries have on average 91% sample size in 2019 compared to 2014.

proportion of each response selection within each survey. I can meaningfully compare response frequency differences within and across surveys as proportions. In both surveys, the most popular response is 5 (~21% and ~18%), reflecting an unwillingness to trade between protecting privacy rights in the face of hindering or combating crime or pursuing crime-fighting strategies. Respondents who picked 5 were not systematically different from others in their response time²¹³. Furthermore, the range of non-responsiveness is similar to other response options²¹⁴. From this evidence, I assume 5 responses are authentic preferences, as valid as all other choices, including the choice not to respond.

The table also calculates the difference in proportions of each choice between surveys. The largest differences are an increase of 3.13 points in the 0 response (fully support privacy rights even if they hinder efforts to combat crime), a decrease of 2.59 points in the 5 response (tradeoff refusal), and a reduction in the 10 response (fully in favor of restricting privacy rights in order to combat crime). I ran a Pearson's Chi-squared test of independence to discard the possibility that the distributions could also be observed if there was no relationship between the independent (years proportions) and dependent variable (response options). The χ^2 test of independence for all table factors tests the null hypothesis that the response categories and survey years are unrelated (498.73, d.f. = 11, p-value = $5.99e^{-100}$). The infinitesimally small p-value allows me to reject the null hypothesis²¹⁵, we accept the alternative hypothesis that each category is different for each point in time. On the right-most column

²¹³ After reviewing interviewer notes on respondent cooperation and completion time, we can report that neutral respondents are no different from other respondents in this regard. All categories of respondents, regardless of their answer, had a modal survey time of 30- 44 minutes, followed by 15 - 29, and 45 - 59 minutes. After turning respondents' time and answers into a frequency, I can see that 9.45% respondents answered 5 and took 30- 44 minutes, followed by 6.6% who answered 10 and took the same amount of time, followed again by 5-respondents who took 15-29 minutes (6.4%). 3.8% of respondents answered 0 (fully support privacy rights) and took 30- 44 minutes (the modal category of the group). The time categories were constructed by the survey authors. In the 2014 survey, respondent cooperation is noted. 3760 neutral respondents were scored excellent and 1754 scored fair. This was the highest level of fair scores in any other category, but respondents who answered 10 (fully restricting privacy) followed—2622 scored excellent and 1031 scored fair. Given these metrics, I am inclined to believe these are people who replied 5 should be taken at face value.

²¹⁴ Non-response rates are also smaller than the ideological variable non-response rates (18.9% in 2014, 14.0% in 2019), and do not present any systematic component to its distribution.

²¹⁵ There is an extremely small chance (p-value) we would observe the relationship's large estimate if the null hypothesis was correct ($p < 0.005$).

is a dummied Pearson's Chi-squared test of independence comparing the difference of each response option to all others, grouped (0 vs. all others, 1 vs. all others ... No response vs. all others). Almost all differences in response proportions between the two surveys are statistically significant except for the minimal change in 6 responses (0.10 percentage point increase).

This table is the first part of the findings I will analyze in this chapter which counters the assumption that most people do not care about privacy²¹⁶. Crime may be a valence issue, but strategies for fighting crime—especially those jeopardizing privacy—are *not* a valence issue. The distributional evidence in the range of demand supports the idea that there could be party competition on the supply of policies against alternative crime-fighting surveillance policies that curtail privacy. However, that competition is unlikely to converge around a median voter, which I will discuss in the second section of the results (logit results).

The models deal with unobservable country-level heterogeneity using country-fixed effects. In the next section, I provide a descriptive overview of responses averaged by countries and some observations about the data. In the section after that, I present results from my hypotheses testing on the correlates of respondents' policy preferences when the outcome is an interval scale and then discuss the results from transforming the variable to a binary category where I distinguish tradeoff refusal responses (5) from all other substantive responses. The appendix lists all other variables' summary statistics without and with the standardization (Table 15 and Table 16).

²¹⁶ As discussed in Chapter 1, this statement is often repeated by American Data Goliaths. In my original survey I replicated this EU question. I offer one cautious comparison since there are 3 years' difference between the last European and the American survey. In the US in 2021, 20.9% picked no tradeoff, 31.3% a response that leaned towards privacy, 41.3% one that leaned towards security, and 6.5% chose not to respond (see appendix Figure 25 for a visualization of the full US distribution). Those distributions are more similar to the pre-GDPR European attitudes than the 2019 ones: No tradeoff 20.9% then 18.3%, privacy 31.3% then 39.4%, Security 41.3% then 37.3%, nonresponse 6.5% then 5.0%. The US' average (5.725) is very similar to the Netherlands' which changed little over time (5.82 then 5.7) but its distribution shape is more similar to the UK's 2014 (but not 2019) except for the security preferences are more polarized in the US (high spike in 10s where the UK's 6+ responses are spread out more evenly).

Descriptives for country-level surveillance

To compare responses by country descriptively, I first calculate the average by country in Figure 21. Lower scores reflect more privacy-desiring responses in the tradeoff; higher scores reflect more security tradeoff demands. There are nearly two points' difference between the lowest and highest averages in the EU countries. Only Austria, the country whose European Union members of Parliament cast a protest no vote for the GDPR because they wanted more strict guidelines, has a higher privacy demand than Germany. Theocharis and Van Deth hypothesize that Germans' low use of social media despite high internet penetration is related to their privacy attitudes (2018). The UK's ranking, almost in the median, is surprising in light of the fact that it is a Five-Eyes signals intelligence partner and has a history of ubiquitous public camera surveillance (closed circuit TV or CCTV). This suggests that widespread surveillance in the UK is not a function of public demand for security.

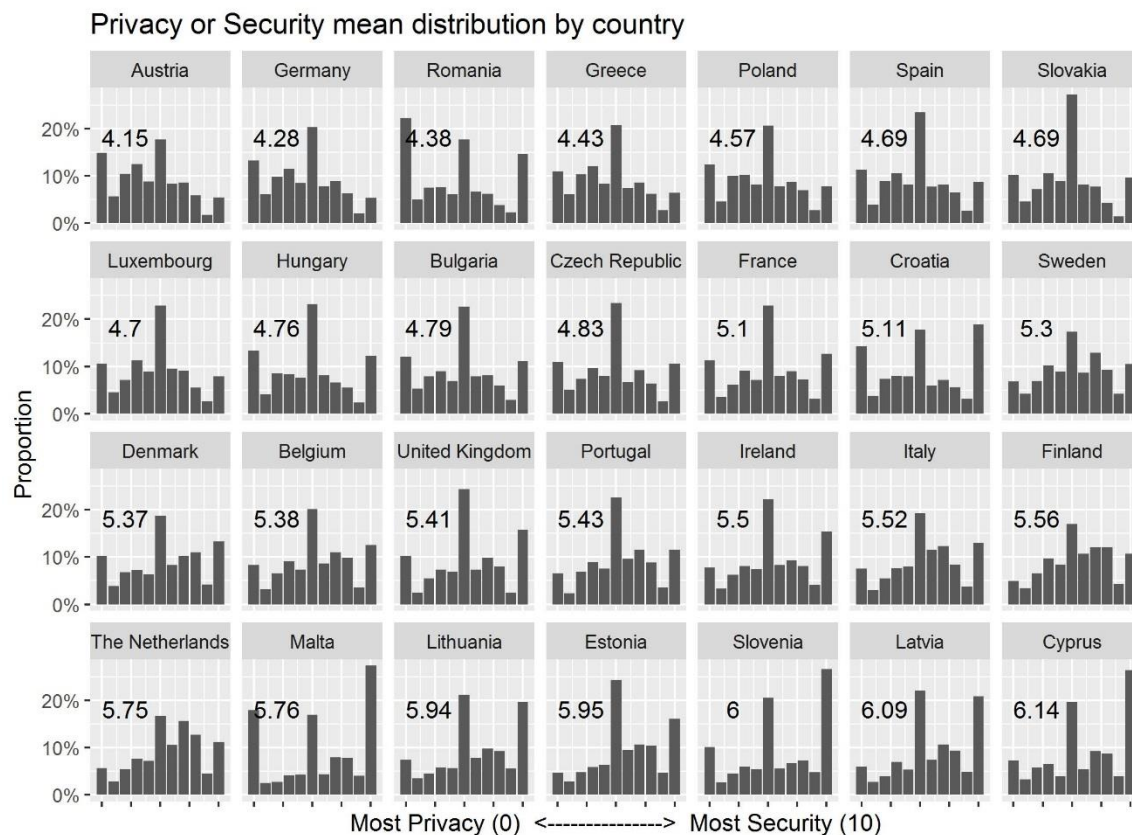


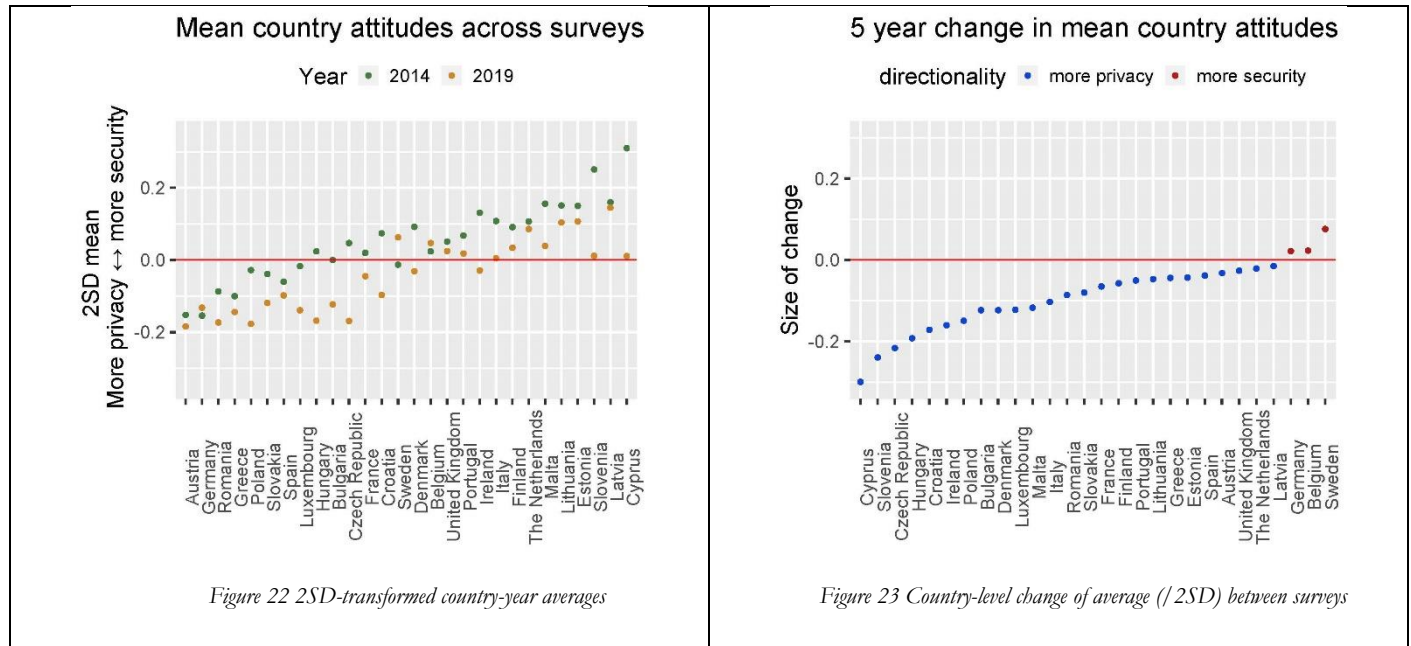
Figure 21 Country-level average preference distribution

Relative differences between countries are not distributed intuitively. The bizarre and non-intuitive patterns between countries' averages further justify using fixed effects for country-level variation accounting and a year variable in the regression model. Regional clustering of attitudes would have suggested historical-institutional patterns shaping shared expectations of privacy and experiences of (in)security. However, neither geography (East-West divide), major religion (Catholic-Protestant confessional tradition), nor economic strength (GDP) seems to drive the aggregate distributions.

However, averages are an imperfect summary to compare nations. Notice how Lithuania, Estonia, and Slovenia have somewhat similar *averages*. However, Estonia has the fewest share of '10' responses, while Slovenia's 10 answers are its modal choice. Malta also has a similar average to the Netherlands. However, Maltese responses are highly populated in utter certainty in the tradeoff choices (0 and 10) and neutrality (5); in contrast, the Dutch have one of the closest approximations to a normal distribution even though the more popular middling categories skew towards more security (7 is the second-most popular category).

To consider the differences between survey waves, I disaggregate the means by year. In Figure 22, I sort the countries on the X-axis by their combined averages (the order in Figure 21). The y-axis standardizes the tradeoff by dividing it by two standard deviations (6.06). The global mean becomes recoded as zero, which constrains the values to a shorter scale and allows a more intuitive comparison with the graph on the right. In Figure 23 I further illustrate the size of the change within countries' average responses. I recode the difference and color-code the shift in direction; I sort the x-axis by the size of the change. Cyprus (the member with the highest pooled average) had the highest swing toward privacy responses in 2019 compared to 2014. Slovenia similarly had a very high pooled average and the second-highest change in the same direction. After the GDPR's passing almost all countries' voters prefer privacy at the cost of fighting crime. Germany, Belgium, and Sweden were the only countries with increased averages in 2019 compared to 2014, but only Sweden's is notable (<0.4

increase in the standardized scale), but the size of the change in Germany and Belgium are small (0.02 increase in standard deviation for both). Sweden's change is 3.8 times larger (0.076), between France's (0.065) and Slovakia's (0.08) change but in the opposite direction.



Privacy-security tradeoff as an interval scale

I code the outcome variable so that a negative correlation sign is interpreted as an increased desire for privacy at the cost of security (“combating crime”), and the unit of change for the independent variables is one standard deviation change. Country-fixed effects help account for hard-to-measure country-specific variation in the outcome²¹⁷. The change in the outcome should be interpreted as one standard deviation change for numeric variables, making the continuous variable effects comparable to categorical variables (Gelman 2008), controlling for all other variables in the model and country-specific characteristics. I grouped the variables in the model according to the theory section, sorting

²¹⁷ The adjusted R² modest but in line with European privacy attitude (experiment) surveys (Ziller and Helbling 2020). It improved when adding country fixed effects. A comparison of OLS models with and without fixed effects is presented in the appendix.

theories by their explanatory power²¹⁸. The model explains approximately 11% of the variation in the interval measure of privacy/security tradeoff (adjusted R^2)²¹⁹.

Figure 24 *Tradeoff regression model dot-plot* visualizes the coefficient estimated by the OLS model and the 95% confidence intervals of each estimate. The null hypothesis for each variable is that X variable plays no effect (e.g., zero) on tradeoff preferences. If a variable or category level with an estimate or confidence interval visually crosses the red vertical line demarcating zero, I cannot reject the null hypothesis with more than 95% confidence. If the estimates and confidence intervals do not cross zero, I can reject the null hypothesis (no effect) and accept the alternative hypothesis pertaining to that variable. The traditional regression table is available as Table 17 in the appendix.

²¹⁸ I go through the variables in the order of most to least contributing to the adjusted R^2 . When I tested the variables clustered by theories, the model with postmaterial variables had an adjusted R^2 0.093, the model with party and ideological variables had an adjusted R^2 0.079, the institutional model had an adjusted R^2 0.068, the model with classic cleavage variables had an adjusted R^2 0.064, the model testing EU cleavage variables had an adjusted R^2 0.062, and sociodemographic variables an adjusted R^2 0.058.

²¹⁹ I test error variance, which appears to be homoscedastic ($p = 0.390$) (i.e., random disturbance in the relationship between the independent variables and the dependent variable; the residuals are independent and not autocorrelated ($p = 0.840$)).

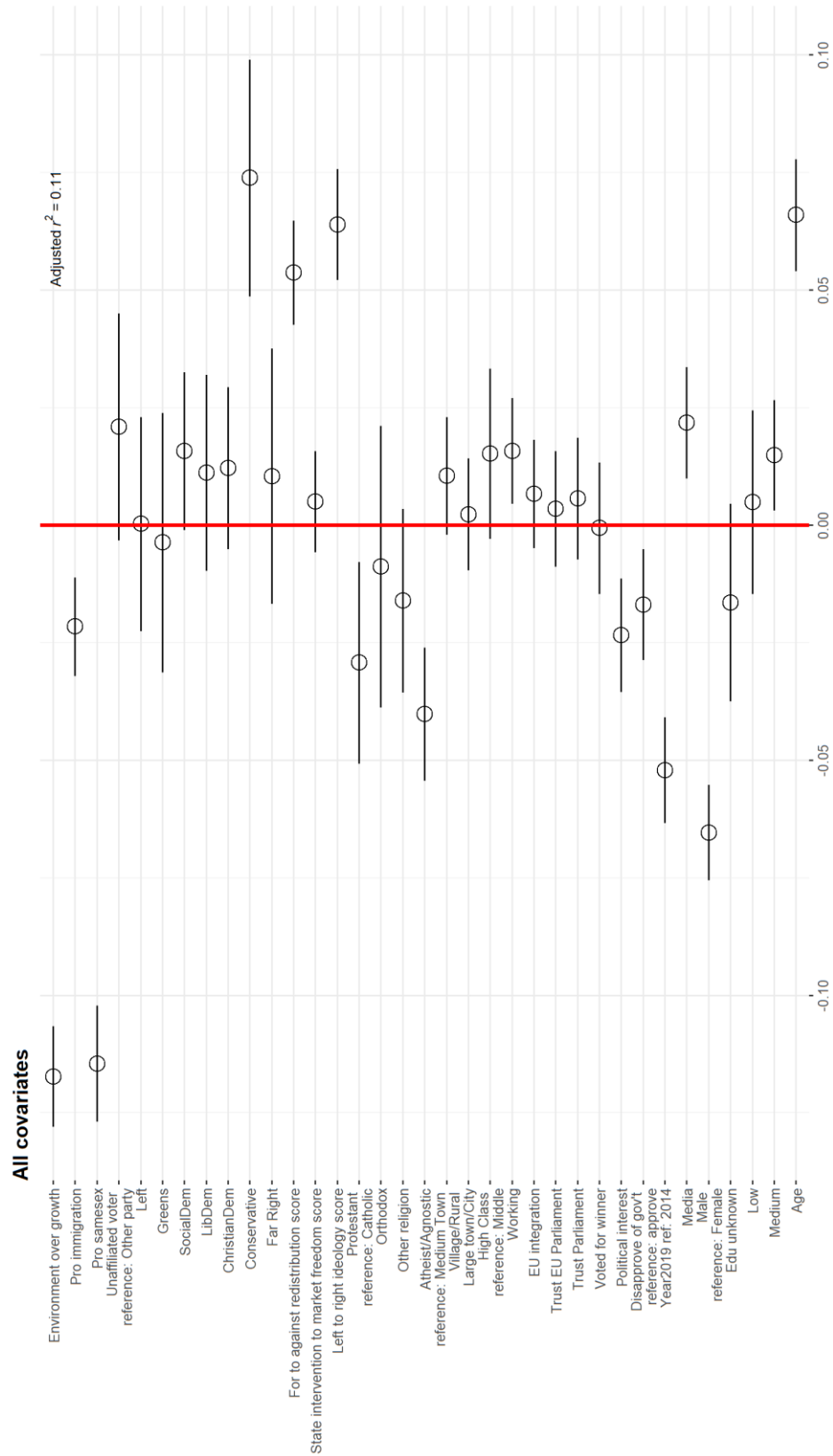


Figure 24 Tradeoff regression model dot-plot

Postmaterialism emphasizes quality of life, while materialism is concerned with securing life (survival) regardless of its quality. I hypothesized that those with postmaterialist values would be associated with privacy preferences, and materialists would prefer security. All three preference responses related to postmaterial theory²²⁰ are correlated to the privacy-security tradeoff in the way I expected. A one standard deviation change in the homosexual marriage question in the direction of “You are fully in favor of same-sex marriage” is associated with a -0.114 change in the tradeoff toward privacy preferences. A change in one standard deviation in the environmental question in the direction of “environmental protection should take priority even at the cost of economic growth” is associated with a -0.117 change in the tradeoff toward privacy preferences. These two values are associated with the largest change in the outcome. One standard deviation toward being opposed to a restrictive policy on immigration is associated with a -0.0215 move toward privacy. The smaller substantive effect is nonetheless statistically significant (95%) and consistent in its directionality with postmaterialist theory²²¹.

Conservative party voters are the only statistically significant group with clarity in their preference for security (0.0739 change in SD, the third strongest correlation in the model). The reference category is Other, aggregating respondents with non-substantive party vote choices. No other party’s vote choice is statistically associated with a tradeoff choice compared to Other vote respondents in any direction. While I anticipated this finding in the “fuzzy middle” hypothesis for centrist parties, I hypothesized a mirrored privacy preference for Left and Green voters, not expecting the lack of clarity and statistical effect for these voters.

²²⁰ Attitudes towards prioritizing the environment over economic growth, positive attitudes towards same sex marriage, and positive attitudes towards immigration.

²²¹ The directionality is also present if I use the 2014 most important issues responses categorized into materialist/postmaterialist values.

A continuous measure of ideology (0 left – 10 right) is positively and strongly associated with tradeoff preferences, with a one standard deviation change in the ideology score (0.5) associated with a 0.064 ($p < 0.05$) standard deviation increase in the tradeoff toward security. Ideological preferences explicitly measuring the size of the state are also in the hypothesized direction though only the measure of economic redistribution preferences is statistically significant (0.054, $p < 0.05$)²²². The hypotheses that both attitudes favoring interventionism and redistribution would mirror left-right ideological placement is only partially met. The evidence suggests that people's desire or distaste for state intervention/freedom in the market and civil liberties is not statistically associated with their tradeoff preference (0.005, $p > 0.1$); their attitudes toward state action on redistribution in the face of wealth inequality and privacy versus crime is.

I also hypothesized that respondents' positive relationships with their domestic political institutions, measured in terms of trust and approval, would be associated with a willingness to cede privacy in the tradeoff because they would have fewer reasons to be suspicious of abuse of power. In contrast, mistrusting and dissatisfied respondents would be unwilling to expand policing powers at the cost of privacy protections. I find no evidence that trust is statistically significantly associated with trading privacy for security. However, disapproving of the government is statistically significantly associated with preferring privacy (0.0169 SD change) compared to those who approve of the government. Furthermore, the hypothesized direction for political interest (positively correlated to higher security preferences) is reversed but statistically significant²²³. That is, a standard deviation increase in political interest is associated with a change of -0.023 in the standard deviation of the tradeoff toward privacy preferences.

²²² Left-right placement is weakly correlated positively with economic interventionism (0.154 $p < 0.001$) and somewhat moderately correlated positively with redistribution (0.250 $p < 0.001$).

²²³ This hypothesis was based on previous work finding a positive association between trust in government, political interest and approval (Catterberg and Moreno 2006). However, in this data, the relationships are only positive and statistically significant for trust and political interest, the two other combinations are *negative* but not statistically different from the null hypothesis estimate.

Variables capturing the classic cleavages are categorical. The results require nuanced analysis because no variable has statistically significant effects in the tradeoff from all its categories. The class cleavage association is limited to working-class respondents, who are statistically significantly more pro-security (0.0158 change in the tradeoff's standard deviation) than middle-class (reference category) and upper-class respondents. There is a moderate presence of a religious/secular cleavage, with non-religious people having the highest preference for privacy (almost a 0.04 change in the outcome's standard deviation), followed by the non-confessional Protestant sects (0.0292 change), with Catholics as the reference category. Orthodox and other religions have no tradeoff preference differences compared to Catholics. Perhaps respondents with confessional religious faiths are accustomed to thinking there is no true privacy if their god is omniscient. From there, it may be inconspicuous to religious people that the state, too, should be able to look in on its citizens. Further speculation is beyond the scope of this chapter but might be a fruitful avenue for future research.

Turning toward the European Union, trust in its Parliament and attitudes toward further integration are not statistically significantly associated with tradeoff preferences (against our hypothesis). These results suggest that neither privacy (the more straightforward case to make) nor security (the more challenging case) are associated with the EU policy-making bodies, despite both issues' federalization.

The sociodemographic controls of (increasing) age and being a man (compared to being a woman) are statistically significantly associated with a tradeoff but in opposite directions. Age is the fourth largest estimate in the model. One standard deviation change in age is associated with a positive 0.066 change in trading security against privacy; male self-identification is the fifth largest estimate, associated with a -0.0653 SD change toward privacy, compared to women. This effect is consistent with gender dynamics found in other surveys, which served as the basis for my hypothesis expectation (Huddy, et al. 2005). A medium level of education is statistically significantly associated with a tradeoff

preference change towards security (0.0149 SD change), compared to the high education reference category, but neither low education nor undisclosed levels are associated with the tradeoff in any statistically significant way. Heightened media consumption is positively associated with a 0.022 increase in pro-security attitudes in the tradeoff. Media effects might be due to coverage trends ('if it bleeds, it leads'), where news production emphasizes crime and insecurity in coverage compared to many other topics²²⁴.

Lastly, the variable distinguishing survey years reflects the "sharpening" attitudes towards privacy addressed in the descriptive statistics. Answering in 2019 is associated with a 0.0521 change in the tradeoff's standard deviation toward privacy compared to 2014, controlling for all other variables in the model. This suggests that, instead of a demand → policy supply story, we are more likely seeing a policy supply → support story. We do not have data for the tradeoff before the Snowden revelations. However, do to know that European Union Parliament members were elected in 2019 by voters that had overall more clarity in their preferences for privacy after the institution delivered on a piece of legislation than when the issue was a year old. Though I cannot speak causally, the order of events suggests that voters' willingness to emphasize privacy, instead of or security or both equally, followed the passing and first year of data protection enforcement. The mechanism may be familiarization with the issue through political debate, as well as the increased visibility of data retention disclosures, explicit requests for permissions in online services, etc.

²²⁴ The 2014 survey included had a longer battery asking how people received their news but the 2019 did not so I cannot distinguish between online and TV news consumption. More respondents got their news from TV than from the internet and TV viewers were more willing to trade security for privacy. Those who read newspapers were more willing to express a concrete policy preference than those who do not. Internet news did not seem to have a substantial effect on its readers' opinions or desire to express them.

Examining the refusal to trade off privacy and security

The 11-point scale's modal response category in both surveys is 5 (~20%). In this section, I consider that outcome as a binary to preferring a tradeoff position—independent of the direction. The exercise is exploratory, but is important to public opinion research on willingness to express or self-censor policy preferences (Berinsky and Lavine 2011, Schlozman, Verba and Brady 2012). This analysis will reveal characteristics of those who feel potentially conflicted about the two goals and weigh them equally important. I re-calculated the model with the transformed outcome using logistic regression and all the variables from the OLS. I only report statistically significant variables associated with refusing or making the tradeoff in at least one category or as a function of a standard deviation change (for numeric variables).

The “5” responses refusing the tradeoff are of substantive interest, so I code this category as 1 and all other responses as 0 (the modal category when grouped, ~80%). The directionality of this recode does not affect the variables' associated effects. A negative sign in the logit or percentage should be interpreted as associated with the odds of making the tradeoff, and a positive sign as the odds of refusing to make the tradeoff. The size of a logit's log odds cannot be interpreted directly, so exponentiate the logit estimates as percentages.

Term (1 SD if continuous)	Logit estimate	Std. error	exponentiated estimate	Odds as percent
Male (ref Female)	-0.126***	0.028	0.882	-11.8%
Media (1 SD)	-0.096***	0.033	0.909	-9.1%
Not religious (ref Yes)	-0.095***	0.034	0.910	-9.0%
Approve to disapprove: of same-sex marriage	-0.089***	0.034	0.915	-8.5%
of environment over econ growth	-0.156***	0.029	0.855	-14.5%
Vote:				
FarRight (reference Other)	-0.183***	0.078	0.833	-16.7%
Conservative	-0.215***	0.072	0.807	-19.3%
ChristianDem	-0.118***	0.048	0.889	-11.1%

LibDem	-0.095	0.058	0.909	-9.1%
SocialDem	-0.02	0.046	0.980	-2.0%
Greens	0.039	0.077	1.040	4.0%
Left	0.048	0.063	1.049	4.9%
Unaffiliated party	-0.012	0.066	0.988	-1.2%
Year 2019 (reference 2014)	-0.119***	0.031	0.888	-11.2%

Table 14 Logit model's statistically significant exponentiated estimates.

Women have lower odds (by almost 12%) to refuse to make the tradeoff, compared to men, in line with previous findings of gendered expression of politics and policy preferences (Beauvais 2019). A change of one standard deviation in consuming less media during the respective EU campaigns is associated with 9.1% odds of refusing the tradeoff. Only two of the postmaterialist values are statistically significantly associated with the choice to not to trade off or trade privacy against security. A one standard deviation decrease in the attitude toward approving of same-sex marriage and protecting the environment against economic growth are statistically significantly associated with refusing to make the tradeoff by 8.5% and 14.5% odds, respectively.

Responding during the 2014 EU election is associated with 11.2% higher odds of refusing to make the tradeoff compared to 2019. In this model, I collapsed religious categories. Religious respondents have a 9% increased odds of refusing the tradeoff compared to those who are non-religious. In contrast to the linear model, the logit estimates put all right-leaning voters, whether center-right (Christian Democrats), right (Conservative), or Far Right, as having statistically significantly higher odds of making the tradeoff (11.1%, 19.3%, and 16.7%) compared to those grouped in the other voter category. Green and Left voters have higher odds of refusing the tradeoff (positive sign estimates, 4%, and 4.9%, respectively), but these estimates are not statistically significantly different from the null hypothesis, so we cannot state this with 95% confidence. The same goes for Social Democrats and Liberal Democrats, but their estimates' signs are associated with making the tradeoff.

Conclusion

This chapter lays the groundwork for further research on European's desire for privacy. The European reaction to the Snowden revelations, at the policy supply and demand level, provides an alternative comparison to the US. In Europe, the political cost of the surveillance complex, driven by American demands for data, seemed to become higher—reputationally at first for politicians dealing with the fallout and later directly associated with increased privacy demands.

This chapter used secondary data that provides a direct insight into one of the justifications for expanding mass surveillance: the promise of increased security. American attitudes favoring surveillance increased when policies make law enforcement and when disliked groups are made salient. Some European governments are members of intelligence-sharing alliances with the US. The UK in particular, was the first country to sign up during World War II to the data sharing agreement (Radden Keefe 2005), later bringing in its Commonwealth nations (Canada, New Zealand, and Australia), creating the Five Eyes organization (Privacy International, Molinaro 2021). As discussed in Chapter 1, The US has extended/delegated their intelligence gathering to European nations in a web of quasi-quid-pro-quos where governments can at times rely on the US, the central node, to convey surveillance information gathered by other partners if they also conduct foreign espionage. Denmark, France, and the Netherlands are the European Nine Eyes partners while Belgium, Denmark, Germany, Italy, Spain, and Sweden are the European members of a less closely knit Fourteen Eyes membership.

Despite the political justification that surveillance is necessary to thwart terrorism, Europeans have still experienced foreign and domestic terrorism during that time. In a tradeoff pitting security against privacy, European attitudes have varied across nations and time.

In contrast to other European studies, I was able to analyze privacy and security as a tradeoff instead of using two valence measures inferred to be mutually exclusive (Friedewald, Lieshout, et al. 2014). First, I find that preferences for privacy *at the cost of* security are most strongly associated with

attitudes toward quality of life versus materialist values, exemplified by attitudes toward same-sex marriage, prioritizing environmentalism over economic growth, and accepting immigration. This suggests that in people's minds, privacy is a component, maybe even a necessary one, of autonomy and well-being. Second, issue-ownership for security in voters' minds is not symmetrical to issue-ownership for privacy. Conservative party voters have more explicit security preferences than other voters. Right-wing ideology, construed in a left-right space or through market freedom and non-redistribution of wealth, is also associated with a more traditional demand for governments to provide security, even at the cost of privacy. The mirror image is the left-wing demand for privacy, even at the expense of the government's ability to combat crime. Europeans who care about privacy are not a negligible electoral minority in many of the EU countries, and their numbers are growing as time passes and as policies protecting privacy become institutionalized (e.g., GDPR, right to be forgotten, etc.). In 2014, 41.3% of Europeans preferred some security even at the cost of privacy, while 31.3% wanted the opposite, and 20.9% wanted both equally. Five years later, security preferences were statistically significantly lower, at 37.3%, while privacy preferences grew from 31.3% to 39.4%, and fewer people (18.3%) were willing to refuse to trade one for the other.

The European Union's institutions have been at the forefront of an international and domestic critique of the surveillance complex. A report analyzing its use by European Union members characterized deputized surveillance as a "gangrenous" technology whose impact "reverberates on its own constituent governments' democratic health and peoples' freedom" (European Parliament 2022). Despite the European Union's policy-supplying role, these preferences are more closely associated with voters' approval of their government and interest in politics, not on trust in the European Parliament or their domestic Parliament. In many European countries, an entrepreneurial party could capitalize on domestic demand and run on privacy successfully (Siewert and König 2019), particularly

if they contrast privacy against police surveillance powers accessible to entrenched but distrusted governments or parties in power.

Substantive choices on a tradeoff between privacy and security are somewhat associated with demographic characteristics, like age, gender, education, and class, but these do not provide a complete picture. Voter choice variables and country-year fixed effects improve our understanding but do not explain all the preference variation.

The modest explanatory power of the OLS model (11% adjusted R^2) should incentivize additional comparative work within and in contrast to Europe. Are Europeans satisfied with their novel privacy-protecting policies, or is this just the start? Do they want better enforcement of the current rules? What accounts for the heterogeneity in distributions and relative mean differences across European Union members, and will this heterogeneity decrease if policies ‘federalize’ rights and regulation on Data Goliaths? For example, to what degree will national capacity or domestic political will to investigate data breaches and enforce GDPR fines reinforce people’s perception that their privacy concerns matter, or will policy enforcement fail and produce voter dismay?

Future research ought to keep track of preference trends. Smaller parties initiated public deliberation and political discourse on privacy, yet the 2016 General Data Protection Regulation was a product of almost complete consensus at the EU parliament. Larger/entrenched parties proved capable of acting in ways that American parties could not or were unwilling to. But they are not immune to future capture by Big Tech. The Irish Data Protection Commission has taken the lead on cases against Data Goliaths because they are headquartered there for tax purposes. Privacy civil society actors have accused the Irish DPC of deliberately dragging its feet and acting in bad faith to shield them (Baker 2020, None of Your Business 2020, People Vs. Big Tech 2023). Might these obstacles mobilize voter demand for better oversight, or will Europeans become despondent if their privacy-protecting enforcement mechanisms fall short?

If enforcement is heterogeneous, will this influence some European citizens' informational environment? And if sufficiently enforced, will the European data protections incentivize Data Goliaths to rethink their surveillance needs and capacities, constraining data collection and its flow in the surveillance complex even at the cost of American access? Will the internet splinter to accommodate the divergent European and American expectations? Or will they decide that alienating European customers and governments is a tenable cost of doing business in exchange for the status quo? All these questions require an expanded and comparative research agenda on the interplay between supply and demand across advanced democratic governments.

Bibliography

- Access Now. 2023. *EU ministers are targeting encryption. We need to know more*. January 13. Accessed April 24, 2023. <https://www.accessnow.org/eu-ministers-targeting-encryption-need-know/>.
- Angrist, Joshua D., and Steffen Pischke. 2009. *Mostly Harmless Econometrics: An Empiricist's Companion*. Princeton: Princeton University Press.
- Baker, Jennifer. 2020. *Schrems Slams Slow Irish DPA*. June 02. Accessed May 3, 2023. <https://www.cpomagazine.com/data-protection/schrems-slams-slow-irish-dpa/>.
- BBC News. 2011. *Pirate Parties: From digital rights to political power*. October 18. Accessed November 14, 2016. <http://www.bbc.com/news/technology-15288907>.
- Beauvais, Edana. 2019. "Discursive Inequity and the Internal Exclusion of Women Speakers." *Political Research Quarterly* 1-14.
- Berinsky, Adam, and Howard Lavine. 2011. "Self-Monitoring and Political Attitudes." In *Improving Public Opinion Surveys*, edited by John H. Aldrich and Kathleen M. McGraw, 27-45. Princeton: Princeton University Press.
- boyd, danah. 2014. *It's complicated: the social lives of networked teens*. New Haven: Yale University Press.
- Budge, Ian, and Dennis J. Farlie. 1983. *Explaining and Predicting Elections: Issue Effects and Party Strategies in 23 Democracies*. London: Allen & Unwin.
- Burkell, Jacqueline, and Priscilla. M Regan. 2019. "Voter preferences, voter manipulation, voter analytics: policy options for less surveillance and more autonomy." *Internet Policy Review* 8 (4): 1-24. doi:10.14763/2019.4.1438.
- Burns, Janet. 2018. "Whistleblower: Bannon Sought To Suppress Black Voters With Cambridge Analytica." *Forbes*, May 18.
- Catterberg, Gabriela, and Alejandro Moreno. 2006. "The Individual Bases of Political Trust: Trends in New and Established Democracies." *International Journal of Public Opinion Research* 18 (1): 31-48.
- Converse, Philip E. 1964. *The nature of belief systems in mass publics*. Vol. 18. 1-3 vols. Critical Review. doi:10.1080/08913810608443650.
- Corporate Europe Observatory. 2018. *Shutting down ePrivacy: lobby bandwagon targets Council*. April 06. Accessed June 02, 2021. <https://corporateeurope.org/en/power-lobbies/2018/06/shutting-down-eprivacy-lobby-bandwagon-targets-council>.

- . 2017. *The industry lobby battle against ePrivacy*. October 17. Accessed June 07, 2021. <https://corporateeurope.org/en/power-lobbies/2017/10/big-data-watching-you>.
- Council of the EU and the European Council. 2021. *Terrorism in the EU: facts and figures*. Infographic, Brussels: Council of the EU and the European Council. <https://www.consilium.europa.eu/en/infographics/terrorism-eu-facts-figures/>.
- Dalton, Russell J., and Martin P. Wattenberg. 2000. *Parties Without Partisans: Political Change in Advanced Industrial Democracies*. Oxford: Oxford University Press.
- Dalton, Russell. 2020. "The Representation Gap and Political Sophistication: A Contrarian Perspective." *Comparative Political Studies* 1-29. doi:10.1177/0010414020957673.
- Downs, Anthony. 1957. *An Economic Theory of Democracy*. New York: Harper.
- Eddy, Melissa. 2022. "Right to Privacy Extends to Foreign Internet Users, German Court Rules." *The New York Times*, May 19: Section A, Page 17. Accessed April 16, 2022. <https://www.nytimes.com/2020/05/19/world/europe/germany-privacy.html>.
- European Parliament. 2022. *Draft Report Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance*. Brussels: European Parliament. [https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA\(2022\)732268_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf).
- Fisher, Sara. 2019. *Facebook users in the U.S. and Canada are the most valuable*. February 22. Accessed February 22, 2019. <https://www.axios.com/facebook-users-valuable-united-states-europe-c7ee74ad-8012-400f-a142-fe110dd6b6af.html>.
- Fraile, Marta, and Raul Gomez. 2017. "Bridging the enduring gender gap in political interest in Europe: The relevance of promoting gender equality." *European Journal of Political Research* 56: 601-618. doi:<https://doi-org.proxy3.library.mcgill.ca/10.1111/1475-6765.12200>.
- Friedewald, Michael, Marc Lieshout, and Sven Rung. 2016. "Modelling the Relationship Between Privacy and Security Perceptions and the Acceptance of Surveillance Practices." *Privacy and Identity Management. Time for a Revolution? : 10th IFIP Advances in Information and Communication Technology*. Edinburgh: Springer International Publishing. 1-18.
- Friedewald, Michael, Marc Lieshout, Sven Rung, Merel Ooms, and Jelmer Ypma. 2014. "Privacy and Security Perceptions of European Citizens_ A Test of the Trade-Off Model." *9th Privacy and Identity Management for the Future Internet in the Age of Globalisation*. Patras: Springer. 39-53. doi:10.1007/978-3-319-18621-4_4.
- Gandy, Oscar H. 1995. "The role of theory in the policy process: A response to Professor Westin." In *Toward an Information Bill of Rights and Responsibilities*, edited by C. Firestone and J. Schement, 99-106. Washington, D.C.: The Aspen Institute Communications.
- Garcia, Blake E., and Nehemia Geva. 2016. "Security Versus Liberty in the Context." *Terrorism and Political Violence* 48: 30-48. doi:10.1080/09546553.2013.878704.
- Gelman, Andrew. 2008. "Scaling regression inputs by dividing by two standard deviations." *Statistics in Medicine* 27: 2865-2873. <https://onlinelibrary.wiley.com/doi/10.1002/sim.3107>.
- Gershtenson, Joseph, Jeffrey Ladewig, and Dennis L. Plan. 2006. "Parties, Institutional Control, and Trust in Government." *Social Science Quarterly* 882-902.
- Hagemann, Sara, Sara B. Hobolt, and Christopher Wratil. 2016. "Government responsiveness in the European Union: evidence from council voting." *Comparative Political Studies* 50 (6): 850-876. https://eprints.lse.ac.uk/64513/7/Hobolt%20et%20al.%20_Government%20responsiveness.pdf.
- Hampson, Fen Osler, and Eric Jardine. 2016. *Look who's watching: surveillance, treachery, and trust online*. Waterloo: Centre for International Governance Innovation.
- Hargattai, Eszter, and danah boyd. 2010. "Facebook Privacy settings: who cares?" *First Monday*. <https://firstmonday.org/article/view/3086/2589>.

- Herschinger, Eva, Markus Jachtenfuchs, and Christiane Kraft-Kasack. 2011. "Scratching the heart of the artichoke? How international institutions and the European Union constrain the state monopoly of force." *European Political Science Review* 3 (3): 445-468.
- Hooghe, Liesbet, and Gary Marks. 2018. "Cleavage theory meets Europe's crises: Lipset, Rokkan, and the transnational cleavage." *Journal of European Public Policy* 25 (1): 109-135. doi:10.1080/13501763.2017.1310279.
- Hooghe, Liesbet, and Gary Marks. 2019. "Grand theories of European integration in the twenty-first century." *Journal of European Public Policy* 26 (8): 1113-1133. doi:10.1080/13501763.2019.1569711.
- Huddy, Leonie, Stanley Feldman, Charles Taber, and Gallya Lahav. 2005. "Threat, Anxiety, and Support of Antiterrorism Policies." *American Journal of Political Science* 49 (3): 593-608.
- Inglehart, Ronald. 2008. "Changing Values among Western Publics from 1970 to 2006." *West European Politics* 31 (2): 130-146.
- Inglehart, Ronald. 2007. "Postmaterialist Values and the Shift from Survival to Self-Expression Values." In *The Oxford Handbook of Political Behavior*, by Russell J. Dalton and Hans-Dieter Klingemann, 223-240. Oxford: Oxford University Press.
- . 1977. *The Silent Revolution: Changing Values and Political Styles Among Western Publics*. Princeton: Princeton University Press.
- Jones, Meg Leta. 2018. *Ctrl + Z*. New York: New York University Press.
- Kitschelt, Herbert. 2018. "Party Families and Political Ideologies." *Oxford Research Encyclopedia of Political Behavior, Political Values, Beliefs, and Ideologies*.
- Kriesi, Hanspeter, Edgar Grande, Romain Lachat, Martin Dolezal, and Simon Bornschier. 2008. *West European Politics in the Age of Globalization*. New York: Cambridge University Press.
- Kriesi, Hanspeter, Edgar Grande, Romain Lachat, Martin Dolezal, Simon Bornschier, and Timotheos Frey. 2006. "Globalization and the transformation of the national political space: Six European countries compared." *European Journal of Political Research* 45 (6): 921-956. doi:10.1111/j.1475-6765.2006.00644.x.
- Krueger, Brian S., Samuel J. Best, and Kristin Johnson. 2020. "Assessing Dimensions of the Security-Liberty Trade-off in the United States." *Surveillance & Society* 18 (1): 104-120.
- Lacy, Dean. 2001. "A Theory of Nonseparable Preferences." *American Journal of Political Science* 45 (2): 239-258.
- Lambert, Ronald D., James E. Curtis, Steven D., Brown, and Barry J. Kay. 1986. "In search of left/Right Beliefs in the Canadian Electorate." *Canadian Journal of Political Science* 541-563.
- Laurer, Moritz, and Timo Seidl. 2020. "Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation." *Policy & Internet* 257- 277. <https://onlinelibrary.wiley.com/doi/10.1002/poi3.246>.
- Lavigne, Mathieu. 2022. "Misinformation." In *Elgar encyclopedia of technology and politics*, edited by Andrea Ceron, 356 . Northampton: Edward Elgar Publishing.
- Lührmann, Anna, and Bryan Rooney. 2020. "Autocratization by Decree: States of Emergency and Democratic Decline." *Comparative Politics* 53 (4): 617-649.
- Lupia, Arthur. 1994. "Shortcuts versus encyclopedias: Information and voting behavior in California insurance reform elections." *American Political Science Review* 88 (1): 63-76.
- Marks, Gary, David Attewell, Jan Rovny, and Liesbet Hooghe. 2021. "Cleavage Theory." In *Handbook on the EU Crisis*, by Marianne Riddervold, Jarle Trondal and Akasemi Newsome, 173-198. London: Palgrave.
- Marks, Gary, David Attewell, Jan Rovny, and Lisbeth Hooghe. 2017. *Dealignment Meets Cleavage Theory*. Accessed October 2018.

- Marks, Gary, Liesbet Hooghe, Moira Nelson, and Erica Edwards. 2006. "Party Competition and European Integration in the East and West: Different Structure, Same Causality." *Comparative Political Studies* 39 (2): 155-175. doi:10.1177/0010414005281932.
- Maslow, Abraham H. 1954. *Motivation and Personality*. New York City: Harper.
- Meffert, Michael F., Michael Guge, and Milton Lodge. 2018. "Good, Bad, and Ambivalent: The Consequences of Multidimensional Political Attitudes." In *Studies in Public Opinion: Attitudes, Nonattitudes, Measurement Error, and Change*, edited by Willem E. Saris and Paul M. Sniderman, 63-92. Princeton: Princeton University Press. muse.jhu.edu/book/60994.
- Meguid, Bonnie M. 2008. *Party Competition between Unequals: Strategies and Electoral Fortunes in Western Europe*. New York: Cambridge University Press.
- Milmo, Dan. 2023. "Signal app warns it will quit UK if law weakens end-to-end encryption." *The Guardian*, February 24. <https://www.theguardian.com/technology/2023/feb/24/signal-app-warns-it-will-quit-uk-if-law-weakens-end-to-end-encryption>.
- Molinaro, Dennis G., ed. 2021. *The bridge in the parks: the Five Eyes and Cold War counter-intelligence*. Toronto: University of Toronto Press.
- Moss, Sebastian. 2020. "Danish whistleblower details NSA collaboration, submarine cable spying, surveillance data center." *Data Center Dynamics*, November 18. <https://www.datacenterdynamics.com/en/news/danish-whistleblower-details-nsa-collaboration-submarine-cable-spying-surveillance-data-center/>.
- News Limited. 2016. *A controversial Pirate Party politician has been found dead in his home*. September 21. Accessed November 14, 2016. <http://www.news.com.au/world/europe/a-controversial-pirate-party-politician-has-been-found-dead-in-his-home/news-story/8c47268db4ec848e4abb117212c206fa>.
- None of Your Business. 2020. *Open Letter on "confidential" dealings in Facebook case*. May 24. Accessed May 3, 2023. <https://noyb.eu/en/open-letter>.
- Peets, Lisa, Marty Hansen, Sam Jungyun Choi, Marianna Drake, and Jiayen Ong. 2021. *European Parliament Votes in Favor of Banning the Use of Facial Recognition in Law Enforcement*. October 21. Accessed April 26, 2023. <https://www.insideprivacy.com/artificial-intelligence/european-parliament-votes-in-favor-of-banning-the-use-of-facial-recognition-in-law-enforcement/>.
- People Vs. Big Tech. 2023. *LGBTQ+ groups tell Leo Varadkar: reform the Irish Data Protection Commission*. February 22. Accessed May 3, 2023. <https://peoplevsbig.tech/lgbtq-groups-tell-leo-varadkar-reform-the-irish-data-protection-commission>.
- Petrocik, John R. 1989. "The Theory of Issue Ownership: Issues, Agendas, and Electoral Coalitions in the 1988 Elections." *American Political Science Association*. Washington, D.C.
- Popa, Sebastian Adrian, Wouter van der Brug, Sara B. Hobolt, and Hermann Schmitt. 2019. "European Election Study 2019 Voter Study." Vers. First release. *European Election Study*. MZES, University of Mannheim. November 01. Accessed November 07, 2019.
- Popkin, Samuel L. 1991. *The Reasoning Voter: Communication and Persuasion in Presidential Campaigns*. Chicago: University of Chicago Press.
- Privacy International. n.d. *The Five Eyes*. Accessed November 25, 2016. <https://www.privacyinternational.org/node/51>.
- Radden Keefe, Patrick. 2005. *Chatter: dispatches from the secret world of global eavesdropping*. New York: Random House.
- Rueda, David, and Daniel Stegmueller. 2016. "The Externalities of Inequality: Fear of Crime and Preferences for Redistribution in Western Europe." *American Journal of Political Science* 60 (2): 472-489. doi:10.1111/ajps.12212.
- Rydgren, Jens. 2018. "The Radical Right: An Introduction." In *The Oxford Handbook of the Radical Right*. Oxford: Oxford University Press.

- Schlozman, Kay Lehman, Sidney Verba, and Henry E. Brady. 2012. *The Unevenly Chorus: Unequal Political Voice and the Broken Promise of American Democracy*. Princeton: Princeton University Press.
- Schmitt, Hermann, Sebastian Adrian Popa, and Felix Devinger. 2015. "European Parliament Election Study 2014, Voter Study, SVoter Study, Supplementary Study." Vers. 1.0.0. *European Election Studies*. GESIS Data Archive, Cologne. Accessed February 12, 2017. doi:10.4232/1.5161.
- Schneier, Bruce. 2015. *Data and Goliath: the hidden battles to collect your data and control your world*. New York: W.W. Norton & Company.
- Scott, Mark, and Nicola Clark. 2015. "European Publishers Play Lobbying Role Against Google." *The New York Times*, August 28: Section B, Page 1. <https://www.nytimes.com/2015/08/29/technology/european-publishers-play-lobbying-role-against-google.html>.
- Siewert, Markus B., and Pascal D. König. 2019. "On digital front-runners and late-comers: Analyzing issue competition over digitization in German subnational elections." *European Political Science Review* (2019), 11, 11: 247-265. doi:10.1017/S1755773919000109.
- Statewatch. 2020. *Germany asks what should the EU do about encryption for law enforcement?* October 14. Accessed April 24, 2023. <https://edri.org/our-work/germany-asks-what-should-the-eu-do-about-encryption-for-law-enforcement/>.
- Stolle, Dietlind, and Elisabeth Gidengil. 2010. "What do Women Really Know? A Gendered Analysis of Varieties of Political Knowledge." *Perspectives on Politics* 8 (1): 93-109. doi:10.1017/S1537592709992684.
- Tham, Henrik. 2001. "Law and Order as a Leftist Project? The Case of Sweden." *Punishment & Society* 3 (3): 409-426. doi:10.1177/1462474501003003004.
- Theocharis, Yannis, and Jan W. Van Deth. 2018. "The continuous expansion of citizen participation: A new taxonomy." *European Political Science Review* 10 (1): 139-163. doi:10.1017/S1755773916000230.
- Tufekci, Zeynep. 2021. "Facebook, Youth and Privacy in Networked Publics." *Proceedings of the International AAAI Conference on Web and Social Media* 6 (1): 338-345. <https://ojs.aaai.org/index.php/ICWSM/article/view/14270>.
- Van der Sar, Ernesto. 2006. *Interview with Swedens Pirate Leader Rickard Falkvinge*. June 20. Accessed June 7, 2010. <https://torrentfreak.com/interview-with-swedens-pirate-leader-rickard-falkvinge/>.
- Viola, Lora Anne, and Pawel Laidler. 2022. *Trust and transparency in an age of surveillance*. New York: Routledge.
- Welzel, Christian, and Ronald Inglehart. 2005. *Modernization, Cultural Change, and Democracy: The Human Development Sequence*. Cambridge, UK: Cambridge University Press.
- Zaller, John R. 1992. *The Nature and Origins of Mass Opinion*. Cambridge: Cambridge University Press.
- Ziller, Conrad, and Marc Helbling. 2020. "Public Support for State Surveillance." *European Journal of Political Research*.

Appendix

Variable	Original mean, sd, range, % not missing	Standardized mean, sd, range, % not missing	Government feelings		
DV privacy to security score	Mean 5.2, sd 3.03, range: 0.0 - 10.0, 94%	Mean 0.00, sd 0.50, range: -0.85 - 0.80, 94%	Approve	39%	39%
Age	Mean 49, sd 17, range: 16 - 99, 100%	Mean 0.00, sd 0.50, range: -0.94 - 1.43, 100%	Disapprove	61%	61%
Education			Political interest		Categories standardized
High	41%	41%	0	17%	-0.79417145
Medium	39%	39%	1	30%	-0.265449036
Low	11%	11%	2	38%	0.263273379
Unknown	8.50%	8.50%	3	15%	0.791995793
Gender			Voted		
Female	53%	53%	LibDem	8.90%	8.90%
Male	47%	47%	Other	36%	36%
Media	Mean 2.78, sd 1.39, range: 0.00 - 5.00, 99%	Mean 0.00, sd 0.50, range: -1.00 - 0.80, 99%	Other (Refused System missing Unlisted party)	36%	36%
Class			FarRight	3.90%	3.90%
Middle	50%	50%	LibDem	8.90%	8.90%
Working	42%	42%	Conservative	5.20%	5.20%
High	8.00%	8.00%	ChristianDem	16%	16%
Region			SocialDem	16%	16%
Town	40%	40%	Greens	3.50%	3.50%
Large town/city	32%	32%	Left	5.60%	5.60%
Village/Rural	28%	28%	Unaffiliated	4.90%	4.90%
Religion			National vote		
Atheist/Agnostic	26%	39%	loser	79%	79%
Catholic	39%	26%	winner	21%	21%
Orthodox	13%	12%	Trust Parliament		Categories standardized
Protestant	9.80%	13%	0	22%	-0.675441638
Other	12%	9.80%	1	28%	-0.291347839
Approve to disapprove: same-sex marriage	Mean 5.0, sd 4.0, range: 0.0 - 10.0, 96%	Mean 0.00, sd 0.50, range: -0.62 - 0.62, 96%	2	11%	0.092745961
of immigration	Mean 4.5, sd 3.2, range: 0.0 - 10.0, 94%	Mean 0.00, sd 0.50, range: -0.69 - 0.87, 94%	3	32%	0.476839761
of environment over growth	Mean 6.30, sd 2.77, range: 0.00 - 10.00, 96%	Mean 0.00, sd 0.50, range: -1.14 - 0.67, 96%	4	7.20%	0.86093356

Left to right ideology score	Mean 5.1, sd 2.6, range: 0.0 - 10.0, 83%	Mean 0.00, sd 0.50, range: -0.98 - 0.93, 83%	Trust EU Parliament		Categories standardized
State intervention to market freedom score	Mean 4.8, sd 2.7, range: 0.0 - 10.0, 91%	Mean 0.00, sd 0.50, range: -0.88 - 0.96, 91%	0 1	16% 25%	-0.779581365 -0.382993493
Robin Hood	Mean 4.0, sd 3.0, range: 0.0 - 10.0, 94%	Mean 0.00, sd 0.50, range: -0.68 - 1.00, 94%	2	13%	0.013594378
EU integration	Mean 6.0, sd 3.1, range: 1.0 - 11.0, 91%	Mean 0.00, sd 0.50, range: -0.80 - 0.80, 91%	3 4	38% 7.90%	0.410182249 0.806770121

Table 15 Variable distributions

Country	Sample proportion	
Germany	4.70%	
Austria	3.70%	
Belgium	3.70%	
Bulgaria	3.80%	
Croatia	3.70%	
Cyprus	1.80%	
Czech Republic	3.80%	
Denmark	3.70%	
Estonia	3.70%	
Finland	3.70%	
France	3.70%	
Greece	3.70%	
Hungary	3.70%	
Ireland	3.70%	
Italy	3.70%	
Latvia	3.60%	
Lithuania	3.70%	
Luxembourg	1.80%	
Malta	1.80%	
Poland	3.90%	
Portugal	3.60%	
Romania	3.70%	
Slovakia	3.70%	
Slovenia	3.80%	
Spain	3.70%	
Sweden	3.80%	
The Netherlands	3.70%	
United Kingdom	4.30%	
Year		
2014	53%	53%
2019	47%	47%

Table 16 Country year sample distributions

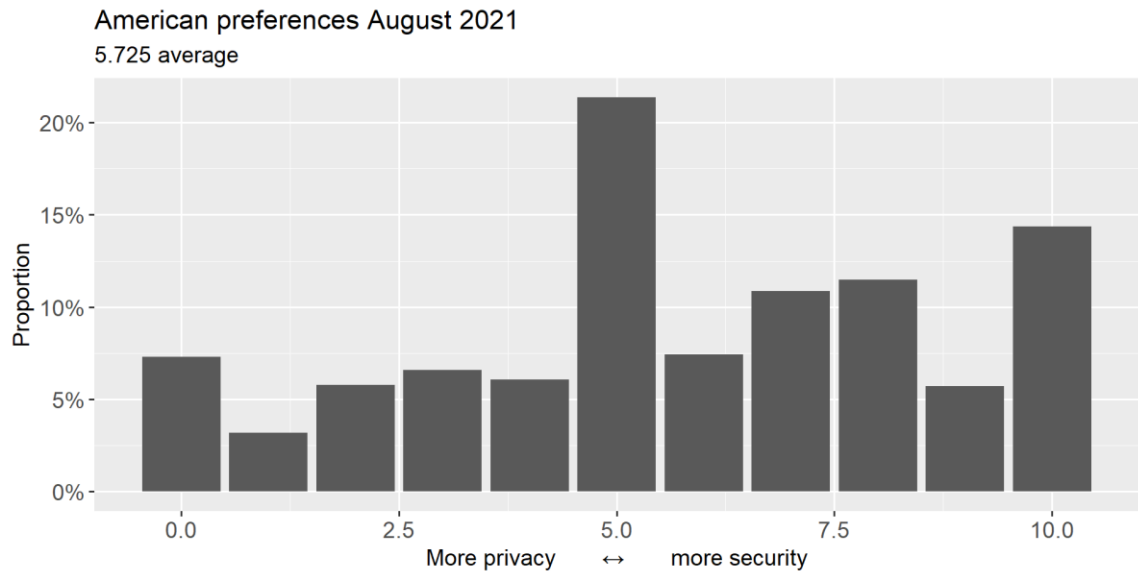


Figure 25 2021 distribution of American data ($n=1493$)

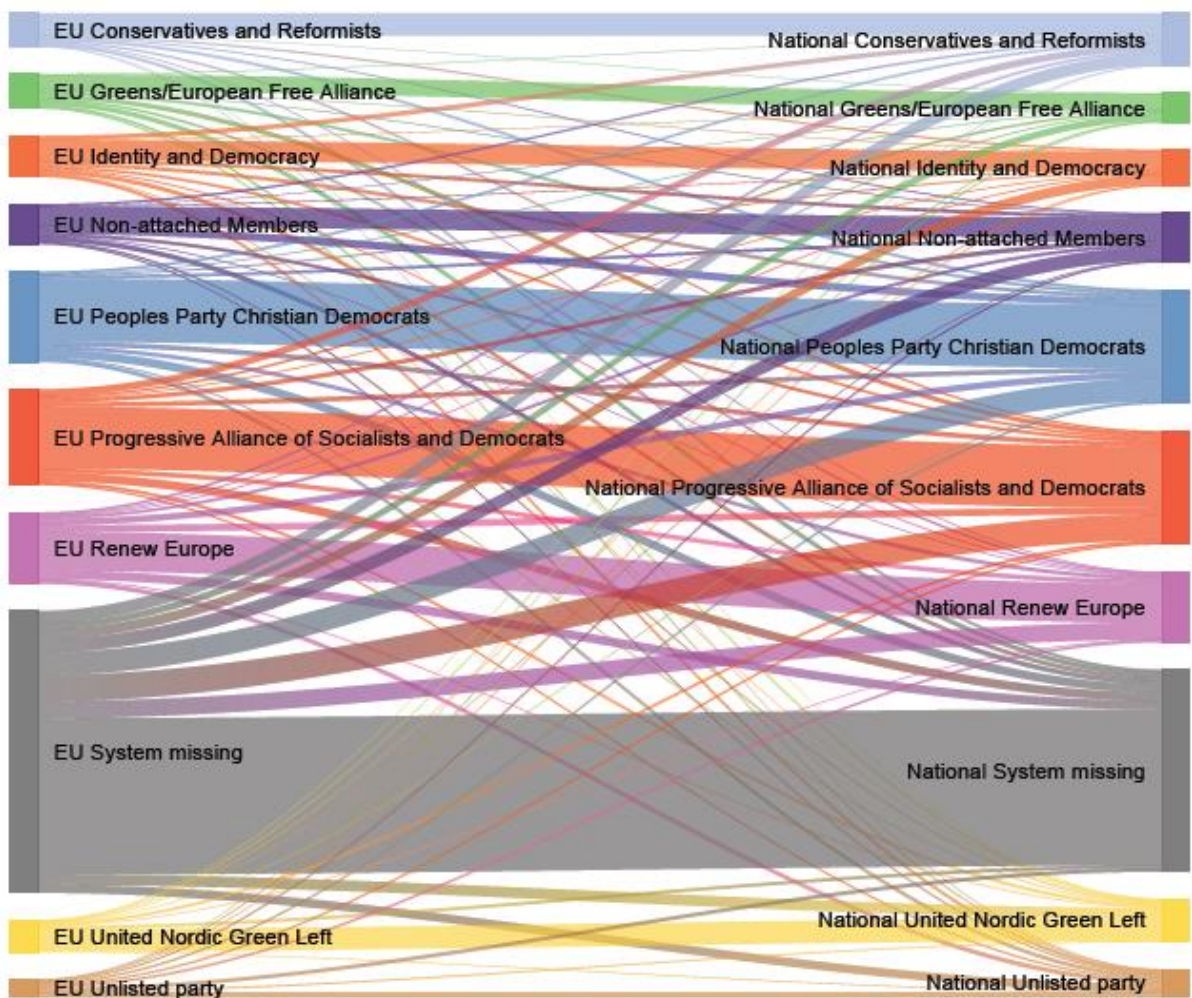


Figure 26 Vote preference National and EU party families

Dependent variable: Privacy to Security change in SD		
	Estimate	Standard error
Age	0.066***	(0.006)
Education Medium (ref High)	0.015**	(0.006)
Education Low	0.005	(0.010)
Education Undisclosed	-0.016	(0.011)
Male (ref Female)	-0.065***	(0.005)
Media	0.022***	(0.006)
Class (ref Medium) Working	0.016***	(0.006)
High	0.015*	(0.009)
Region (ref Town) Large town/city	0.002	(0.006)
Village/Rural	0.011*	(0.006)
Religion Atheist/Agnostic (ref Catholic)	-0.040***	(0.007)
Other Religion	-0.016	(0.010)
Orthodox	-0.009	(0.015)
Protestant	-0.029***	(0.011)
Approve to disapprove:		
of same-sex marriage	-0.114***	(0.006)
of immigration	-0.022***	(0.005)
of environment over econ growth	-0.117***	(0.005)
Ideology Left to Right	0.064***	(0.006)
State intervention to market freedom	0.005	(0.005)
Economic redistribution	0.054***	(0.006)
Disapprove of govt (ref Approve)	-0.017***	(0.006)
Political interest	-0.023***	(0.006)
Voter:		
Voted Far Right (ref Other)	0.01	(0.014)
Conservative	0.074***	(0.013)
ChristianDem	0.012	(0.009)
LibDem	0.011	(0.011)
SocialDem	0.016*	(0.009)
Greens	-0.004	(0.014)
Left	0.0003	(0.012)
Unaffiliated party	0.021*	(0.012)
Voter's party in power? Yes (ref No)	-0.001	(0.007)
Trust national Parliament	0.006	(0.007)
Trust EU Parliament	0.004	(0.006)
Support EU integration	0.007	(0.006)
Year 2019 (ref 2014)	-0.052***	(0.006)
Observations	34,482	
R ²	0.113	
Adjusted R ²	0.112	
Residual Std. Error	0.465 (df = 34419)	
Note:	*p<0.1; **p<0.05; ***p<0.01	

OLS models with Country Fixed Effects, continuous variables standardized to
change in 1 standard deviation

Table 17 Tradeoff OLS regression estimates

Term (1 SD if continuous)	APE Estimate	Std Error	CI low	CI high	Z- statistic	Pr ($> z $)
Age	0.009	0.004	0	0.017	2.056	0.04
Male (ref Female)	-0.019	0.004	-0.027	-0.011	-4.633	0
Media	-0.013	0.005	-0.022	-0.004	-2.866	0.004
ClassWorking	0.005	0.004	-0.004	0.013	1.072	0.284
ClassHigh	-0.01	0.008	-0.025	0.005	-1.359	0.174
Not religious (ref Yes)	-0.014	0.005	-0.024	-0.005	-2.931	0.003
Approve to disapprove:						
of samesex marriage	-0.009	0.005	-0.019	0	-1.999	0.046
of environment over growth	-0.028	0.004	-0.036	-0.021	-7.298	0
State intervention to market freedom score	-0.001	0.004	-0.008	0.007	-0.195	0.845
Economic redistribution	0.002	0.004	-0.006	0.01	0.567	0.571
Disapprove of gov't ref approve	-0.002	0.004	-0.01	0.007	-0.401	0.689
Political interest	-0.007	0.005	-0.016	0.002	-1.445	0.148
Voter:						
FarRight (ref Other)	-0.024	0.01	-0.044	-0.003	-2.281	0.023
Conservative	-0.031	0.009	-0.049	-0.012	-3.297	0.001
ChristianDem	-0.018	0.006	-0.03	-0.006	-3.009	0.003
LibDem	-0.013	0.008	-0.028	0.002	-1.668	0.095
SocialDem	-0.002	0.006	-0.014	0.01	-0.299	0.765
Greens	0.004	0.012	-0.018	0.027	0.375	0.707
Left	0.008	0.009	-0.01	0.026	0.845	0.398
Unaffiliated party	-0.007	0.009	-0.025	0.012	-0.716	0.474
Trust EU Parliament	-0.001	0.004	-0.01	0.007	-0.33	0.742
Year 2019 (reference 2014)	-0.022	0.004	-0.031	-0.014	-5.042	0

Table 18 Logit's Average Predicted Effects Estimates

ARPU from Facebook											Q4 2015 revised in 2016 filing
SEC K-10 fillings	Q4 2013	Q1 2014	Q2 2014	Q3 2014	Q4 2014	2014	Q1 2015	Q2 2015	Q3 2015	Q4 2015	
US Canada:	6.03	5.85	6.44	7.39	9	7.17	8.32	9.3	10.49	13.54	13.7
Europe:	2.61	2.44	2.84	2.87	3.45	2.9	2.99	3.36	3.47	4.5	4.56
Asia Pacific	0.95	0.93	1.08	1.18	1.27	1.115	1.18	1.29	1.39	1.59	1.6
Rest of the world:	0.84	0.7	0.86	0.85	0.94	0.8375	0.8	0.9	0.94	1.22	1.1
	2015	Q1 2016	Q2 2016	Q3 2016	Q4 2016	2016	Q1 2017	Q2 2017	Q3 2017	Q4 2017	2017
US Canada:	11.07	12.43	14.34	15.56	19.81	15.535	17.07	19.38	20.21	26.76	20.855
Europe:	3.776	3.98	4.72	4.75	5.98	4.8575	5.42	6.28	6.85	8.86	6.8525
Asia Pacific	1.41	1.56	1.77	1.89	2.07	1.8225	1.98	2.13	2.27	2.54	2.23
Rest of the world:	0.992	0.91	1.13	1.21	1.41	1.165	1.27	1.48	1.59	1.86	1.55
	Q1 2018	Q2 2018	Q3 2018	Q4 2018	2018	Q1 2019	Q2 2019	Q3 2019	Q4 2019	2019	
US Canada:	23.59	25.91	27.61	34.86	27.9925	30.12	33.27	34.55	41.41	32.646667	
Europe:	8.12	8.76	8.82	10.98	9.17	9.55	10.7	10.68	13.21	11.035	
Asia Pacific	2.46	2.62	2.67	2.96	2.6775	2.78	3.04	3.24	3.57	3.1575	
Rest of the world:	1.68	1.91	1.82	2.11	1.88	1.89	2.13	2.24	2.48	2.185	
	Q1 2020	Q2 2020	Q3 2020	Q4 2020	2020	Q1 2021	Q1 2021	Q1 2021	Q1 2021	2021	
US Canada:	34.18	36.49	39.63	53.56	40.965	48.03	53.01	52.34	60.57	53.4875	
Europe:	10.64	11.03	12.41	16.87	12.7375	15.49	17.23	16.50	19.68	16.36	
Asia Pacific	3.06	2.99	3.67	4.05	3.4425	3.94	4.16	4.3	4.89	4.3225	
Rest of the world:	1.99	1.78	2.22	2.77	2.19	2.64	3.05	3.14	3.43	3.065	

Annualized average revenue Per user								
	2014	2015	2016	2017	2018	2019	2020	2021
US Canada:	7.17	11.07	15.54	20.86	27.99	32.65	40.97	53.49
Europe:	2.90	3.78	4.86	6.85	9.17	11.04	12.74	16.36
Asia Pacific	1.12	1.41	1.82	2.23	2.68	3.16	3.44	4.32
Rest of the world:	0.84	0.99	1.17	1.55	1.88	2.19	2.19	3.07
	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	
Annual rate of change	54%	40%	34%	34%	17%	25%	31%	
	30%	29%	41%	34%	20%	15%	28%	
	26%	29%	22%	20%	18%	9%	26%	
	18%	17%	33%	21%	16%	0%	40%	

Average difference	2014	2015	2016	2017	2018	2019	2020	2021
US Canada:	baseline	baseline	baseline	baseline	baseline	baseline	baseline	baseline
Europe:	0.40	0.34	0.31	0.33	0.33	0.34	0.31	0.31
Asia Pacific	0.16	0.13	0.12	0.11	0.10	0.10	0.08	0.08
Rest of the world:	0.12	0.09	0.07	0.07	0.07	0.07	0.05	0.06
	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	
Annual rate of change in difference to US	-0.06	-0.03	0.02	0.00	0.01	-0.03	-0.01	
	-0.03	-0.01	-0.01	-0.01	0.00	-0.01	0.00	
	-0.03	-0.01	0.00	-0.01	0.00	-0.01	0.00	

Figure 27 US Securities and Exchange Commission Facebook filings on average revenue per user by region

Dissertation Conclusion

Over two decades, the world, particularly wealthy nations, has experienced massive internet adoption. People across a spectrum—from academic experts, armchair pundits, and investors to plain old Jane and Joe Schmoe—have reflected on their relationship to technology, spurred by the rapid and broad availability of this technology.

One approach to technology, dubbed technodeterministic, has utopian and pessimistic variants. The former would conclude, “The internet will liberate us!” and the latter that “The bots will subjugate us!” but both emphasize the role of technology at the cost of human agency. Around the time of Obama’s first election, and later Occupy Wall Street and the Arab Spring, the digital gap in was shrinking. As a result, online political organizing was bolstering democratic movements across regime types, and many pundits echoed a utopian version of technodeterminism. At the moment, technodeterministic pessimism runs through op-eds around the dangers of children’s access to the internet, informational overload, targeted ads, proliferating political misinformation, echo chambers, and other moral panics 2.0.

An alternative perspective sees techno-determinism as anti-humanist, regardless of whether the outcome is rosy or dreadful. Drawing from philosophy, communication, anthropologist, and technologist scholars, the Science, Technology, and Society field advocated calling internet features “affordances”. STS scholars were deliberate in their rejecting technodeterministic language. They replace causal or structuring language like “the internet lets users communicate across the world” with the idea that the internet allows users to communicate across the world. It was up to people whether to do so or not. An emphasis on agency is still vital, placing humans—not machines—at the center of whatever happens next.

Around the early 2010s, the internet went from being available in offices to white-collar elites or slow connections in shared desktop PC at home. An economic version of the technodeterministic

utopian narrative took shape too. Capitalist societies were moving on from industrialization to service economies, and, as the thinking went, their service economies were increasingly run with data. This would be the start of a “knowledge economy”. The aspirational dream *du jour* was that, as the rest of the world industrialized, the countries with formidable knowledge economies would become a place where people wouldn’t have to labor—they’d think, paint, and be creative for a living! Pirate parties, and anti-copyright left-wing political organizations, aspired to represent this growing creative class from within advanced democracies’ parliaments.

But Facebook’s cross-tracking cookies and Google’s ad tracking were already operational, even if they had not broken into mainstream consciousness. Furthermore, the political process that produced the Digital Millennium Copyright Act in the United States had prioritized lobbying from copyright holders, who had relatively more influence in the 1990s than fledgling online services. Copyright-holding media producers convinced Congress to place extensive content monitoring and removing responsibilities on these online services, which became informational gatekeepers by the end of the next decade. They envisioned an internet that replicated the media ecosystem’s view of consumers as passive recipients of content (Gillespie, 2006). The collapse of the Dot-com boom left online services looking for cheap labor to produce content; the Web 2.0 they built afforded users incentives to become free labor. The Web 2.0 paradigm seemed a rosy PR way to spin the fact that internet users were providing vast amounts of unpaid labor—producing knowledge, data, and new content to consume online (i.e., *prosumers*, see Toffler, 1980; Ritzer, Dean, & Jurgenson, 2012; Zuboff, 2019). Google, an intermediary service in terms of search, was also an intermediary in copyright enforcement (Gillespie, 2018). The company grew into its gatekeeping role, which has led to anti-trust complaints in Europe and the US.

To conform to legal and economic pressures, Google developed tools to respond to increasingly large complaints over URL removals. Internet Service Providers also faced pressures to

monitor and identify online piracy and throttle connections from specific programs, decreasing the speed of unlawful distribution. A cottage industry of web crawling and reporting services cropped up, managing complaints for copyright holders and handing them off to online and internet service providers. Their legacy lives on in the pervasive surveillance of online behavior.

In many ways, this doctoral dissertation concludes the latest turn on the spiral I started in my bachelor's. Or, to mix geometric metaphors, I find myself once again bouncing off the last angle of a triangular relationship between the state, markets, and people, torn between their roles as citizens and consumers, albeit dwindling in power on either side. In the years since I started the Ph.D., the power of markets on consumers has gone mainstream, with academics like Harvard business school professor Shoshana Zuboff coining the phrase “surveillance capitalism” (2019) and law scholar Tim Wu bringing attention to Big Data’s drive to keep us online as the “attention economy” (2016).

At a recent Georgetown event, *Cop Out: Automation in the Criminal Legal System*, the Executive Director of Just Futures Law, Paromita Shah pronounced on her surprise at finding how much of capitalism has incorporated surveillance as a means for profit (Georgetown Center on Privacy & Technology, 2023). Indeed, capitalism has so profoundly embedded surveillance we hardly notice its euphemisms. Data is the new oil, it is value-added, it is logistics, it is prediction, it is training, it is learning, and it is smart cities and widgets. Where does all this data come from? It comes from us, whether we want it or not. It comes from what we do, but it also comes from our mere existence, data, and metadata. Surveillance has become euphemized into banality. Surveillance is no longer just a government’s search and seizure as part of a more extensive targeted judicial process. It is embedded into every entity we interact with, private or public, tracking, monitoring, collecting, and analyzing where we are, who we talk to, and our transactions (Wagner, 2018). But each of these components can be atomized and discussed in isolation from tracked people’s lives. A lodestar of my dissertation was to resist this impetus. I have aimed to measure people’s attitudes toward a surveillance complex

that captures the holistic fluidity of their data (Bauman & Lyon, 2012), produced by shared data-maximizing interests of governments and companies, instead of siloing individuals as citizens *or* consumers.

Social media company CEOs and bipartisan administrations have told people mass online surveillance is no big deal to everyone who doesn't have something to hide (H. A. Popkin 2010, Solove 2011, Solon 2017), so why dissent? Their response to many people's privacy concerns has been, "if you don't like it, leave". But exile is not a democratic answer; it aims to dismiss dissent. It is an oppressive retort, espoused when questioning and organizing are threats to entrenched interests. In the US and Europe, the data I have analyzed shows that privacy concerns are not outliers and that people have preference diversity depending on who is surveilling and for what.

As our internet-connected devices follow us, physical interactions are "datafied", and the lines between the online world and offline become increasingly blurred. Our world is becoming digitized and merged with our computer-mediated interactions. Do we still have human agency in deciding how we use technologies? We must ask, is it really an affordance and is it really consent, when there is only one way to interact? Is our choice only to love it or leave? My research has shown a wide variation in privacy concerns within Americans and across time and space in the EU. For example, almost 89% of Americans agreed (strongly or somewhat) "I am concerned about online privacy", and 87% agreed that the government should disclose to citizens the use of their online data in investigations. But 50% also wanted the government to monitor online behavior, 67% expressed support for a policy that deputizes online services' monitoring, and 73% wanted those companies to report their findings to law enforcement. This pull between a desire to fight crime and privacy is manifest in the response variations in Europe. About 41% of respondents in 2014 refer to security even if this presents obstacles to privacy (31%), and 21% refuse to trade off one for the other, but by 2019 we see a sharp

demand increase in privacy (almost 40%), lower security preferences (37%) and fewer ambiguous respondents (18%).

The question of public opinion is not devoid of structuring factors. Our choices and beliefs about choice availability are not formed *tabula rasa*. The dissertation starts by centering the study of mass surveillance public opinion around a critical examination of the environment where these opinions occur by describing the history and logic of the surveillance complex. This dissertation reflects my assessment that we interact in a system where governments and companies try hard to normalize surveillance in countries where democratic values are supposed to be ‘the most advanced’. With that baseline, I explore and critique previous literature on the theory and empirical public opinion of surveillance attitudes. I then put forward original measurement ideas, testing their validity and discussing how they contribute to political science and interdisciplinary surveillance research and theorizing.

I flag two other overlooked issues: first, governments of advanced democracies have been unwilling to build (and thus be forced to defend politically) a parallel surveillance system operating independently from companies. Instead, they have used many ways to get at the data already captured by online services and fostered their growing capabilities. Second, mass surveillance is frequently justified in terms of policing deviance. But the role of intergroup relations on public opinion, particularly attitudes towards disliked groups, is overlooked. In the remaining part of this conclusion, I will highlight key points of my research.

In Chapter 1, **Deputation in the surveillance complex**, I produced a historical account of the political and economic incentives post-World War II that gave rise to an American governance strategy reliant on corporations. I argued that, unlike the contracts-based relationships that dominated the military-industrial complex, the surveillance complex relies on a broader set of behaviors linking the American government to surveillance-producing corporations, making the concept of deputation

more appropriate. This institutional-focused chapter deviates from the rest of the dissertation's attention to behavioral public opinion but is foundational to my concept of the surveillance complex as a phenomenon with a political economy. The chapter is thus important to my argument that governments shape the technological and informational ecosystem in which public opinions take form.

To support my argument that the American government has a more prominent role to play than the surveillance capitalism literature has allowed for, I pursued three clusters of evidence. First, I argued that the model of delegated control, where American representative democracy substituted voters' direct knowledge of sensitive and classified surveillance policies for interbranch oversight, had been disrupted by intelligence exceptionalism, allowing law and order agencies to sidestep objections on both (voters and institutional) fronts. To back this claim, I presented evidence of how multiple administrations across party lines have pursued avenues efforts that deputized companies and dismissed privacy concerns. Accompanying evidence of weakened interbranch checks and balances included the American Legislative's and Judiciary's willingness to acquiesce in the face of the administrations' expansive views of its powers. The chapter documents how they have rubber-stamped bills, retroactively immunized collaborating companies, and issued gag orders in secret court cases.

Second, I argued that the American government had played a dual role in expanding the supply of surveillance technologies available to itself via the marketplace. It has invested in surveillant technologies, leaving direct involvement to the most egregious cases of privacy violations. In these cases, it has usually imposed non-punitive fines. It has also mobilized to reduce the demand for privacy by refusing to acknowledge surveillance practices and by prosecuting whistleblowers and journalists who disclose them. Surveillance technologies have benefited from direct government investments (e.g., NSF grants, data purchases), forbearance (e.g., non-enforcement of existing privacy laws), their

deregulation, and codifying carveouts in law that tolerate data insecurity, which allows companies to become Data Goliaths and open the door for data brokers' proliferation.

Third, the US government has benefited politically and economically from deputized surveillance. Setting up its own duplicate surveillance system at a scale that reflects its current access would require extensive resource mobilization. That would make surveillance practices more evident, requiring it to justify its economic cost with an ensuing political cost. Instead, it has institutionalized obtaining and using data 'by hook or by crook'. This chapter contrasts an alternative technodeterministic explanation of contemporary online surveillance, which envisions Data Goliath companies as the main drivers of surveillance capacities and governments as passive observers or incapable of keeping up with the market's technologies. My distinctive perspective begs Political Science to contribute to the interdisciplinary field of surveillance studies. I highlight the deployment of mass surveillance as a politically self-interested choice, making the invisible hand that guides the market visible. Future Political Science research in this regard can explicitly study deregulation and forbearance of market surveillance as an avenue of generalized political profit in the shape of campaign data. For example, politicians who rely on running campaigns with data analytics obtained from market surveillance have a conflict of interest in choking off their own access to data with regulation. But the conflicts of interest between the use of data to get elected and the regulation of data once in office has, so far, not been explicitly articulated or treated as an area of study in political communications and campaigning²²⁵.

The emergence of a political economy of surveillance subfield could be one way to systematize research questions, measurements, and findings between fields of research that focus on state or

²²⁵ This is perplexing, since the biggest beneficiaries of campaign surveillance—candidates who win—end up deciding whether or not to regulate companies engaging in corporate and deputized surveillance. We end up with moments of political kabuki where Senate Judiciary Committee members like Orrin Hatch, a senator since 1974, publicly asks Facebook how it makes money.

corporate surveillance. It could also further study the politics of the surveillance complex, including deputized surveillance, the development and ownership of techniques and infrastructures, political and economic incentives, and political costs of surveillance from domestic and comparative points of view. It is my hope this dissertation plants a path forward.

Chapter 2, descriptively titled **Measuring Privacy Concerns under the Surveillance Complex**, is the first of three empirical chapters analyzing public opinion on the surveillance complex in advanced democracies, specifically the United States and European Union member states. The chapter departs from previous public opinion studies focusing on government or corporate surveillance separately. Instead, I ask a nationally representative sample of Americans about policies across the surveillance complex simultaneously, which gives us a clearer picture of where contradictions and linkages lay.

In this chapter, I introduce my operationalization of attitudes about the surveillance complex and deputized mass surveillance. I compare attitudes to general/non-attributed surveillance against when it is produced and ensconced by the government, juxtapose it to market-circumscribed surveillance, and when the government deputizes companies. Helen Nissenbaum has a rich theory around how information about data is used, by whom, and for what. This information shapes the context where expectations and norms are produced. She theorizes that contextual integrity is violated when data flows in obscurity and without people's consent. By this definition, deputized surveillance violates contextual integrity. I test her theoretical framework: are attitudes when data produced in a commercial sphere is accessible to the government different than when contextual integrity is intact? I hypothesize that people's attitudes toward deputized surveillance are substantively (and statistically) separate from their attitudes toward other forms of surveillance. To test my hypothesis, I surveyed 1,493 Americans via LUCID's online panel throughout August 2021. I asked for their agreement on implementing a range of surveillance policies.

I analyzed respondents' preferences using a data-reduction technique called Principal Components Analysis. Americans' responses produce a multi-dimensional space. This finding alone is a contribution to empirical privacy research. The few researchers who discuss multiple sources of surveillance tend to average out all sorts of practices, whether unattributed (e.g., "I am concerned about my data"), from governments, or companies, into a single index. Using Principal Components Analysis, scree plot testing, and pairwise and network correlation analyses as robustness checks, I conclude that combining or averaging out differences in opinions by surveillance sources is unjustifiable from a theoretical and empirical point of view. The state's and the market's respective surveillance policies produce two dimensions with moderate cross-"contamination". But deputized surveillance responses make a clear and distinct dimension of attitudes. This finding bolsters my more overarching contribution to privacy studies: the public perception of deputized surveillance is more than the sum of its parts.

I discuss in the chapter why Nissenbaum arrives at a normative stance that contextual privacy violations are unjust. The implication in her work is that people would (or perhaps that they should) have negative opinions of these practices. But the survey data challenges the expectation that people are uncomfortable with contextual integrity violations. The data instead gives credence to Chapter 1's argument that deputation is pursued over direct surveillance as a less costly option politically and economically. Americans are relatively more accepting of deputized surveillance practices than when the government does it directly. And they are much more accepting when companies proffer their data to the government than when they use it for commercial objectives. As I revisited above, the most accepted deputized policy for Americans is only used in Germany, which has codified strong hate speech laws, including commercial services' duty to report hateful online interactions.

Theorizing and measuring the phenomenon of privacy concerns will be better served by a deliberate impetus to be holistic but precise, with clarity in survey language. Future research should

endeavor to understand how mass surveillance data changing hands becomes more alluring to voters and thus less politically costly to governments than when governments carry out these policies directly. Are voters assuming that companies act as a check against abuses? If so, why do they trust companies to scrutinize data requests while also disliking self-interested market surveillance? Down the line, the research could also focus on hypothesis-testing to clarify what drives the cross-contamination of government and market surveillance practices, whether people's perceptions of the effectiveness of policies impact their acceptance, and how prevalent respondents think these practices are.

Chapter 3, **Who is mass online surveillance for?** builds on the empirical findings of Chapter 2, with an experimental component embedded in my survey of Americans. The title question has a double meaning: Do people assume mass surveillance is, paradoxically, targeted?, and who is demanding mass online surveillance? The chapter provides informational clarity seldom available in media and politicians' discourse of mass online, specifically deputized, surveillance. The experiment makes explicit how people exercise power over others' privacy, the effects of this collective decision-making, and the justifications used to arrive at surveillance decisions by analyzing intergroup dynamics on two deputized surveillance policies. Surveillance technology promises perfect enforcement. Surveillance policies that make disliked group members salient elicited higher acceptance. When the policy highlighted a liked group, approval decreased. Respondents who saw both, in randomized sequential order, had the opportunity to change their minds, and many of them did. But disliked groups induced a stronger acceptance of surveillance relative to disliked groups. Thus, information about privacy conflicts between disliked and liked groups did not produce a symmetrical reaction. If respondents saw disliked groups first and agreed to surveil them, they were not equally enthusiastic about rejecting surveillance for liked groups, inducing a weaker change of opinion (rejecting surveillance). If respondents saw liked groups first, their initial disagreement with mass surveillance was counteracted much more intensely when they read that disliked groups would also be surveilled.

Through my two-stage vignette experiment, I conclude that people accept mass online surveillance for liked group members, even if they prefer not to surveil them, because they are more willing to surveil disliked group members. The cumulative process I identify is vital because all governments and collaborating companies publicly justify the surveillance complex with security needs (national safety, fraud, etc.). This tradeoff produces collective complicity, handing over one's and everyone else's data, compromising privacy concerns to "go after bad guys". When both pieces of information were juxtaposed, the strength of disliked group surveillance could not be counterbalanced enough to cancel out the first preference by reminding respondents that liked groups' data was also monitored. This dynamic is present in policies that veer towards criminalization, like reporting to police when companies deem online posts to break the law and when the surveillance policy highlights the persistent way in which everyone's geolocation data is collected with no a priori reason. The cumulative effect of these spread-out preferences is a collective immobilization against the surveillance of liked groups. While I have not studied opinions on explicitly innocent others, these results would likely extend to this group. Future research should establish if this is the case.

This chapter explains one mechanism behind the demand for surveillance, particularly when linking the policy to subsequent harm involving law enforcement, compared to a surveillance policy that emphasizes ubiquity without further justification. The distinction between policies upends Gary Marx and Kerr et al.'s theoretical expectations that invisible/frictionless data collection that hides law enforcement's role produces less resistance. It challenges this assumption by highlighting how re-defining surveillance away from monitoring towards subsequent securitized harm is associated with higher public support. This chapter contributes to surveillance studies and American politics by focusing on a significant trend. Identity and group politics seem to be dominating policy-making. American privacy is undergoing a judicial and political reinterpretation, as exemplified by the abortion-reversing ruling *Dobbs v. Jackson Women's Health Organization*. Considerations over whether some

groups should not have privacy are seemly motivating its redefinition as a privilege, justifying mass surveillance under the idea that people who have done nothing wrong will have nothing to fear from the subsequent use of that data.

One person's decision not to, or inability to, secure their communications puts others' privacy at risk, creating a collective action problem where we become complicit in mass surveillance. When it comes to digital communications, when a person decides 'I have nothing to hide', they also decide those they interact with have nothing to hide. This chapter, above all others, answers the dissertation title's question: is the absence of mobilization against mass online surveillance because people are immobilized against action or petrified of others/of not surveilling others²²⁶? I suggest two avenues for understanding when and how each answer is true via policy differences and intergroup relations. Introducing a scenario where liked group members are also harmed by more surveillance (or, de facto, benefit from less surveillance) allows people to respond on behalf of in-groups without the stigma of association with out-groups. However, the experiment shows the limits of sympathetic frames. Americans seem willing to reconsider their opinion of mass surveillance and throw under the bus liked groups to surveil disliked groups.

If people do not accommodate the privacy rights of diverse liked groups to the same extent as they accommodate for surveillance of disliked groups, we end up in a situation where everyone has a reason for accepting mass surveillance despite misgivings, or at the very least, a motivation not to mobilize against it. Future research should investigate how and why policies considered 'too extreme' or too heavy-handed in one regard become acceptable and whether intergroup dynamics are present outside of the US. One explanation I advance is that acceptance increases when disliked groups are made salient, particularly if governments and popular discourse extra-judicially criminalize them. This brings me to another avenue of future research on policy variation and wording frame choices. The

²²⁶ A third option, that they are unable to live a digital life with technologies that provide privacy, is tackled in Chapter 1.

elite and media speech role is ripe for analyzing people's prior understanding of policies. We might also ask, how is the certainty that surveillance only harms criminals arrived at if we do not know who the criminals are without mass surveillance?

In Chapter 3, I reference how only Germany requires online services to monitor and report users who violate hate-speech laws to enforcement agencies. Germany has one of the most stringent and proactive hate speech regimes in Western democracies. Paradoxically, it has one of the highest citizen demands for privacy and has spearheaded the institutionalization of more robust privacy rights across the Europe Union. Surprisingly, monitoring with a duty to report was the most accepted deputized policy in the US sample, where hate speech laws are lax. This seeming contradiction complicates our understanding of institutions' supply and citizens' demand for surveillance.

In Chapter 4, **European attitudes towards privacy and security as policy tradeoffs**, I pivot from the American supply and demand for mass online surveillance to European attitudes (demand). I detail briefly the institutional European context and response to the publication of Edward Snowden's revelations that American surveillance practices have gone global, unsparing allies' and foes' communications.

The chapter uses secondary data from two European Union voter study survey waves. I analyze European Union citizens' attitudes before and after the bloc's adoption and incipient enforcement of the General Data Protection Regulation (GDPR). Before then, the question of a privacy-security tradeoff was outside the voter study's radar. The disclosures closed political debate around the subject—previously dissenting nations reversed their opposition, and passing the GDPR became a politically necessary reaction after Snowden's revelations. In Europe, the political supply of privacy as a policy gained ground against the counterargument that security requires surveillance.

This chapter's data provide further evidence that we should scrutinize Data Golliath's blanket statement, "People don't care about privacy". It also indirectly critiques the idea that the US

government's inaction is a politically natural or even savvy response to 'outlier' demand. Data constraints drive me to focus on individual correlates for the privacy-security tradeoff before/after GDPR, although I provide an exploratory country-level analysis in the chapter's Appendix. Within this period, Europeans became 1) more pro-privacy and 2) less unwilling to make the tradeoff (i.e., a diminished refusal to make the tradeoff). This data supports the idea that institutions can play a role in mobilizing privacy concerns (Europe) or demobilizing them (US).

Before the Snowden revelations, European Union politicians were divided on their support for new data protection rules, encouraged in part by President Obama's lobbying against stringent regulation that could choke trans-Atlantic data transfers. But the final GDPR vote reflected near unanimity in its support—Austria protest voted claiming some aspects were less rigorous than the 1995 directive.

What kind of voters care about privacy? Did 2014 election voters care so much about privacy they stopped caring about security? Did they send these politicians to the European Parliament with a clear mandate, or did the regulatory policy supply precede any demand increase for privacy preferences?

I tested competing theories of electoral preferences in the EU sample ($n = 52,885$) to understand voter preferences using country-year fixed effects OLS and logistic regression. Prioritizing privacy in the tradeoff correlated with three preference responses reflecting postmaterialist values²²⁷. Respondents with high political interest and those distrusting the government were statistically more likely to prefer privacy to security. Sociodemographics have the least explanatory power, but men, atheists/agnostics, and Protestants are more associated with privacy preferences than women, Catholics, and other religious groups. In contrast, people with right-wing ideology, Conservative

²²⁷ Accepting homosexual marriage, immigration support, and prioritizing the environment over economic growth.

voting preferences, and those opposing economic redistribution were associated with security preferences. Using logistic regression, I analyze responses by separating those who refused to make the tradeoff from those with any substantive preference on either side of the issue.

I included an exploratory analysis of responses averaged by country-year. Comparative European research is an expanding field (Ziller & Helbling, 2020; Friedewald, Lieshout, Rung, Ooms, & Ypma, 2014), but studies focus on a handful of countries. Developing an EU-wide theory of variation between countries is needed. Aggregating the data highlights several puzzles that should be pursued in comparative privacy research. First, no obvious or theoretically suggested explanation exists for the difference in distributions between countries. Beyond the highest preferences for privacy in the tradeoff expressed by Austrian and German populations, the average tradeoff score appears almost randomly distributed. This highlights how some of our assumptions about privacy preferences can come off as nearly anecdotal. For example, the UK has many cameras worldwide, but it ranks 17/28 according to its average (5.41, min = 4.15, max = 6.14), making it almost the median country.

I hope future comparative research will analyze whether Americans' intergroup dynamics occur in Europe, the effect of Europeans' ability to exercise their rights through GDPR protection on their preferences, and their perception of their government's capacity to enforce data security. Lastly, European regulation begets a broader question: do/can voters perceive privacy as security? If so, what policy supply and demand elements must be present? And are Americans receptive to this perspective?

In the dissertation's introduction, I argued that online mass surveillance subverted critical questions of democratic governance: dissent must be allowed in democracies. Democracy is a governance strategy to manage divergent interests and opinions. This reasoning underlies values like freedom of speech and assembly. Freedom requires privacy because people contain multitudes. Some might want to ask how we can make mass surveillance less undemocratic. I would argue that this oxymoron cannot stand—one condition bends to the other. If human agency matters, people have to

be able to exercise the right to decide who to be, how, when, where, and to whom. Autocracies demand consistent loyalty and use surveillance to check for it. Democracies cannot also use a tool that enforces perfect compliance and hope to remain a democracy.

Furthermore, democracies have not been transparent about how the surveillance complex makes us complicit in each others' surveillance. Governments and companies tell people not to worry about surveillance, and they undermine or disincentivize the development of technologies that ensure privacy. These actions place us in a digital world where surveillance of ourselves and others is unavoidable. In this informational and technologically suppressing environment, people are also told "no one (else) cares about surveillance" as a justification to avoid regulation or its enforcement. In this regard, Europe is increasingly departing from the US, but that stance is recent and conflicting goals, like monitoring hate speech, threaten a return to increased online surveillance. The quantitative data I've analyzed shows that while some people express preferences for surveillance, those who want privacy are not a small minority. Governments cannot ignore this conflict in public opinion and avoid regulating access to mass surveillance data while credibly claiming to be democratic.

Technical chapter: Sampling and Survey Wording

This chapter outlines the survey sample collection procedure and decisions on dropped respondents and presents the complete survey questionnaire, including response distribution statistics.

Sampling

Data from chapters 2 and 3 were obtained through a unique nationally representative survey of Americans that I collected via a survey. Ethics approval was obtained with Isadora Borges Monroy, listed as the Principal Investigator, under file #21-02-032, for collection between March 5, 2021, to March 4, 2022, and renewed until March 3, 2023. The survey was conducted in 2021, between August 9 and 25th, with 99% of responses collected between the 9th and the 13th. 2,390 people began the survey, but 1,845 (77.19%) finished, i.e., consented to submit the survey at the end, making their responses viable for analysis. Of these, 352 (19.07%) were dropped for failing the attention check (see question). This produces a final sample size of 1,493 respondents. Average completion time was 17 minutes (median = 11:30 minutes, 3rd quartile = 16:30 minutes).

The survey was programmed in Qualtrics and distributed through LUCID Theorem. LUCID is an American company hired as an intermediary to find and pay respondents. Its "Theorem" program is reserved for academics with a lower cost. The company promises the sample reflects a nationally representative distribution in terms of age, gender, race, education, and region; external validation exercises have found LUCID quota samples approximate nationally representative probability samples in terms of demographic characteristics and survey experiment effects (Coppock & McClellan, 2019). In the table below, I compare the final sample for this survey to the nationally representative target distribution table LUCID provided, with additional census data grouped into a three-category education variable. I find similar marginal distributions of the essential socio-demographic characteristics. Party identification leans Democrat at the cost of Independents, but Republican identification is almost equal to Gallup poll data conducted during that period.

Demographic Group	Target %	Sample %:
Age: 18-24:	13	10
Age: 25-34:	20	19
Age: 35-44:	20	19
Age: 45-64:	33	30
Age: 65-99:	14	20
Gender: Male	49	48
Gender: Female	51	52
Race: White (Non-Hispanic)	68	74
Race: Black (Non-Hispanic)	12	9
Race: Hispanic	12	6
Race: Other Ethnicity	10	11 (8% Asian + 3% Other)
Education	from CENSUS data	
Less than complete college	53	42
College	32	42
More than college	12	14
Partisan Identification	From Gallup August 2-17, 2021	
Democrat	28	38
Independent	40	30
Other	NA	<1
Republican	28	27

Table 19 Socio-demographic distributions

The external validity of samples and selection bias of people in online surveys

The question of external validity—specifically whether the causal estimates derived from an online experiment would persist in *other* settings—should be discussed compared to the alternatives available for quantitative doctoral research. This is worth addressing for several reasons. For the most part, the monetary and time costs of random-digit-dialing or in-person interviewing are usually out of reach for student-led research. Convenience samples are a more feasible alternative. In academia, they tend to be made up of fellow university students (in one's institution), but recruitment costs are also not negligible (Berinsky & Huber, 2012) or depend on professors gatekeeping access to their class' students. In a pandemic, where students were conducting all work online, offline recruitment was even less feasible than usual. It is also geographically limiting to carry out in-person recruitment with cash payouts, so external validity is constrained by physical proximity characteristics (e.g., samples made of

mostly liberal college towns). Furthermore, university convenience samples, by definition, are not nationally representative in many ways, particularly regarding age.

On the second point, the external validity of a survey of attitudes towards online surveillance being conducted online, on a platform that requires some form of respondent monitoring (linked to payment), we are likely to have a sample of people who are comfortable giving their banking information. This is likely the most sensitive distinction since all forms of REB-approved research require some form of tracking and identification of individuals for consent purposes, so concerns over identification per se plague all modes of data collection. Respondents paid but not in cash are also subject to some form of financialized identification method.

However, disclosing payment information is not unusual for most Americans. First, payment digitalization has become normalized in the US, where cross-banking services are non-existent (compared to Canada's Interac). Third-party services like Venmo have made financial surveillance default and normalized by making payment histories public²²⁸. Second, as the "privacy paradox" research has identified, people's willingness to disclose is usually inconsistent with their beliefs on privacy (Svirsky, 2019) and even more inconsistent when financial incentives are involved. According to that research, willingness to engage in paid activities like survey research is *not systematically* correlated to privacy concerns.

The one caveat is the possibility of under-sampling people who *are* more consistent with their beliefs and behaviors on privacy. This issue can be addressed in two ways. One argument is that by

²²⁸ Venmo is owned by PayPal, which was started by conservative political bankroller Peter Thiel, who was later replaced by Elon Musk, both of whom embody the libertarian "Silicon Valley Ideology" criticized by Jen Schradie as producing technologies that advance non-inclusive technologies (Schradie, 2015). Venmo's use of public disclosure of transactions notoriously led to an ongoing criminal investigation of Representative Matt Gaetz's payments to girls for sex (Franceschi-Bicchierai, 2021). Still, in its wake, reporters found many members of the Biden family had public settings, including payments made on behalf of the President (Mac, Notopoulos, Brooks, & McDonald, 2021). In 2018 the Federal Trade Commission settled with the company over privacy violation accusations, charging that "Venmo failed to disclose information to consumers about the ability to transfer funds and privacy settings; violated Gramm-Leach-Bliley Act" (US Federal Trade Commission, 2018), but its settings were allowed to remain public by default.

minimizing human interaction (face-to-face or on the phone), online surveys can enhance some sense of anonymity, even before encountering the consent form, which addresses identifiability. By splitting payment from the survey, respondents who are worried about it are freed from giving their names in the study and can provide proximal or wrong information to decrease identifiability (year of birth, misgendering). They are also free from signing, with their name, a consent form, which diminishes the effect of the data-sharing cue compared to an offline paper-based interaction (Connors, Krupnikov, & Ryan, 2019). However, self-selection into online survey platforms is the main issue. People concerned with being identified online may be less likely to fill out online surveys. But this does not mean they are more likely to participate in other forms of paid surveys (phone or paper) since these modes might also require providing financial contact information. Unless they are being paid cash in a lab setting or not paid at all, (non)respondents (i.e., the privacy concerned who are avoidant of surveys by virtue of their concerns) are likely never to be surveyed regarding any topic ²²⁹. Whether an unpaid survey design—online and offline—would attract a bigger proportion of privacy-concerned respondents is an empirical question that academics could test in a future replication study.

A second argument is that from a practical perspective, people are only genuinely identifiable when disclosing payment information to LUCID—but not to the researcher. The fact that this information is mediated by a company, which does not have access to the responses, and is never known to the researcher, produces de-identifiability. The consent form reiterates that the researcher has no way of knowing who the participants are, which should incentivize confidence in the privacy concerned with engaging in the research. Furthermore, those who are truly consistent in their concerns and behaviors are likely to employ these workarounds for other reasons in their life. In other words, people who are consistent in their privacy behavior and concerns would be the most motivated to

²²⁹ This observation regards Political Science, which echoes Economics' quantitative research practices. Other fields do not expect paid research, particularly in domains that favor qualitative methods, like ethnographies or interviews; or fields where deception of the study's topic is acceptable, like Psychology (Druckman, et al. 2011, 7-9)

find alternatives to being online anonymously in their day-to-day internet use (VPN use, etc.), which might reduce worries about becoming identified by LUCID for payment as a less big deal.

Once the hurdle of giving financial transfer data to an online survey company is overcome, contact with REB disclosure of data protection should lead those who are privacy concerned to remain in the survey compared to corporate studies with no data protection assurances. There is debate about whether people even read, let alone pay attention to, consent forms (Berinsky, Margolis, & Sances, 2016). However, an REB transparency study of de-identified data use's effect on survey responses found that people paid attention to consent forms and that higher transparency in how data is used increased response reliability (Connors, Krupnikov, & Ryan, 2019).

What about people who are privacy concerned and are unwilling to participate in online surveys *because* of this concern? By the very nature of how we define this group, we are making it impossible to reach these people. They likely consider that surveillance is never acceptable, though this is an assumption. They may also just be prioritizing their privacy and be accepting of surveillance of others (especially disliked groups) if they think their personal ability to evade surveillance is what determines harmful outcomes. Also, this sample includes people who believe surveillance is never acceptable—they are not absent from participating in online surveys while holding these beliefs. One of the issues at hand, sometimes called “the privacy paradox”, is the “inconsistency”²³⁰ between beliefs and behavior that can be surveilled. The alternative would be a structural perspective: the technological environment makes it nearly impossible to live one’s life consistently. This outlook is largely ignored in economics, given the dominance of behavioral studies that dominate privacy surveys.

One methodological question warranting future research is whether those who do not fill out online surveys are systematically more likely to participate in offline surveys or are just systematically

²³⁰ Behavioral economics identifies people who state they are privacy concerned but do not avoid non-private behaviors as “paradoxical” instead of critiquing the economic environment that incentivizes no genuine alternatives with privacy, coined by Barnes (2006).

non-participant and whether differences in survey modality preferences are due to the feasibility of untraceable (cash) payments. In this dissertation, particularly for chapter 3, the specific counterfactual question is whether people who self-select from online surveys would respond *to the experiment* in systematically different ways. Concretely, would people who refuse to participate in online surveys systematically react differently to being told no group member, a liked group member, and/or a disliked group member will have their data monitored, compared to a person who does participate in an online survey? If so, my results may be the product of an under-sampling of respondents who refuse to accept surveillance in any circumstance (including the disliked condition), so the effect of disliked treatment may be biased (overestimated).

Missingness overview

Using the `nanian` R package, I analyze item-response missingness, coded as not available (NA). This is a crucial step, primarily if questions about privacy concerns produce higher rates of missing data than other questions. Figure 28 presents survey items ordered as they are displayed to the respondent. It codes a missing response as a dash and a present response as grey space to highlight absence instead of data. Because randomization rules produce high levels of NAs when people are assigned to control or one of the alternative treatments, I exclude the experiments and the 50:50 randomized market or government geolocation item from this graph. We can see that two questions, one at the beginning and one almost at the end, had more missingness. Figure 29 orders the items by descending missingness, and the variable names are easier to read. From the latter, we can clearly identify that News Source (“How do you get your news? Check all that apply:”) had the most data missingness (5.09%, 74/1493), followed by Generalized Trust (“Generally speaking, would you say that most people can be trusted or that you need to be very careful in dealing with people?”; 4.55%), and some self-censorship (2.61%) on how many additional surveys they had taken in the past 7 days.

by respondent, experiment assignments excluded

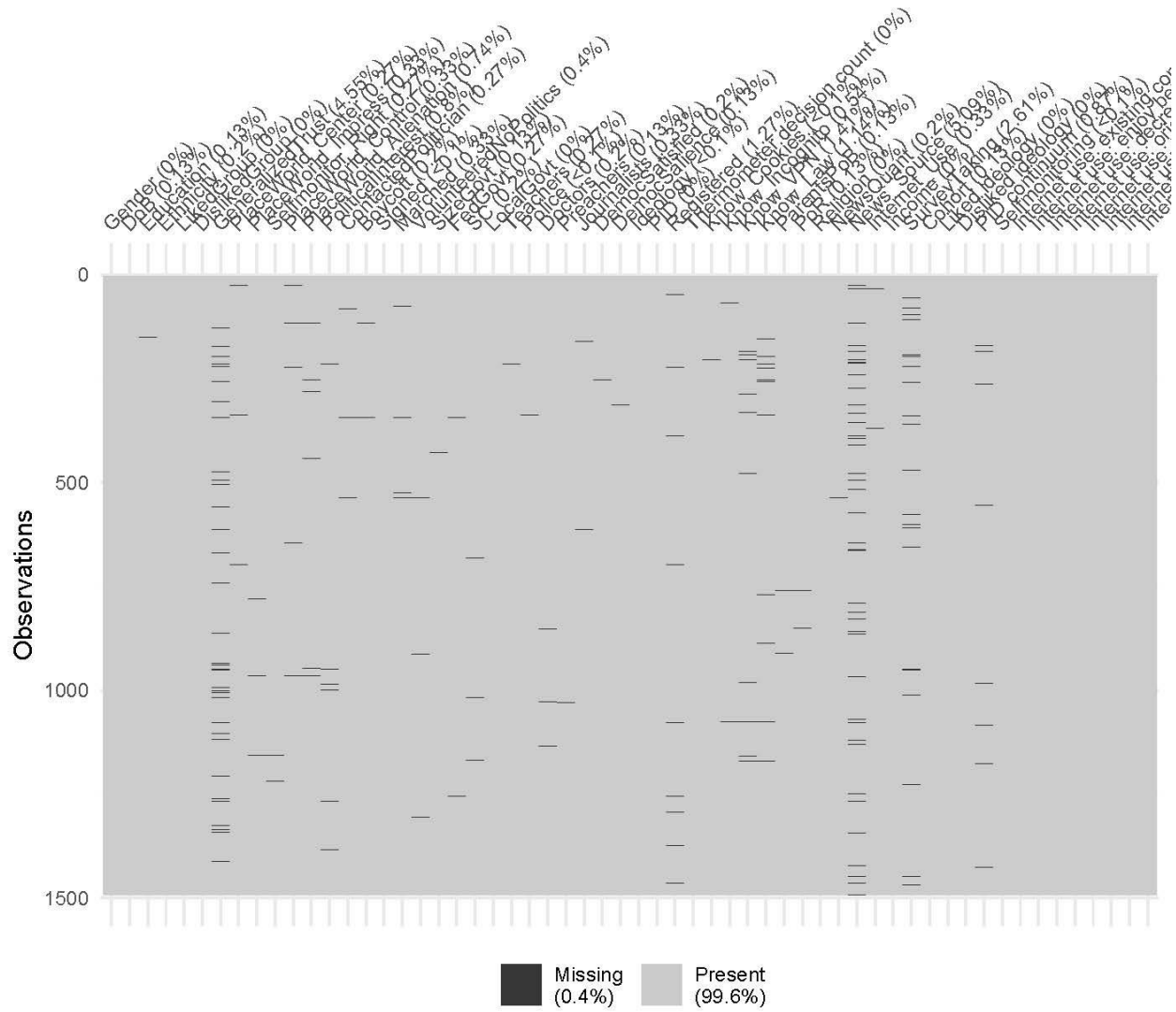


Figure 28 Response missingness, questions in order of appearance

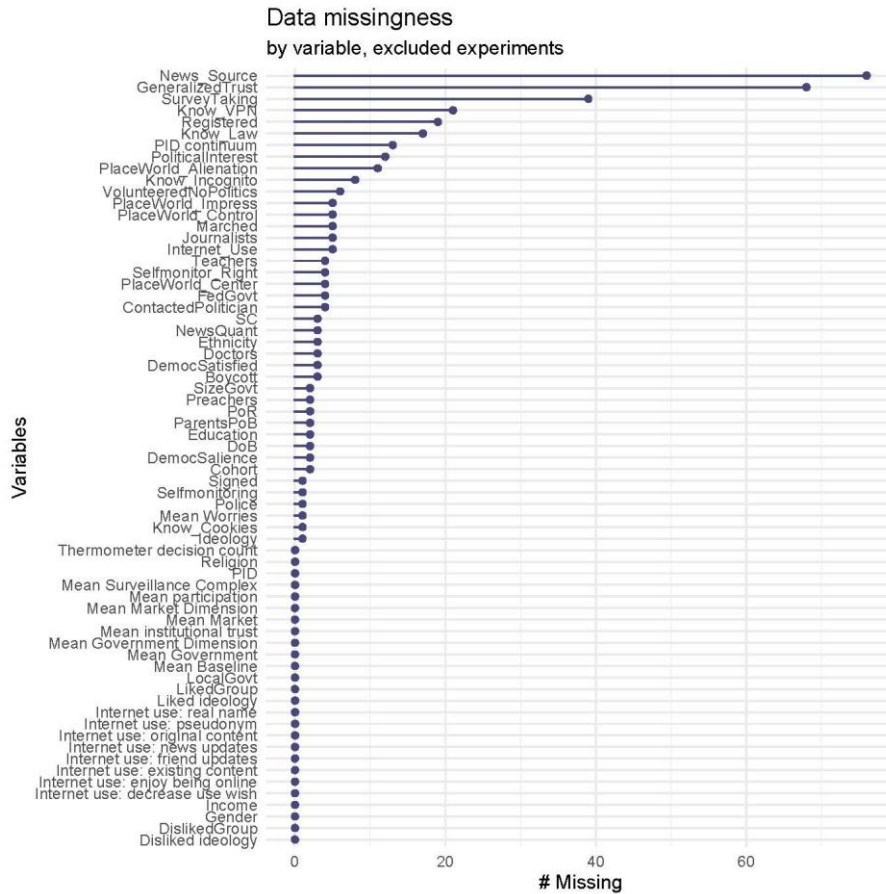


Figure 29 Response missingness, ordered by percent NA's

Reading the survey codebook

In the following pages, I reproduce the survey questionnaire, including the response options and the distribution of item responses. If the type of response is a long interval, I use summary statistics (i.e., duration of survey taking in minutes); otherwise, I detail each response's percentage. When the question order within the block is randomized,  it will appear above it.

Questionnaire wording and response distributions

Duration (in minutes)

Min.	1st Qu.	Median	Mean	3rd Qu.	Max.
2.067	7.567	11.500	17.576	16.633	1388.333

Start of Block: Consent

Thank you for considering participating in the study on how Americans view government policies that involve companies. You must be 18 years or older to participate. This study is conducted by Isadora Borges Monroy, a PhD Candidate of McGill University. The survey should take approximately 10 minutes to complete.

Your opinion is important to understanding how Americans feel. The questions about this survey are considered private and confidential. All answers are converted into numeric entries in a spreadsheet. Researchers call this a database. This database will then be analyzed and used in academic articles that will be published in scientific journals. Fully anonymized results from the survey will be shared publicly, but only in aggregate form. This study has been approved by McGill University's Research Ethics Board (REB: 21-02-032).

You can end your participation at any time by simply closing your browser and no data will be transmitted to the researcher. You may also refuse to participate in parts of the study or decline to answer any of the questions. Once submitted, we cannot remove responses since we cannot identify individuals.

Please contact Isadora Borges Monroy (isadora.borgesmonroy@mcgill.ca) with any questions/clarifications about the project or Dietlind Stolle, supervising Professor of Political Science (dietlind.stolle@mcgill.ca). If you have any ethical concerns or complaints about your participation in this study and want to speak with someone not on the research team, please contact the McGill Ethics Manager at 514-398-6831 or lynda.mcneil@mcgill.ca.

Please select "Continue to survey" if you have read the above and consent to participate in this study. You can print your own copy of this consent form by clicking on the print button. If you do not consent to participate in the study please select exit and you will be directed away from the site of this study.

Exit Continue to survey



Print this page

Consent results

- ☐ Continue to survey (2) = 1493
- ☐ Exit (1) = excluded from analysis

End of Block: Consent

Start of Block: Thanks for participating

AnonFeedbackAbandon Thank you for considering taking the survey. If you would like to convey anything to the researcher anonymously, you may do so below. If not, leave it blank. The next window will redirect you and will be the last. [If clicked on Exit]

End of Block: Thanks for participating

Start of Block: Controls and heterogeneous effects

Gender To get a representative sample, we like to know a few things about you. What is your gender?

- ☐ Male (0) 47.6%
 - ☐ Female (1) 50.7%
 - ☐ Non-binary / third gender (3) 1.7%
 - ☐ Prefer not to say (99) 0%
-

DoB What's your year of birth?

- ☐ 1920 or earlier (101)
- ☐[abridged]
- ☐ 2002 (19)
- ☐ 2003 (18)

Summary statistics:	Cohort recoding (age as of 2021)
Min in sample:1925	Gen Z 18-24: 11.9%
1st Qu.: 1959	Millennial 25-40: 30.1%
Median: 1976	Gen X 41-56: 23.0%
Mean: 1974	Boomer 57-75: 30.1%
3rd Qu.: 1989	Silent 75+: 4.8%
Max. : 2003	NA: 0.1%
NA's: 2	

Education What is the highest level of education you completed?

Education recode percent

Low 47.8%

College 38.0%

High 12.9%

DK/NA 1.2%

- ☐ No schooling (1, Low)
 - ☐ Some elementary school (unfinished) (2, Low)
 - ☐ Completed elementary school (3, Low)
 - ☐ Completed high school/GED (4, Low)
 - ☐ College degree (bachelors or technical accreditation) (5, College)
 - ☐ Master's degree (6, High)
 - ☐ Professional degree or doctorate (7, High)
 - ☐ Don't know / Prefer not to respond (99)
-



Ethnicity Which of the following comes closest to how you would describe your ethnic background?

- ☐ White (1) 71%
- ☐ Native American, including Alaska Native (2)
- ☐ Asian (3) 4%
- ☐ Black (4) 12%
- ☐ Hispanic or Latin American (5) 8%
- ☐ Middle Eastern (6)
- ☐ Native Hawaiian or other Pacific Islander (7)
- ☐ Other (8)
- ☐ Don't know / Prefer not to respond (99)

Ethnicity recoded	percent
White	70.7%
Black	11.7%
Other	9.1%
Hispanic or Latin	8.3%
NA	0.2%

End of Block: Controls and heterogeneous effects

Start of Block: Groups



LikedGroup



We will now show you a list of groups of people. Please pick the **ONE** group you would **MOST LIKE** to have as your neighbor. Even if you like more than one, please pick the group that you would **most prefer** to have as a neighbor.

- ☐ A gun-rights advocate (5)
- ☐ A climate change skeptic (8)
- ☐ A homosexual person (12)
- ☐ An immigrant (14)
- ☐ A member of the Ku Klux Klan (19)
- ☐ A member of Black Lives Matter (20)
- ☐ A feminist (21)
- ☐ An atheist (23)
- ☐ A religious fundamentalist (24)
- ☐ An anti-vaxxer (27)

Liked Group	Percent	Ideological category	
members of the Ku Klux Klan	1.3%		
anti-vaxxers	2.1%	Leftwing	61.0%
climate change skeptics	7.4%	Rightwing	39.0%
atheists	8.4%		
feminists	9.0%		
religious fundamentalists	9.4%		
immigrants	13.4%		
members of Black Lives Matter	13.9%		
homosexuals	16.2%		
gun rights advocates	18.8%		

Page Break

 DislikedGroup  We will now show you a **similar** list of groups of people. This time, please pick the **ONE** group you would **NOT LIKE** to have as your neighbor, your **LEAST** preferred group.

- ☐ A gun-rights advocate (5)
- ☐ A climate change skeptic (8)
- ☐ A homosexual person (12)
- ☐ An immigrant (14)
- ☐ A member of the Ku Klux Klan (19)
- ☐ A member of Black Lives Matter (20)
- ☐ A feminist (21)
- ☐ An atheist (23)
- ☐ A religious fundamentalist (24)
- ☐ An anti-vaxxer (27)

Disliked Group	percent	Ideological	category
immigrants	2.4%	Leftwing	31.6%
climate change skeptics	2.9%	Rightwing	68.4%
feminists	3.3%		
homosexuals	4.2%		
anti-vaxxers	4.6%		
religious fundamentalists	5.4%		
atheists	6.0%		
gun rights advocates	6.2%		
members of Black Lives Matter	15.7%		
members of the Ku Klux Klan	49.3%		

End of Block: Groups

Start of Block: Trust and politics

 GeneralizedTrust Generally speaking, would you say that most people can be trusted or that you need to be very careful in dealing with people?

☐ Most people can be trusted (1) 33.6%

☐ Need to be very careful (0) 61.9%

NA 4.6

 PlaceWorldSelfmonito Generally speaking, would you agree or disagree with the following?

	Agree (1)	Disagree (0)	NA
You are often the center of attention (Selfmonitor_Center)	☐ 26.3%	☐ 73.4%	0.3%
You try hard to impress other people (Selfmonitor_Impress)	☐ 29.4%	☐ 70.3%	0.3%
Most people you disagree with turn out to be wrong (Right)	☐ 64.5%	☐ 35.2%	0.3%
You are able to control the important things in your life (Control)	☐ 77.2%	☐ 22.5%	0.3%
You often feel like a stranger in your own country (Alienation)[R]	☐ 43.7%	☐ 55.5%	0.7%

Self-monitor Dimension summary

Min.	1st Qu.	Median	Mean	3rd Qu.	Max.
0.0	0.0	0.0	0.28	0.50	1.00

Cronbach's alpha of dimension: 0.5 [95%CI: 0.45 to 0.55]

Page Break

PoliticalInterest How much interest do you have in politics?

- ☐ None (0) 13.4%
- ☐ A little (1) 26.5%
- ☐ Some (2) 33.5%
- ☐ A lot (3) 25.9%
- NA 0.8%
-

 PoliticalPart In the last twelve months, how often have you done any of the following activities?

Min.	1st Qu.	Median	Mean	3rd Qu.	Max.				
0.00	0.00	0.60	0.71	1.20	3.00				
						Never (0)	One (1)	Two times (2)	Three or more times (3)
Contacted a politician (including over social media) (ContactedPolitician)						☐ Mean: 0.67	☐	☐	☐
Purchased or boycotted a product for political reasons (Boycott)						☐ Mean: 0.72	☐	☐	☐
Signed a petition (online or in-person) (Signed)						☐	☐ Mean: 1.09	☐	☐
Participated in a demonstration, march or rally (in person only) (Marched)						☐ Mean: 0.39	☐	☐	☐
Volunteered for a community organization with no political ties (VolunteeredNoPolitics)						☐ Mean: 0.68	☐	☐	☐

Page Break

SizeGovt Some people think the government should provide fewer services, even in areas such as health and education, in order to reduce spending. Other people feel that it is important for the government to provide many more services even if it means an increase in spending. Where would you place yourself on this scale?

- ☐ Cut services to reduce spending (-1) 20.4%
- ☐ Stay as it is (0) 32.2%
- ☐ Increase services with more spending (1) 33.0%
- ☐ Haven't thought much about it (99 DK) 14.3%

Page Break



TrustInsts For each item listed, how much confidence do you have in...

	None at all (0)	A bit (1)	Some (2)	A lot (3)
The federal government (FedGovt)	☐	☐ Mean:1.29	☐	☐
The Supreme Court (SC)	☐	☐ 1.60	☐	☐
Local government (LocalGovt)	☐	☐ 1.48	☐	☐
Teachers (Teachers)	☐	☐	☐ 1.98	☐
Police (Police)	☐	☐	☐ 1.79	☐
Doctors (Doctors)	☐	☐	☐ 2.19	☐
Preachers (Preachers)	☐	☐ 1.45	☐	☐
Journalists (Journalists)	☐	☐ 1.28	☐	☐

Min. 1st Qu. Median Mean 3rd Qu. Max.
0 1.25 1.62 1.63 2.00 3.00
Cronbach's alpha: 0.81 [95%CI: 0.80 to 0.82]

Page Break

DemocSatisfied How satisfied are you with the way democracy works in the US?
[Reversed order in code]

- ☐ Not satisfied at all (0) 11%
 - ☐ Not very satisfied (1) 27%
 - ☐ Fairly satisfied (2) 44%
 - ☐ Very satisfied (3) 18%
-

DemocSalience How important is it for you to live in a country that is governed democratically? where 1 means not important at all, and 10 means extremely important

Min. 1st Qu. Median Mean 3rd Qu. Max. NA's
1.000 6.000 9.000 7.768 10.000 10.000 2

- ☐ Not at all 1 (1)
 - ☐ 2 (2)
 - ☐ 3 (3)
 - ☐ 4 (4)
 - ☐ 5 (5) 8.5%
 - ☐ 6 (6)
 - ☐ 7 (7)
 - ☐ 8 (8)
 - ☐ 9 (9)
 - ☐ Extremely 10 (10) 40%
-

Ideology In politics, people sometimes talk about liberal and conservative. Where would you place yourself on the scale below? A score of 0 means you consider yourself extremely liberal, while a score of 10 means you consider yourself to be extremely conservative.

Min. 1st Qu. Median Mean 3rd Qu. Max. NA's

0 3.75 5.00 5.23 7.25 10.00 1.00

- ☐ Extremely liberal 0 (0) 4.4%
- ☐ 1 (1) 6.6%
- ☐ 2 (2) 7.2%
- ☐ 3 (3) 6.9%
- ☐ 4 (4) 24%
- ☐ 5 (5) 6.6%
- ☐ 6 (6) 9.7%
- ☐ 7 (7) 9.6%
- ☐ 8 (8) 5.4%
- ☐ 9 (9) 12.5%
- ☐ Extremely conservative 10 (10) 7.1%

Page Break

 PID Generally speaking, do you usually think of yourself as a:

- ☐ Republican (1) 29%
- ☐ Democrat (2) 42.9%
- ☐ Independent/Other (3) 28.1%

[shown when PID choice is Democrat or Republican]

 StrengthPID How strongly do you *identify* as a
\${q://QID240/ChoiceGroup/SelectedChoices}? Do you:

- ☐ Identify strongly as a \${q://QID240/ChoiceGroup/SelectedChoices} (1) 43.3%
Strong Democrat 62.4% Strong Republican: 37.6%
- ☐ Identify moderately as a \${q://QID240/ChoiceGroup/SelectedChoices} (0) 28.7%
Weak Democrat 55.6% Weak Republican 44.4%

NA (because PID choice was not Democrat or Republican): 28.1%

[shown when selected PID Independent or Other in PID question]

 ForcedPID If you *had* to make a choice between one of the two major parties, which
would be *less objectionable* to you?

- ☐ Democrat (5) 13.6%
- ☐ Republican (14) 13.6%
- NA (because PID choice was not forced): 72.6%

PID as a continuum: coding strong, weak
and forced as leans for combined sample:

Strong Democrat	27.0%
Moderately Democrat	15.9%
leans Democrat	13.6%
leans Republican	13.6%
Moderately Republican	12.7%
Strong Republican	16.3%
<NA>	0.9%

Registered Are you registered to vote?

☐ Yes (1) 81.8% (50 state data has 65% registration rates but that is calculated with total population including underage, this sample has 18+ only respondents)

☐ Not sure (2) 3.8%

☐ No (3) 13.1%

NO: 1.3%

End of Block: Trust and politics

Start of Block: Attention Check1

AttnCheck Some people like chocolate ice cream, and some like vanilla. Regardless of your preference, how much is 5+4?

☐ Vanilla (0)

☐ Chocolate (0)

☐ Total: (1) _____

Automated survey ending for Vanilla and Chocolate. Accepted answers in Total: "9", "W9" (accommodating for typo), "Nine", "nine" . All other responses were marked as inattentive, removed from the sample, and replaced by LUCID.

End of Block: Attention Check1

Start of Block: Study2+MktGeo



Baseline We would like to know how you feel about privacy when you are online.

	Strongly disagree (0)	Somewhat disagree (1)	Somewhat agree (2)	Strongly agree (3)
I am concerned about online privacy. (Baseline_Concerned)	3.1%	8.6%	43.0%	44.9%
Information online is used in ways people cannot predict. (Baseline_Unpredictability)	2.7%	9.2%	46.1%	41.6%
*Ultimately, people are responsible for keeping their online data private. (Baseline_Responsibility)[R]	4.3%	17.3%	50.4%	27.6%
Reports of misused online data (stolen, leaked, hacked) have been more frequent in the past 12 months. (Baseline_Misuse)	3.7%	10.9%	44.7%	40.5%
Min.		3rd		
1st Qu.		Qu.		
Median	Mean	Max.		
0.25	1.75	2	1.95	2.25
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25	1.75	2	2.27	2.67
0.25				

 Market Think about **online commercial services**, like internet providers, search engines, websites, and apps. Do you agree or disagree that they:

	Strongly disagree (0)	Somewhat disagree (1)	Somewhat agree (2)	Strongly agree (3)
Should not have a legal duty to keep the data they collect from being stolen, hacked or leaked. (Market_Safety)[R]	40.9%	16.3%	23.1%	19.4%
Should not make money from selling people's online activity data. (Market_Money)	5.1%	10.1%	25.7%	58.4%
Should take users' information to provide personalized content. (Market_Content_Change)[R]	24.8%	28.1%	33.2%	13.4%
Should keep track of what users post and delete it based on "community standards". (Market_Censor)[R]	19.9%	24.2%	37.6%	18.0%
Should not show different services and prices based on the information they collect on users. (Market_Service_Change)	8.5%	20.0%	40.7%	30.5%
 Companies should be allowed to collect location data when visiting private places. (Market_Geolocation)[R]	33.4%	28.6%	25.3%	12.7%

Min. 1st Qu. Median Mean 3rd Qu. Max.
0.1667 1.4 1.8 1.8401 2.2 3.00
Dimension summary (Safety, Content change, Censor, Geolocation)
0.00 1.00 1.667 1.648 2.25 3.00
Cronbach's alpha of dimension: 0.70 [95%CI: 0.68 to 0.73]

Page Break

Tradeoff On a scale of 0 to 10, where: **0** is you fully support privacy rights even if they hinder efforts to combat crime and **10** is you fully support restricting privacy rights in order to fight crime, where do you stand?

Min. 1st Qu. Median Mean 3rd Qu. Max. NA's
0.000 4.000 5.000 5.723 8.000 10.000 36

☐ Privacy rights 0 (0) 7.1%

☐ 1 (1) 3.1%

☐ 2 (2) 5.6%

☐ 3 (3) 6.4%

☐ 4 (4) 5.9%

☐ 5 (5) 20.8%

☐ 6 (6) 7.2%

☐ 7 (7) 10.6%

☐ 8 (8) 11.2%

☐ 9 (9) 5.6%

☐ Fight crime 10 (10) 14.0%

NA 2.5%

Min.	1st Qu.	Median	Mean	3rd Qu.	Max.	NAs
0	4	5	5.53	8	10	37

 Government Thinking about the **government**, do you agree or disagree that:

	Strongly disagree (0)	Somewhat disagree (1)	Somewhat agree (2)	Strongly agree (3)		
Federal agencies and state officials should be able to exchange data on citizens. (Government_Share)[R]	22.2%	23.7%	38.5%	15.4%		
The local police should be able to access anyone's government records without a warrant. (Government_localAccess) [R]	39.7%	25.8%	23.0%	11.2%		
The government should not have to ask a judge for access to online information about people. (Government_Warrantless)[R]	36.0%	25.8%	25.1%	13.0%		
Citizens should be notified by the government if their online data has been used in an investigation. (Government_Disclose)	3.7%	9.0%	30.9%	55.9%		
 The government should be allowed to collect location data when visiting public places. (Government_Geolocation)[R]	20.1%	30.8%	36.9%	12.3%		
Min.	1st Qu.	Median	Mean	3rd Qu.	Max.	NAs
0.00	1.00	1.50	1.544	2.00	3.00	1
Dimension summary (Share, Local access, Warrantless, Geolocation)						
0.00	1.00	1.75	1.76	2.33	3.00	
Cronbach's alpha of dimension: 0.77 [95%CI: 0.76 to 0.79]						

 Deputized Now, think about the **government and commercial online services** like internet service providers, websites and apps. Do you agree or disagree with the following policies?

	Strongly disagree (0)	Somewhat disagree (1)	Somewhat agree (2)	Strongly agree (3)
Online services should monitor people who break American laws. (Deputized_MMMonitor) [R]	11.4%	21.5%	43.2%	23.4%
Online services should report people who break laws to the government. (Deputized_MReport) [R]	10.6%	16.5%	44.5%	27.6%
The government should monitor online behavior such as social media posts. (Deputized_GMonitor) [R]	23.0%	26.4%	34.0%	16.1%
The government should be able to track location data from online services. (Deputized_GLocation) [R]	21.7%	28.9%	34.7%	14.1%

Min. 1st Qu. Median Mean 3rd Qu. Max.
 0.00 1.25 1.75 1.63 2.00 3.00
 Cronbach's alpha: 0.80 [95%CI: 0.78 to 0.81]

WorriesExperiences Think about your online searches, websites you visit, apps you use, or posts you make. In the past year, how frequently has the following happened while engaging in these activities?

Min. 1st Qu. Median Mean 3rd Qu. Max. NA's
0.0000 0.3333 0.8333 0.9422 1.5000 3.0000 1

Cronbach's alpha 0.88 [95% CI 0.87, 0.89]

	Never (0)	Rarely (1)	Sometimes (2)	Frequently (3)
I worry strangers might harass me (Worries_1Experiences_Strangers)	27.6%	27.6%	32.0%	12.3%
I worry that people who know me might ridicule me (Worries_2Experiences_ridicule)	37.0%	27.4%	25.3%	9.8%
I worry about getting in trouble at work or school (WorriesExperiences_3Work)	49.3%	21.8%	20.1%	8.6%
I worry about getting into trouble with the law (WorriesExperiences_4Law)	52.5%	21.2%	17.3%	8.6%
I have been the target of threats or intimidation online (WorriesExperiences_5Intimidated)	57.3%	17.9%	16.6%	7.8%
My information has been posted online against my wishes (WorriesExperiences_6Nonconsent)	52.0%	20.1%	18.8%	8.4%

End of Block: Study2+MktGeo

Start of Block: Study2+GovGeo

End of Block: Study2+GovGeo

STUDY 5

Affect randomization distributions					
Vignette 1	n	percent	Vignette 1 AND Vignette 2		
Liked	483	32.4%		Liked	Disliked
Disliked	503	33.7%	Liked	0	483 (32.35%)
Control	507	34.0%	Disliked	503 (33.69%)	0
Vignette 2	n	percent	Control	254 (17.01%)	253 (16.95%)
Liked	757	50.70%	Geolocate policy = 747 (50.03%) Report policy = 746 (49.97%)		
Disliked	736	49.30%			

Analysis of responses in study 3 are ordered as increasing support for surveillance (should not ... to should). However, the *directionality* shown to each respondent was randomly assigned  (Definitely should not, Probably should not, Don't care, Probably should, Definitely should OR Definitely should, Probably should, Don't care, Probably should not, Definitely should not) to minimize order effects between and within respondents and discourage straight-lining.

Study 2 battery responses are coded to reflect increased privacy concerns, as that is the substantive area of interest of the chapter. The deputized surveillance battery is reverse coded in the chapter 3 models to keep the discussion in the same direction (rejection to acceptance) as appropriate for the substantive issue of that chapter.

Start of Block: Study3 LikedXGeolocate

LikedGeolocate1 In politics, there are often winners and losers. Imagine your representative in Congress is casting a tie-breaking vote for the following policy: **The government will access anyone's location data from online services.** This policy affects \${e://Field/PositiveAffect}. How would you like them to vote?

- ☐ Definitely should not support the policy (1) 34.3%
 - ☐ Probably should not support the policy (2) 23.6%
 - ☐ Don't care (3) 14.0%
 - ☐ Probably should support the policy (4) 17.4%
 - ☐ Definitely should support the policy (5) 10.7%
-

Page Break

CounterDisIXLoc A report submitted to the committee identifies that **this law on government's access to location data from online services** would also affect

{e://Field/NegativeAffect}. How would you like your representative in Congress to cast their tie-breaking vote?

- ☐ Definitely should not support the policy (1) 17.4%
- ☐ Probably should not support the policy (2) 16.5%
- ☐ Don't care (3) 19.4%
- ☐ Probably should support the policy (4) 26.9%
- ☐ Definitely should support the policy (5) 19.8%

End of Block: Study3 LikedXGeolocate

Start of Block: Study3 LikedXReport

 LikedReport4 In politics, there are often winners and losers. Imagine your representative in Congress is casting a tie-breaking vote for the following policy: **The government requires online services to monitor and report users who violate any law to enforcement agencies.** This policy affects {e://Field/PositiveAffect}. How would you like them to vote?

- ☐ Definitely should not support the policy (1) 16.6%
- ☐ Probably should not support the policy (2) 14.9%
- ☐ Don't care (3) 21.2%
- ☐ Probably should support the policy (4) 29.5%
- ☐ Definitely should support the policy (5) 17.8%

Page Break

 CounterDislXReport A report submitted to the committee identifies that this law **requiring companies to monitor and report online violations of the law to enforcement agencies** would also affect \${e://Field/NegativeAffect}. How would you like your representative in Congress to cast their tie-breaking vote?

- ☐ Definitely should not support the policy (1) 7.1%
- ☐ Probably should not support the policy (2) 8.3%
- ☐ Don't care (3) 20.3%
- ☐ Probably should support the policy (4) 31.5%
- ☐ Definitely should support the policy (5) 32.8%

End of Block: Study3 LikedXReport

Start of Block: Study3 DislikedXGeolocate

 DislikedGeolocate1 In politics, there are often winners and losers. Imagine your representative in Congress is casting a tie-breaking vote for the following policy: **The government will access anyone's location data from online services.** This policy affects \${e://Field/NegativeAffect}. How would you like them to vote?

- ☐ Definitely should not support the policy (1) 17.9%
- ☐ Probably should not support the policy (2) 17.9%
- ☐ Don't care (3) 17.5%
- ☐ Probably should support the policy (4) 25.9%
- ☐ Definitely should support the policy (5) 20.7%

Page Break

CounterLikedXLoc A report submitted to the committee identifies that **this law on government's access to location data from online services** would also affect \${e://Field/PositiveAffect}. How would you like your representative in Congress to cast their tie-breaking vote?

- ☐ Definitely should not support the policy (1) 26.7%
- ☐ Probably should not support the policy (2) 22.7%
- ☐ Don't care (3) 16.3%
- ☐ Probably should support the policy (4) 22.7%
- ☐ Definitely should support the policy (5) 11.6%

End of Block: Study3 DislikedXGeolocate

Start of Block: Study3 DislikedXReport

DislikedReport4 In politics, there are often winners and losers. Imagine your representative in Congress is casting a tie-breaking vote for the following policy: **The government requires online services to monitor and report users who violate any law to enforcement agencies.** This policy affects \${e://Field/NegativeAffect}. How would you like them to vote?

- ☐ Definitely should not support the policy (1) 11.9%
- ☐ Probably should not support the policy (2) 10.7%
- ☐ Don't care (3) 16.3%
- ☐ Probably should support the policy (4) 30.2%
- ☐ Definitely should support the policy (5) 31.0%

Page Break

CounterLikedXReport A report submitted to the committee identifies that this law **requiring companies to monitor and report online violations of the law to enforcement agencies** would also affect $\{e://Field/PositiveAffect\}$. How would you like your representative in Congress to cast their tie-breaking vote?

- ☐ Definitely should not support the policy (1) 14.3%
- ☐ Probably should not support the policy (2) 18.7%
- ☐ Don't care (3) 17.1%
- ☐ Probably should support the policy (4) 31.5%
- ☐ Definitely should support the policy (5) 18.3%

End of Block: Study3 DislikedXReport

Start of Block: Study 5 Control Geolocate

ControlGeolocate1 In politics, there are often winners and losers. Imagine your representative in Congress is casting a tie-breaking vote for the following policy: **The government will access anyone's location data from online services.** How would you like them to vote?

- ☐ Definitely should not support the policy (1) 28.3%
- ☐ Probably should not support the policy (2) 27.6%
- ☐ Don't care (3) 16.9%
- ☐ Probably should support the policy (4) 19.7%
- ☐ Definitely should support the policy (5) 7.5%

End of Block: Study 5 Control Geolocate

Start of Block: Study3 Control Report

ControlReport4 In politics, there are often winners and losers. Imagine your representative in Congress is casting a tie-breaking vote for the following policy: **The**

government requires online services to monitor and report users who violate any law to enforcement agencies. How would you like them to vote?

- ☐ Definitely should not support the policy (1) 8.3%
- ☐ Probably should not support the policy (2) 15.4%
- ☐ Don't care (3) 20.6%
- ☐ Probably should support the policy (4) 37.9%
- ☐ Definitely should support the policy (5) 17.8%

End of Block: Study3 Control Report

Start of Block: Study3 ControlGeolocate Counterarguments

ControlGeolocXLiked A report submitted to the committee identifies that **this law on government's access to location data from online services** would also affect \${e://Field/PositiveAffect}. How would you like your representative in Congress to cast their tie-breaking vote?

- ☐ Definitely should not support the policy (1) 30.0%
- ☐ Probably should not support the policy (2) 20.0%
- ☐ Don't care (3) 19.2%
- ☐ Probably should support the policy (4) 22.3%
- ☐ Definitely should support the policy (5) 8.5%

ControlGeolocXDislik A report submitted to the committee identifies that **this law on government's access to location data from online services** would also

affect \${e://Field/NegativeAffect}. How would you like your representative in Congress to cast their tie-breaking vote?

- ☐ Definitely should not support the policy (1) 11.3%
- ☐ Probably should not support the policy (2) 22.6%
- ☐ Don't care (3) 20.2%
- ☐ Probably should support the policy (4) 34.7%
- ☐ Definitely should support the policy (5) 11.3%

End of Block: Study3 ControlGeolocate Counterarguments

Start of Block: Study3 ControlReport Counterarguments

ControlReportXLiked A report submitted to the committee identifies that **this law requiring companies to monitor and report online violations of the law to enforcement agencies** would also affect \${e://Field/PositiveAffect}. How would you like your representative in Congress to cast their tie-breaking vote?

- ☐ Definitely should not support the policy (1) 18.5%
 - ☐ Probably should not support the policy (2) 12.9%
 - ☐ Don't care (3) 21.0%
 - ☐ Probably should support the policy (4) 33.9%
 - ☐ Definitely should support the policy (5) 13.7%
-

ControlReportXDislik A report submitted to the committee identifies that this law **requiring companies to monitor and report online violations of the law to**

enforcement agencies would also affect $\{e://Field/NegativeAffect\}$. How would you like your representative in Congress to cast their tie-breaking vote?

- ☐ Definitely should not support the policy (1) 4.7%
- ☐ Probably should not support the policy (2) 14.7%
- ☐ Don't care (3) 19.4%
- ☐ Probably should support the policy (4) 35.7%
- ☐ Definitely should support the policy (5) 25.6%

End of Block: Study3 ControlReport Counterarguments

Start of Block: Knowledge

The not sure response is always at the end ; all other responses

 Know_Cookies **We would like to ask you questions about your familiarity with online tools. If you are unsure, please do not guess.**

If a website uses cookies, it means that the site:

Correct	52.9%
Not sure	22.2%
Wrong	24.9%
NA	0.1%

- ☐ Can see the content of all the files on the device you are using (0)
- ☐ Is not a risk to infect your device with a computer virus (0)
- ☐ Will automatically prompt you to update your web browser software if it is out of date (0)
- ☐ Can track your visits and activity on the site (1)
- ☐ Not sure (0)

 Know_Incognito Many web browsers offer a feature known as “private browsing” or “incognito mode.” If someone opens a website on their computer at work using incognito mode, which of the following groups will NOT be able to see their online activities?

Correct	17.5%
Not sure	34.6%

Wrong	47.3%
NA	0.5%

- ☐ The group that runs their company's internal computer network. (0)
 - ☐ Their company's internet service provider (0)
 - ☐ A coworker who uses the same computer (1)
 - ☐ The websites they visit while in private browsing mode (0)
 - ☐ Not sure (0)
-



Know_VPN A Virtual Private Network, or VPN, allows you to do the following:

Correct	28.1%
Not sure	32.2%
Wrong	38.3%
NA	1.4%

- ☐ Hide your searches from search engines like Google (0)
 - ☐ Encrypt your email so only the person receiving it can read it (0)
 - ☐ Mask your real location to websites_(1)
 - ☐ Protect you from online viruses, phishing attacks and spyware (0)
 - ☐ Not sure (0)
-



Know_Law Does the federal government have laws protecting personal information held by online companies?

Correct	27.8%
Not sure	38.8%
Wrong	32.6%
NA	1.1%

- ☐ Yes, all online personal information is legally protected (0)
- ☐ It depends, some types of personal information are legally protected (1)
- ☐ No, online personal information is not legally protected (0)
- ☐ Not sure (0)

Min.	1st Qu.	Median	Mean	3rd Qu.	Max.
0.00	0.00	0.25	0.32	0.50	1.00

Cronbach's alpha 0.42 [95% CI 0.37, 0.47]

End of Block: Knowledge

Start of Block: News and internet

Page Break

ParentsPoB Finally, we would like to know a bit more about your background. Where were your parents born?

- ☐ Both parents born in the US (1) 80.8%
- ☐ Both parents born in another country (2) 9.8%
- ☐ One parent born in the US (3) 9.2%

NA 0.1%

PoR Which of the following best describes the area you live in?

- ☐ Rural farm (1) 14.7%
 - ☐ Town (2) 15.9%
 - ☐ Suburban (3) 40.1%
 - ☐ Urban (4) 29.1%
-



Religion What is your religion, if you have one?

Not religious (stated none or none stated): 22.2%

Religious: 77.8%

- ☐ Atheist/Agnostic (0) 10.0%
- ☐ Catholic (1) 20.2%
- ☐ Protestant, non-evangelical (3) 11.3%
- ☐ Protestant, evangelical (4) 10.9%
- ☐ Other Christian (5) 17.3%
- ☐ Buddhist (6) 1.6%
- ☐ Hindu (7) 0.4%
- ☐ Jewish (8) 2.2%
- ☐ Muslim (9) 3.4%
- ☐ Don't know / Prefer not to answer (99) 12.2%
- ☐ Other (98) 10.4%

Page Break

NewsQuant During a typical week, how frequently do you watch, read, or listen to **news** on TV, radio, printed newspapers, or the Internet, not including sports?

- ☐ Never (0) 4.8%
 - ☐ Rarely (1) 20.0%
 - ☐ Three times a week (2) 18.9%
 - ☐ Often (3) 21.4%
 - ☐ Daily (4) 34.6%
 - NA 0.2%
-

News_Source How do you get your news? Check all that apply:

- ☐ Radio (1) 30.6%
- ☐ Podcasts (2) 14.6%
- ☐ Newspapers (3) 26.6%
- ☐ TV (4) 70.9%
- ☐ Independent media (not mainstream) (5) 18.9%
- ☐ Social media posts (6) 39.3%
- ☐ My neighbors (7) 8.51%
- ☐ Organizations I'm a member of (8) 4.19%

NA (None selected): 5.09%

Page Break



Internet_Use What type of behaviors and feelings best describes your internet use?
Click all that would, on average, reflect how you normally act and feel.

- ☐ I use online media to stay updated about friends (1) 43.0%
- ☐ I use online media to stay updated about news (2) 39.0%
- ☐ I follow, retweet, like or vote on existing content (4) 21.1%
- ☐ I post original content, opinions, or replies to others' content (5) 25.9%
- ☐ I enjoy being online (6) 52.8%
- ☐ I wish I could be online less frequently (7) 14.3%
- ☐ I use my real name online (9) 42.9%
- ☐ I use an alternative name, username or pseudonym online (10) 16.9%
- NA 0.3%

Page Break

Income Which bracket best describes your total household income before taxes?

- ☐ Up to \$20,000 (1) 18.0%
- ☐ Between \$20,001 and \$40,000 (2) 22.8%
- ☐ Between \$40,001 and \$70,000 (3) 22.0%
- ☐ Between \$70,001 and \$100,000 (4) 13.9%
- ☐ Between \$100,001 and \$250,000 (5) 14.6%
- ☐ More than \$250,000 (6) 1.3%
- ☐ Don't know / Prefer not to answer (99) 7.2%

Recoded Income	percent
Low (>20K)	18.0%
Middle	58.8%

High (100K+)	15.9%
DK/NA	7.2%

SurveyTaking How many online surveys have you taken in the past 7 days, without counting this one?

- ☐ 0 (1) 14.4%
- ☐ 1-5 (2) 32.5%
- ☐ 6-10 (3) 20.6%
- ☐ More than 10 (4) 32.4%

End of Block: News and internet

Start of Block: Thanksx2

AnonFeedbComplete Thank you for participating in the survey. The next window will redirect you to log your completion of the survey and will be the last. If you would like to convey anything to the researcher anonymously, you may do so below. If not, leave it empty and click the forwards arrow.

End of Block: Thanksx2
