

Digital Surveillance and the Elimination of the Human Rights Encounter

Wanshu Cong

Faculty of Law

McGill University

Montreal, 2019

A thesis submitted to McGill University in partial fulfillment of the requirements
of the degree of Doctor of Civil Law

December 2019

Abstract

Digital surveillance is increasingly used in the decision-making process in both the public and private sectors and this forms a new logic of governing. This study argues that surveillance-based governing tremendously changes the human rights encounter between individual and institution, the event in which an individual can address and resist the regulatory power of the institution. Digital surveillance, understood as a form of governing, creates conditions for perfect certainty and imposes specific order of things, while dissolving the time and space of the human rights encounter, transforming individual subjectivity and totalizing the infinity and plurality of human affairs. This study draws on Levinas' ethics and Arendt's political theory to critique the elimination of the human rights encounter by the surveillance-based governing and its all-encompassing and totalising power. It argues that the elimination of the human rights encounter amounts to the deprivation of human agency, as well as the avoidance by the powerful institution of its human rights responsibility to people subjected to its power. In addition, the study problematizes the current regulatory regimes for digital surveillance which adopt an instrumentalist approach to law and use law to tame surveillance-based governing. The study argues that legalistic management is detached from the rule of law, perpetuates the elimination of human rights encounter by surveillance-based governing, and reinforces the intrinsic power asymmetry between the surveillance institution and the individual subjected to the power of the institution. In view of the normative implications of the loss of human rights encounter, it is necessary to empower individual rights-subjects and to recast the power equilibrium between individual and surveillance institution. This study argues that an account of the rule of law which is inspired by Levinas' ethics and Arendt's political theory can provide a possibility of emancipation.

Résumé

La surveillance numérique est de plus en plus utilisée dans le processus décisionnel à la fois dans le secteur public ET le secteur privé et cela constitue une nouvelle logique de gouvernance.

La présente étude soutient que la gouvernance fondée sur la surveillance change profondément “human right encounter” entre individu et institution, une situation dans laquelle un individu peut discuter et résister au pouvoir réglementaire de l’institution. La surveillance numérique, comprise comme une forme de gouvernance, transforme la subjectivité de l’individu et réduit l’infinité et la pluralité des affaires humaines en créant des conditions de certitude parfaite et en imposant un ordre des choses. Cette étude s’inspire de l’éthique Levinassienne et de la théorie politique de Arendt pour critiquer l’élimination de « human rights encounter » par la gouvernance fondée sur la surveillance et son pouvoir universel et totalisant. Elle soutient que l’élimination du « human rights encounter » revient à la privation de l’agentivité de l’individu, ainsi qu’à l’évitement par les institutions puissantes de leurs responsabilités *vis-à-vis des droits humains des autres*. De plus, cette étude problématise les régimes réglementaires actuels pour la surveillance numérique qui adoptent une approche instrumentale de la loi et utilise la loi pour dompter la gouvernance fondée sur la surveillance. Cette étude soutient que la gestion legaliste est détachée de l’état de droit, perpétue l’élimination de « human rights encounter » par la gouvernance fondée sur la surveillance, et renforce l’asymétrie du pouvoir intrinsèque entre l’institution de surveillance et l’individu soumis au pouvoir de cette institution. Aux vues des implications normatives de la perte de « human rights encounter », il est nécessaire de donner le pouvoir à l’individu et de remanier l’équilibre des pouvoirs entre individu et institution de surveillance. Cette étude soutient qu’une approche de l’Etat de Droit qui est inspirée de l’éthique Levinassienne et de la théorie politique de Arendt peut offrir une possibilité d’émancipation.

Acknowledgements

This project could not be done without the support of so many people.

To my supervisor, Professor Frédéric Mégret. Thank you for challenging my ideas, providing valuable feedback, trusting me and giving me the freedom to explore, allowing me to be confused, and guiding me through the uncertainties in the past four years. Thank you for teaching me how to think and write as a critical legal scholar.

To my thesis committee, Professor Mark Antaki and Professor Evan Fox-Decent. Thank you for carefully reading my drafts and providing helpful comments. Thank you for kindly listening to my doubts and helping me engage with them constructively.

To McGill Law Faculty and McGill Graduate and Post-Graduate Studies. Thank you for providing the funding which allowed me to go for conferences outside Canada and for other logistic and administrative support that assured my residence in Canada and enabled me to focus on finishing my thesis.

To my dearest parents in China. Lingdi Gu and Jianping Cong. Thank you for your love.

To my friends at McGill. Nanying Tao, Tanya Monforte, Tanya Krupiy, Maria Manoli, Upasana Dasgupta, Eytan Tepper, Alex Ezenagu, Christopher Whitehead, Joan Murray, Peter Szigeti. Thank you for being my writing buddies and for exchanging drafts and ideas. Thank you for listening to my babbles.

To the IGLP community. Many of the ideas in my thesis were inspired, challenged and provoked by many wonderful people at the IGLP. Thank you.

To Shifu Shadia. Thank you for teaching me to observe and control my mind.

To Thomas. Thank you for always being there for me.

List of Abbreviations

ACLU: American Civil Liberties Union

AoM: Autonomy of Migration

CJEU: Court of Justice of the European Union

COMPAS: Correctional Offender Management Profiling for Alternative Sanctions

DHS: US Department of Homeland Security

DPD: EU Data Protection Directive

ECtHR: European Court of Human Rights

GCHQ: UK Government Communications Headquarters

GDPR: EU General Data Protection Regulation

IPT: UK Investigatory Powers Tribunal

LEDP: EU Law Enforcement Data Protection Directive

NSA: US National Security Agency

RIPA: Regulation of Investigatory Powers Act 2000 (UK), c23

SIAC: UK Special Immigration Appeals Commission

WP: Art 29 Working Party

Table of Contents

INTRODUCTION.....	1
1. MAINSTREAM PROBLEM-FRAMING ON DIGITAL SURVEILLANCE: CHALLENGES TO HUMAN RIGHTS AND THE RULE OF LAW.....	4
2. A CRITIQUE OF THE MAINSTREAM PROBLEM-FRAMING.....	6
3. AN OVERVIEW OF THE REFRAMING.....	10
4. ROADMAP.....	17
PART I. THE FRANKENSTEIN MYTH PART 1: DIGITAL SUVEILLANCE AND THE ELIMINATION OF THE HUMAN RIGHTS ENCOUNTER	22
CHAPTER 1. STATE DIGITAL SURVEILLANCE AND THE LOSS OF THE HUMAN RIGHTS ENCOUNTER.....	23
1. SCENARIOS OF STATE DIGITAL SURVEILLANCE.....	24
Scenario 1: targeted surveillance by state intelligence authorities.....	24
Scenario 2: bulk data collection by state intelligence services	25
Scenario 3: digital surveillance in law enforcement.....	29
Scenario 4: digital surveillance in the provision of public services	32
2. TRANSFORMATION OF ENCOUNTERS:.....	34
2.1 Encounters with surveillance authorities: transformation and avoidance.....	34
a. The amorphic state surveillance apparatus.....	35
b. The diffusion of the space of surveillance.....	41
c. The manipulation of the time of surveillance	43
d. The post-humanist object of surveillance.....	44
2.2 Encounters with the institutions using surveillance for decision-making.....	48
3. NO FACE-TO-FACE ENCOUNTERS HERE: IMAGERY OF SURVEILLANCE AND THE SURVEILLANCE-ENABLED ENCOUNTER	52
3.1 Panopticon and hunting.....	53
3.2 From hunting to streamlining a loop.....	57
4. SUMMARY	59
CHAPTER 2. COMMERCIAL DIGITAL SURVEILLANCE AND THE LOSS OF THE HUMAN RIGHTS ENCOUNTER.....	60
1. INTRODUCTION	60
2. THE LOGIC OF SURVEILLANCE CAPITALISM AND THE IMPOSSIBILITY OF ENCOUNTER	64
2.1 Google's story	64
2.2 Structural impediments of the human rights encounter in surveillance capitalism.....	67

2.3 The example of the data broker industry and the structural barriers of the human rights encounter	72
3. FROM CUSTOMIZED SERVICE TO CONTROL BY NUDGING	78
4. WRAPPING UP	81
PART II. THE FRANKENSTEIN MYTH PART 2: REGULATING DIGITAL SURVEILLANCE.....	83
CHAPTER 3. A SKETCH OF THE REGULATORY REGIMES FOR DIGITAL SURVEILLANCE.....	86
1. REGULATORY MECHANISMS FOR STATE DIGITAL SURVEILLANCE.....	86
1.1 Bulk digital surveillance programs.....	86
1.1.1 Problem framing.....	86
1.1.2 Problem solving.....	93
1.2 Surveillance in predictive policing and judicial decision-making process	97
1.2.1 Making the acquisition and deployment of new digital surveillance technologies under judicial and democratic scrutiny.....	98
1.2.2 Legal framework addressing the new logic of policing and administration of justice..	101
2. REGULATORY REGIMES FOR COMMERCIAL DIGITAL SURVEILLANCE	105
2.1 Problem framing.....	105
2.2 Problem solving.....	111
3. SUMMARY.....	116
CHAPTER 4. A CRITICAL ANALYSIS OF THE REGULATORY MECHANISMS: THE SECOND INSCRIPTION OF THE FRANKENSTEIN MYTH	118
1. FORMAL LEGALISM AND THE MANAGEMENT OF MULTIPLE CONFLICTING INTERESTS	119
2. INCREASED BUREAUCRATISATION LEADING TO MORE ACCOUNTABILITY LOOPHOLES	127
3. CONCLUSIONS: FROM FUTILITY TO PERVERSITY	133
INTERIM CONCLUSIONS.....	135
PART III. SURPASSING THE SCHEME OF DOUBLE INSCRIPTION: THE HUMAN RIGHTS ENCOUNTER AND THE AMBIVALENCE OF MODERN LAW	141
CHAPTER 5. THE TRANSFORMATION OF THE HUMAN RIGHTS ENCOUNTER AND MODERN LAW	142
1. THE PROTOTYPICAL HUMAN RIGHTS ENCOUNTER UNDER PASTORAL LIBERALISM.....	145
1.1 The transformation of encounter in the process of modernization and political expropriation	146
1.2 Rationalization of encounter by modern law	152
1.3 Modern law as disciplinary apparatus.....	156

2.	PASTORAL HUNTING, SURVEILLANCE AND PASTORAL LIBERALISM	160
2.1	Making a loving and distant shepherd	162
2.2	Producing a remotely knowable and manageable flock	164
3.	THE DARK SIDE OF PASTORAL LIBERALISM AND ITS AMPLIFICATION IN THE DIGITAL CONTEXT	166
3.1	The totalising and illiberal tendency of pastoral liberalism	166
3.2	The rule of law, technology's affordance and the techno-legal restraints on the dark side of pastoral liberalism	168
4.	CONCLUSION.....	173
CHAPTER 6. REVIVING THE HUMAN RIGHTS ENCOUNTER.....		177
1.	THEORETICAL UNDERPINNINGS OF THE HUMAN RIGHTS ENCOUNTER	179
1.1	Appreciating human uncertainty	179
1.1.1	Levinas	180
1.1.2	Arendt	183
1.2	From human encounter to the human rights encounter	186
1.3	Comparing the normative notion of the human rights encounter and the legally-rationalized human rights encounter.....	191
2.	THE RULE OF LAW INSPIRED BY HUMAN RIGHTS ENCOUNTER.....	194
2.1	Rule of law as a frail historical achievement.....	195
2.2	Amplifying the rule of law by the Levinasian and Arendtian human rights encounter	197
3.	NORMATIVE IMPLICATIONS OF THE LOSS OF THE HUMAN RIGHTS ENCOUNTER	200
3.1	Surveillance-based governing	201
3.2	Formal legalism	205
CONCLUDING REMARKS.....		210
BIBLIOGRAPHY		213

Introduction

In southeast of downtown Toronto, 4.9 hectares of land between East Bayfront and Port Lands are being primed for the building of a new community called Quayside. It is part of a joint project called Sidewalk Toronto established in 2017 between Waterfront Toronto (a governmental agency administering the revitalization of Toronto's waterfront), and Sidewalk Labs (owned by Google parent company, Alphabet Inc). The project is said to incorporate new digital technologies into urban design to address issues such as housing affordability, transportation and environmental pollution. To take the example of transportation, the project proposes that autonomous vehicles will be used for public transit and to replace private cars in Quayside. With a shared-ride taxibot network, the autonomous vehicle transit system will offer point-to-point service while saving space and fuel consumption. Moreover, all autonomous vehicles will yield the right of way to pedestrians which will significantly improve the safety of public spaces.¹

Sidewalk Toronto claims that Quayside will be, “the world's first neighborhood built from the internet up,”² and the approach is to build from scratch an urban community in the digital age. Other city-planning projects increasingly incorporate digital technologies to build new or replace old infrastructure. For example, in New York City, over 1700 LinkNYC kiosks are scattered around the five boroughs to replace old telephone booths and offer free services including Wi-Fi, phone calls within the US, and access to city services and maps. Each kiosk also has an environmental sensor and two security cameras (plus one more camera in its tablet which is activated by the user), to capture weather information and street images from the surrounding area.³

While the benefits of these innovative projects seem obvious - e.g., free or cheap public services, environmental protection, the creation of jobs, and the improvement of mobility and of the safety of public space - these projects have raised many questions. Is “smart city” a

¹*Project Vision* (Sidewalk Labs, 2017) at 28.

² *Ibid* at 15.

³ “Frequently Asked Questions”, online: *LinkNYC* <<https://www.link.nyc>>.

euphemism for a surveillance city? A euphemism for test bed of tech companies? A euphemism for the commodification of the personal data of residents and of the data of the public space? These questions raise many issues of data protection and data governance. Indeed, they have been addressed by both projects: Sidewalk Labs proposes a centralized, independent system called Civic Data Trust to control, manage and make accessible all de-identified data and establish rules on the use of data by all entities operating in Quayside;⁴ and LinkNYC has a long privacy policy, which explains, among other things, what and how information is collected, how long data will be stored, who the collected information will be shared with and the conditions of sharing.⁵

However, these questions have broader implications than just data protection and data governance. In the past few years, the public's excitement about smart technologies and digitally-mediated life has been considerably tampered. Dystopian depictions of life under ubiquitous digital surveillance in pop culture, as seen in *Black Mirror*,⁶ are often invoked in public and scholarly discussion about digital technologies.⁷ Moreover, in the few years between the leaks by Edward Snowden⁸ and the Cambridge Analytica scandal,⁹ public debates about digital surveillance have gradually shifted focus from the mass surveillance programs by governmental authorities such as the National Security Agency (NSA) and the Government Communications Headquarters (GCHQ) to more mundane and oft-seen as innocuous surveillance projects, mostly run by commercial entities.

In the era of counterterrorism and the immediate aftermath of the Snowden leaks, state surveillance programs carried out by surveillance and intelligence agencies which have a heightened level of secrecy are seen as posing a great threat to human rights, the principle of the rule of law and democracy. Such threats persist but, to a certain degree, have become normalized

⁴ *Sidewalk Toronto Project Update* (Sidewalk Labs, 2019) at 12.

⁵ LinkNYC, "Privacy Policy", (17 March 2017), online: *LinkNYC* <<https://www.link.nyc/privacy-policy.html>>..

⁶ It is a British sci-fi TV series of dystopian stories about new technologies in the modern world.

⁷ E.g. David Lyon, *The Culture of Surveillance: Watching as a Way of Life* (John Wiley & Sons, 2018); <https://www.cdpconferences.org/call-for-papers-re-coding-black-mirror>.

⁸ In 2013, CIA contractor Edward Snowden leaked highly classified documents to the press about the mass surveillance programs run by the NSA and the GCHQ, including PRISM, UPSTREAM, MUSCULAR and Tempura. See discussion in Part I, Section 1.1.

⁹ In 2017, it was revealed that the company Cambridge Analytica had harvested massive amount of Facebook users' data to profile US voters for the US presidential election in 2016. It was also reported that Facebook had noticed the data breach by late 2015 but did not notify its users and take measures to secure its users' data.

and fused with an even larger scale of surveillance practices. In addition, it is not just those who are from specific social backgrounds, racial groups, or are perceived as having certain criminal propensities who will be impacted by digital surveillance (although certainly, these people's rights are especially threatened due to biased profiling and predictions): Digital surveillance is becoming an inherent part of a new logic of governing and a new form of economy in public and private sectors. It could impact the lives of everyone, from being subjected to targeted commercial advertising, to being scored by insurance companies to determine insurance premiums. In terms of governing, mass collected data is processed by institutions with regulatory powers to inform their decision-making, for example, on how to distribute police resources for crime prevention. In terms of economy, people's behavioral data are collected and processed to explore competitive advantages of the market. Data itself becomes a lucrative product. The surveillance-led form of governing and economy is both embedded in and formative of people's daily experiences in the digital age. The constant penetration of people's private time and space by digital surveillance also implicates the public and political domains. This is vividly shown by the Cambridge Analytica scandal in which the misuse of the users' data of Facebook – the large-scale collection of users' data, profiling and targeted political advertising – has undermined basic democratic procedures.

This study tries to understand the challenges to human rights and the rule of law of ubiquitous digital surveillance from the perspective of the transformation and the elimination of the human rights encounter. While public resistance to digital surveillance programs often raises human rights concerns, especially related to the right to privacy and freedom of expression, this study does not ask how digital surveillance is or is not compatible with specific human rights. Instead, I am interested in how ubiquitous surveillance transforms the power structure of individual-institution relationships and individual experiences and exercises of human rights. In addition, my interest in the challenge posed to the rule of law does not primarily reside in how specific institutions of surveillance can abuse their power, but more in how surveillance, understood as forming a new way of ruling, is different from legal ordering. This study also looks at how the relationship between the two forms of ruling could inform normative critique of surveillance-based governance. In the next few pages, I will explain how this study is informed by and differs from the mainstream framing of the challenges posed by digital surveillance,

briefly sketch out a critique of the mainstream framing and explain the basic orientation of the reframing – the loss of the human rights encounter – as developed throughout this study.

1. Mainstream problem-framing on digital surveillance: challenges to human rights and the rule of law

Strong critical voices have emerged in response to the two examples of digital surveillance technologies in city-planning mentioned earlier. For example, former Ontario privacy commissioner Ann Cavoukian resigned from the Sidewalk project after learning that identifiable personal information would be shared with third-party companies.¹⁰ The sharing of identifiable data with third parties, which also means that data collected from residents are not de-identified immediately, is incompatible with the “privacy by design” framework that Sidewalk has supposedly been committed to. In relation to LinkNYC, rights-groups have raised concerns over the definition and classification of so-called “technical information”.¹¹ According to the LinkNYC privacy policy, it collects technical information from users which includes, “MAC address (anonymized), IP address, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform, device type and device identifiers”.¹² Such information can help identify and track users, but since it is not “personal identifiable information”, it can be shared with third-party companies and law enforcement authorities with fewer restrictions.¹³

The reactions of Cavourkian and New York rights-groups exemplify a common way of problem-framing. State and commercial digital surveillance are often depicted as a black box, and what makes public and judicial scrutiny unsuccessful typically presented as including national security clauses applicable to state intelligence activities, IP and trade secret laws covering technologies, data products and their uses, as well as the institutional opacity of both state surveillance agencies and private companies. The numbing effect of black box is also often

¹⁰ Sean O’Shea, “Ann Cavoukian, former Ontario privacy commissioner, resigns from Sidewalk Labs”, (21 October 2018), online: *Glob News* <<https://globalnews.ca/news/4579265/ann-cavoukian-resigns-sidewalk-labs/>>..

¹¹ E.g. Ava Kofman, “Are New York’s Free LinkNYC Internet Kiosks Tracking Your Movements?”, (8 September 2018), online: *The Intercept* <<https://theintercept.com/2018/09/08/linknyc-free-wifi-kiosks/>>.

¹² LinkNYC, *supra* note 5.

¹³ For example, court order or subpoena is needed only for sharing of personal identifiable data to law enforcement authorities. Technical information can also be shared with advertisers and advertising networks. *Ibid.*

framed in human rights language. For example, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, the UN Special Rapporteur on the right to privacy, the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association have all addressed the chilling effect of state surveillance on these fundamental freedoms, made worse by the lack of sufficient legal framework and accountability mechanisms.¹⁴

As will be explained in more detail in subsequent chapters of this study, the use of human rights language is not necessary to stop digital surveillance. It is rather deployed to formulate regulatory requirements regarding the use of digital surveillance. To a certain degree, the convergence of human rights-protection and the regulation of the practices that would undermine human rights has a well-established tradition in international human rights law. Not only does international human rights law expressly accept limitations on fundamental freedoms, it also provides criteria for restrictions to be lawfully imposed, such as the requirements of being in accordance with law, having legitimate purposes, the test of necessity and proportionality, and effective remedies.¹⁵ Hence, by satisfying these criteria, practices which interfere with fundamental rights are regulated and turned into lawful restrictions of human rights. In a similar fashion, most legal interventions addressing the human rights challenges raised by digital surveillance emphasize the demand of clearer and more accessible legal bases and procedures governing surveillance activities, more institutional and procedural transparency and more robust judicial supervision of state and commercial surveillance activities. The problem initially framed as rights-protection, hence, becomes the problem of legality, transparency and accountability of surveillance activities. By virtue of this convergence of human rights-protection and the regulation of surveillance activities, the protection of human rights also becomes reliant on the proper regulation of digital surveillance.

¹⁴ E.g. Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 23 Sess, UN Doc A/HRC/23/40 (2013); David Kaye, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 34 Sess, UN Doc A/HRC/35/22 (2017); Joseph Cannataci, *Report of the Special Rapporteur on the right to privacy*, 34 Sess, UN Doc A/HRC/35/60 (2017); Clément Nyaletsossi Voule, *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*, 68 Sess, UN Doc A/HRC/28/24 (2018).

¹⁵ E.g. UN Commission on Human Rights, *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, Commission on Human Rights, 41st Sess, UN Doc E/CN.4/1985/4, Annex (28 September 1984).

However, framing human rights challenges posed by digital surveillance into regulatory problems is helpful only to a certain extent. It is important to notice, as this study will show, that such problem-framing, emphasizing the need for a clear legal basis, transparency and accountability of surveillance institutions, has gradually become almost a knee-jerk reaction to digital surveillance in public discourses. It also has the effect of sterilizing other ways of understanding and addressing the issue of digital surveillance. What is more important is that there is a fine line between futility and perversity. When such common problem-framing leads to more and more smoke screens of formal legalism and bureaucratic rationalism for digital surveillance, it is necessary to be critical about that framing, and how what passes for an effort to solve the problem may merely make it worse. What is necessary is to uncover associated presumptions and to examine how those presumptions come into being.

2. A critique of the mainstream problem-framing

Treating human rights challenges posed by ubiquitous digital surveillance as regulatory problems means that digital surveillance as a technology is not questioned for its practical utility as such; the problem is identified as merely the existence of serious defects of formal legality and bureaucratic accountability. In the case of state and commercial data surveillance, the problem is presented as straightforward that the job of legal intervention is to provide a sufficient legal basis for data surveillance activities, to create stringent oversight mechanisms that hold the activity of data surveillance accountable, to make information about data surveillance available to the public and specific individuals, and to help individuals challenge data surveillance activities they are subjected to. These objectives are derived from basic principles of the rule of law and underpinned by natural justice values.¹⁶ At the same time, this framing is also a typically linear way of approaching the issue – linear in the sense that the problem is presented in a clear and easily understandable way for law and policy making, in a context where the framing of the problem already yields its solutions. Such a linear approach is devoted to addressing processual and institutional defects of digital surveillance, while avoiding over-complicated questions about the material conditions, substances and forms of practice of human rights in the world of fast-

¹⁶ E.g. Kate Crawford & Jason Schultz, “Big data and due process: Toward a framework to redress predictive privacy harms” (2014) 55 BCL Rev 93; Lyria Bennett Moses & Janet Chan, “Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools” 37:2 UNSW Law J 643; Danielle Keats Citron, “Technological Due Process” (2008) 85:6 Wash Univ Law Rev 1249.

evolving digital mediation. As this study will show, this linear approach often tends to channel human rights and the rule of law into formal legalism and bureaucratic rationalism, merely manages surveillance activities, and makes it more difficult for individuals to bring concrete human rights claims against surveillance practices.

Critical legal studies on human rights often seek to understand how and why law becomes part of a problem, instead of the solution.¹⁷ This study is very much motivated by that body of scholarship. But there are a variety of reasons why law becomes part of the problem in different contexts. When it comes to the issue of solving human rights problems by regulating the use of new technology in particular, one way of understanding how law becomes part of the problem is described by Kieran Tranter as the double inscription of the Frankenstein myth.¹⁸ The Frankenstein myth describes the widely shared perception that new technologies, while bringing various benefits to human society, also have the potential of causing serious harm and becoming monstrous. Public discourse about digital technologies, big data and AI have expressed this first inscription of the Frankenstein myth that reveals the dark side of digital technologies, especially as seen after the Cambridge Analytica scandal. Law is often invoked to tame the monster, to make sure that the technologies are regulated for the greater good. To *tame* the monster, not to kill the monster. This means that law is involved in a management exercise instead of announcing an outright prohibition as is evident in the case of data surveillance just mentioned.

What is interesting, then, is the second inscription of the Frankenstein myth. As law is invoked as the instrument of society to tame the monster, law itself becomes a technology, a Frankenstein creature that has the potential for both good and bad. For Tranter, this is the paradox of the technical discourse of law. If law is a technology, then we need something else to tame law as well. In the case of data surveillance, as will be discussed in detail in Part II of this study, law's potential for evil is evident in the hyperbolic legalization and increased bureaucratization of accountability mechanisms, which in fact reinforce the secrecy and power

¹⁷ E.g. David Kennedy, "International Human Rights Movement: Part of the Problem? Boundaries in the Field of Human Rights" (2002) 15 Harv Hum Rights J 101; David Kennedy, "The international human rights regime: still part of the problem?" in Rob Dickinson et al, eds, *Examining Crit Perspect Hum Rights* (Cambridge University Press, 2012) 19; Makau Mutua, "Savages, Victims, and Saviors: The Metaphor of Human Rights" (2001) 42 Harv Int Law J 201.

¹⁸ Kieran Tranter, "Nomology, Ontology, and Phenomenology of Law and Technology" (2007) 8:2 Minn J Law Sci Technol 449..

asymmetry at the core of data surveillance. This is where the fine line between futility and perversity is crossed. The technical discourse of law which re-inscribes the Frankenstein myth into law seems to explain why law is part of the problem.

As Tranter has argued, the double inscription of the Frankenstein myth in law and technology scholarship exhibits a particular positivist understanding of law; that is, law is the nomology of sovereignty.¹⁹ Just as Frankenstein comes out of the lab of Victor Frankenstein, law is created by the sovereign and is used as a tool of public policy. This is of course a very reductive view of law, as Tranter points out. But what is also reductive is the view of technology; that technology is considered ontologically separate from society, only engages with society when it causes certain consequences, and is only evaluated for its effectiveness in achieving the goal it is designed for. If we consider both technology and law as not reducible to objects of a sovereign will, but as constitutive of what and how we perceive and experience our relations with others and with the world we inhabit, we could arrive at a different account of law as technology which is socially-embedded and relational.²⁰

To give one example of the constitutive role of technology: the world map that presents the world as a homogenous surface divided by clear lines effectively constitutes the perception of political space as linearly bounded, which also influences the understanding and practice of political authority.²¹ This way of seeing the world enabled by mapping technology is appropriated by international law which has conventionally seen the linearly bounded territory as the essential constitutive element of the sovereign state, the only legitimate form of political authority that has full-fledged personality under international law. This perception of political authority reinforced by international law that emphasizes exclusive territory in turn, also prescribes the way in which new political entities should be constituted. Hence, postcolonial states have firmly accepted the legitimacy of territorial exclusivity.²² Even though sometimes

¹⁹ *Ibid* at 456–461.

²⁰ Don Ihde, *Experimental Phenomenology: Multistabilities*, 2nd ed (Albany: State University of New York Press, 2012); Peter-Paul Verbeek, *Moralizing technology: understanding and designing the morality of things* (Chicago; London: The University of Chicago Press, 2011); Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing, 2015).

²¹ Jordan Branch, “Mapping the sovereign state: Technology, authority, and systemic change” (2011) 65:1 *Int Organ* 1; Nikolas M Rajkovic, “The Visual Conquest of International Law: Brute Boundaries, the Map, and the Legacy of Cartogenesis” (2018) *Leiden J Int Law* 1.

²² See the declaration of the Organization of African Unity in 1964 meeting on border disputes among African states: “all Member States pledge themselves to respect the borders existing on their achievement of national

demarcation lines are controversial due to their colonial origins, the dispute is not about the legitimacy of territorial sovereignty per se but about drawing the correct line.²³ Here, technology is not external to the social but constitutes the social. The constitutive effect of the mapping technology is simultaneously enabling and discouraging: political authority is territorially bounded rather than radiating outward from the center of control.

Bringing the idea of technological mediation to law, a technical discourse of law, which is different from law being a sovereign's instrument, suggests law, just like technology, mediate human relations by operating an encouraging-discouraging structure. Informed by this account of law, we can also view regulatory problems differently. For example, the black-box opacity of surveillance-based governing is not just the evil of digital technologies, and not just the law's failure of reacting to and taming technologies. As Fleur Johns puts it, technolegality is inseverable.²⁴ At the very least, we can attempt to ask how the black-box problem is made possible by existing legal thought and the operation of human rights, or more precisely, what individual-institution relation is structured by human rights law that could give rise to the black-box problem of surveillance. The human rights challenge in the context of data surveillance can then perhaps be described as a joint accomplishment of digital technologies and human rights law, which both have more in common than each (or at least human rights law) allows.

In brief, this study provides a critique of the mainstream problem-framing of human rights challenges posed by digital surveillance in two ways. Using the scheme of the double inscription of the Frankenstein myth, I will show how the mainstream regulatory approach that uses law to (micro)manage the processes of digital surveillance makes law a potential monster. This suggests that the linear way of framing and solving the problem in fact becomes somewhat circular in the sense that the framing of the problem presupposes solutions which turn out to be more problems. Going beyond the double inscription scheme, I will argue that the circular mode is only overcome when law's engagement with technology is not seen as only reactive and post

independence.” Organization of African Unity “Border Disputes among African States.” Resolutions Adopted by the First Ordinary Session of the Assembly of Heads of State and Government Held in Cairo, UAR, from 17 to 21 July 1964, AHG/Res.16(I), available at https://au.int/sites/default/files/decisions/9514-1964_ahg_res_1-24_i_e.pdf.

²³ An example is the territorial dispute between China and India and the controversy over the McMahon Line.

²⁴ Fleur Johns, “Global governance through the pairing of list and algorithm” (2016) 34:1 *Environ Plan Soc Space* 126 at 130.

facto, and human rights challenges are not reducible to either human rights law or surveillance technology, but produced by their complex entanglement and mutual-conditioning.

3. An overview of the reframing

If we accept that law plays a more formative role in producing human rights challenges in the context of digital surveillance, it is possible to critique many existing notions and practices of human rights law. Not only are the practices that reduce the realization of human rights to formal legalism and bureaucratic rationality problematic, as earlier mentioned, but existing notions of human rights – the right to privacy especially – can limit the ways in which we understand the implications of digital surveillance. Persistent questions about the right to privacy, for example, include how much weight should be given to individual consent, what data should be encompassed by the right to privacy, and what kind of control should individuals have over their data, etc.

As will be discussed in Part II, there have been several important proposals in the field of data protection that aim to preserve the liberal subjectivity underlying the right to privacy. For example, informational self-determination, a central notion of European data protection laws, suggests that at issue is not just the right to be left alone, but more fundamentally individual dignity and autonomy. Privacy and data protection are seen as having intermediate value: they empowers individuals to freely develop their personalities and to participate in social and political affairs which are necessary for sustaining a democratic society.²⁵ By connecting the right to privacy to democracy, more sociopolitical and structural factors conditioning the right to privacy become visible. And indeed, one of the most important lesson from the existing scholarship on the right to privacy in the digital age is that to better protect the right to privacy, we need to seek measures that go beyond the protection of an idealized data subject and take seriously the structural disadvantage of individuals in their relationship with data-handling institutions.²⁶

²⁵ Antoinette Rouvroy & Yves Poullet, “The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy” in Serge Gutwirth et al, eds, *Reinventing Data Prot* (Dordrecht: Springer Netherlands, 2009) 45 at 45.

²⁶ E.g. Hildebrandt, *supra* note 21 at 19; Julie E Cohen, “What Privacy is For” (2013) 126 Harv Law Rev 1904; Helen Nissenbaum, “A Contextual Approach to Privacy Online” (2011) 140:4 Daedalus 32; Rikke Frank Joergensen, “The unbearable lightness of user consent” (2014) 3:4 Internet Policy Rev 1.

The insight about the structural power asymmetries between individuals and data--handling institutions informs this study. But instead of only engaging with existing notions of human rights to understand these power asymmetries, this study is motivated by a strikingly simple observation – the transformation of individual-institution encounter. This study will ask what is entailed in the phenomenon, for example, when a driver who receives a ticket for speeding has never encountered a police officer, or that a passenger boarding a train is checked by facial recognition cameras, not by train inspectors. As will be discussed in Part I, digital surveillance transforms the conditions of face-to-face human encounter (the time, the space, the subject, and the object of the encounter) to the point that the encounter is dissolved and eliminated. While certainly in the pre-digital age people did not establish all relationships through a face-to-face encounter in a literal sense, an individual-institution encounter could be experienced or recovered through legal doctrines that spliced and reconnected the time and the space,²⁷ creating a particular “chronotope”²⁸ that brought different actors together.

Many problems raised in the exercising of the right to privacy in the situation of digital surveillance can be related to this basic change of the “chronotope” of encounter – the encounter which normally enables individuals to address the surveilling parties, is constantly changing and eventually dissolved. For example, in commercial surveillance contexts, an individual’s personal information collected by one mobile application can be shared with numerous third-party companies, in the form of raw-data or data derivatives. The third-party company may process shared data with data collected from other sources for all sorts of purposes unknown to individual users and create real-life consequences. There is no encounter between an individual with those third-party companies at any moment, even if the mobile app which initially collects users’ data mentions the sharing of data with third-party companies in its privacy policy. In state surveillance contexts, individuals may not encounter state authorities at all while being subjected to restrictive measures, such as being placed on a no-fly list due to profiling measures. What people encounter are more and more devices and sensors that “datafy” their bodies, behaviors, movements and relationships and collect these data. Either covert or expressed, these are not the kind of encounter in which one can face the “other”, anticipate the other’s behaviors and adjust

²⁷ Hans Lindahl, *Fault Lines of Globalization: Legal Order and the Politics of A-legality* (Oxford, United Kingdom: Oxford University Press, 2013) at 16.

²⁸ Mariana Valverde, *Chronotopes of Law* (Routledge, 2015).

one's own behaviors,²⁹ or address the other and call the other to responsibility.³⁰ Whereas Kafka depicts the absurdity of an encounter with a crazy, self-reproducing bureaucracy, the difference that surveillance-based governing makes is that there may be no encounter in which an individual can even confront the absurdity.

Throughout this study, the transformation of the individual-institution encounter will orient the analysis and understanding of the human rights challenges in the context of ubiquitous digital surveillance. I reframe human rights challenges under ubiquitous digital surveillance as the elimination of the human rights encounter. I borrow the term “human rights encounter” from Itamar Mann. In his work on migration, he describes the encounter between sovereign states and asylum seekers in those terms.³¹ It is an encounter in which the presence of the asylum seeker projects a certain kind of moral and legal imperative that calls the state to its human rights responsibilities.³² The cases Mann examines do not happen at the actual territorial border of the state, but often in the open sea, which he describes as, “a global, ever-present state of nature”.³³ This description, with a bit of Hobbesian flavour, highlights the conflictual and antagonistic characteristics of an encounter in such a hostile space. On one side of the encounter is the *other*: the boat people fleeing from persecution, natural disaster or war in their home countries, suffering from miserable sea conditions in their voyages, starving, sun-torched, dehydrated, and abused by smugglers. They are miserable and exposed to death, and nevertheless in such extreme vulnerability they demand to be granted asylum. On the other side of the encounter is the sovereign state, the totality, the *self*, which dispatches naval vessels to intercept refugee boats and deport asylum seekers to enforce its borders and secure its totality.

But how can the extreme power imbalances make the encounter conflictual? What power do these boat people have over the state? Mann describes the moral anguish that a state agent experiences when facing the gaze of desperate boat people day after day. The gaze of these human beings carries the moral imperative not only to not kill but also to not let them die. This

²⁹ Hildebrandt, *supra* note 21 at 51–52.

³⁰ Emmanuel Levinas, *Totality and Infinity: An Essay on Exteriority*, translated by Alphonso Lingis (Pittsburgh: Duquesne University Press, 2007).

³¹ Itamar Mann, *Humanity at Sea: Maritime Migration and the Foundations of International Law* (Cambridge: Cambridge University Press, 2016).

³² *Ibid* at 12..

³³ *Ibid* at 42.

anguish is the troubling epiphany of the naked face which Levinas describes, “the resistance of what has no resistance”.³⁴ Mann sees the moral anguish as coming from a moral dilemma which boils down to making this choice: either “treating people as humans and risking changing who ‘we’ are (in terms of the composition of our population), or giving up human rights and risking changing who “we” are (in terms of our constitutive commitments)”.³⁵ The dramatic effect of the human rights encounter with extremely vulnerable asylum seekers is therefore to compel the we-community to confront, to be disturbed by and to reconsider its foundational violence.

The double effect - empowering the most vulnerable party and disturbing the sovereign subject - motivates my reframing of the human rights challenges of ubiquitous digital surveillance in this thesis. By using the term “human rights encounter”, I do not mean to straitjacket the experience of individual-institution encounter into existing, institutionalized discourses and practices of rights, but to signpost the high stakes – *i.e.* the disempowerment of individuals under ubiquitous surveillance. Indeed, as I will explain in detail in Chapter 6, a normative notion of the human rights encounter runs largely against the current institutionalized practices of human rights, practices that often reduce individuals to passive and empty vessels. At the same time, the thesis endeavors to “not throw the baby out with the bathwater.” Taking seriously the empowering and enabling aspect of human rights discourse, the notion of human rights encounter aims to reinvigorate human rights by making the experience of human encounter necessary to the conception and experience of human rights.

It would seem that the reframing of human rights challenges as the loss of the human rights encounter also implies the possibility of solutions. It would, however, be precocious to draw solutions without establishing our bearings and properly understanding what is at stake. The human encounter is a simple, everyday phenomenon of human life but it is also a particularly rich notion. I draw on Emmanuel Levinas’ ethics and Hannah Arendt’s political theory to argue that the human encounter is a fundamental existential and constitutive condition of individual and collective subjectivity. For Levinas, encountering the Other who is absolutely strange and cannot be reduced to sameness, and being called by the Other to respond, constitute the self. The Other carries the ultimate authority, commanding me not to kill, and so the self has

³⁴ Levinas, *supra* note 28 at 199.

³⁵ Mann, *supra* note 29 at 11.

infinite responsibility to preserve the alterity of the Other.³⁶ For Arendt, encounters in actions like speaking reveal people's uniqueness, actualize human plurality and weave the web of human relations.³⁷ The human encounter is full of surprises, uncertainties, insecurity and risks. But its anarchic nature is also practically the reason for having legal and political institutions to organize and orient our actions and to contain unpredictable consequences of human action - although such establishments can never really suppress the plurality and infinity of human encounters.³⁸ The human encounter is hence a basic condition for the experience and practice of individual rights and obligations and collective action.

As mentioned earlier, in this study digital surveillance is understood not as an aggregate of technical artefacts but as a form of governing. Surveillance as a form of governing goes beyond simply monitoring by collecting data on individuals and the living environment. What is crucially related to monitoring is the extraction of probabilistic knowledge from massive amounts of behavioral and environmental data, in order to inform decision-making. As a form of governing, surveillance-based decision-making is applied to various situations of the administration and distribution of resources and services that cause material consequences in people's lives. In addition, surveillance-based governing is also a disciplinary regime that constitutes and shapes people's way of behaving and living. This thesis will schematize examples of digital surveillance used in very different circumstances to describe the transformation of human rights encounters – from surveillance for national security reasons, to the profiling-based automation of judicial proceedings, to targeted commercial marketing, etc. Moreover, it does not quite matter whether it is a private entity or public authority that conducts surveillance. While state and commercial digital surveillance may have separate logics (for example, the logic of capitalism may be more specific to commercial digital surveillance by private entities),³⁹ I will speak of surveillance-based governance concerning both areas for the most part of this study to emphasize the exercise of power involved in digital surveillance and to highlight the combination of the exercise of power and technological rationality.

³⁶ Levinas, *supra* note 28 at 198; Emmanuel Lévinas, *Alterity & transcendence* (Linton: Athlone, 1999) at 24.

³⁷ Hannah Arendt, *The Human Condition* (Chicago: University of Chicago Press, 1958) at 183.

³⁸ *Ibid* at 190–191.

³⁹ Shoshana Zuboff, “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization” (2015) 30:1 J Inf Technol 75.

The surveillance-based logic of governance removes the human rights encounter and normalizes the alterity and unexpectedness of human action. And it replaces the participatory and conflictual meaning-making and subject-forming processes in the face-to-face encounter with a unilaterally imposed order of things. The processes of knowledge production and decision-making can be realized in a complete technological loop that excludes human comprehension and political deliberation.

Take the example of autonomous vehicles. Proponents argue that currently all accidents associated with self-driving cars are caused by humans and if all vehicles are self-driving and connected to one network, there will not be car accidents or traffic jams, or when two cars collide the damage can be reduced to the minimum.⁴⁰ While we can somewhat picture a world without car accidents and traffic jams, the functioning of the algorithm is certainly unfathomable. The massive collection of behavioral and environmental data to train the algorithm, the digitization of real-time situations and the translation into the languages of mathematics and informatics understood by the AI, the self-correction and adaptation of the algorithm to new data, etc., all raise serious political and legal issues that have significant implications for democracy and human rights.⁴¹ But within a technologically determinist loop, they are translated into unintelligible technical issues and framed in a discourse of technological objectivity that leaves very little room for human intervention.

It is a seductive assumption framed as determined by the technology – the more data the algorithm gets, the better decision it makes – but before accepting this assumption, it is necessary to ask how political and legal questions are (mis)translated into technological ones. The battle over Google Map’s Street View illustrates such (mis)translation. The launch of Street View in Japan and Germany was strongly resisted by the local residents who raised privacy and security concerns. Google’s solution was to blur specific images upon individual requests. However, this solution completely evaded more important questions, such as how Google could install cameras all over the city and take pictures in the first place.⁴²

⁴⁰ E.g. Jack Stewart, “It Takes a Single Autonomous Car to Prevent Phantom Traffic Jams”, *Wired* (16 May 2018), online: <<https://www.wired.com/story/one-autonomous-car-prevent-traffic-jams/>>.

⁴¹ E.g. Johns, *supra* note 22 at 138; Sheila Jasanoff, “Virtual, visible, and actionable: Data assemblages and the sightlines of justice” (2017) 4:2 *Big Data Soc* 1.

⁴² Siva Vaidhyanathan, *The Googlization of Everything: (And Why We Should Worry)* (University of California Press, 2012) at 99–111.

While the world is not yet a complete cybernetic loop, the operating logic of surveillance-based governance which removes human encounter and automates human action and decision-making, is alarming. The loss of the human rights encounter amounts to the ultimate consolidation of technocratic governance. It eliminates plurality and alterity, the very human conditions that give life and world meaning. Plurality and alterity, understood from the perspectives of Arendt and Levinas, are categorically different from the unexpected correlations of human behavioral data extracted by algorithms. What Levinas and Arendt acknowledge as the most important human condition is in fact the finiteness, partiality and fallibility of our cognition and knowledge. So, encounters with alterity and plurality make us reflect on our existing belief systems and help us change ways of seeing and acting. Such reflection and deliberation are essentially the exercise of freedom.⁴³ The potential of surveillance-based governance of extracting unforeseen patterns of data and creating its own reality is completely different from the plurality and alterity discussed by Arendt and Levinas. Its operating logic is about making human affairs and the living environment completely knowable and transparent so that human reflection and deliberation become superfluous. The elimination of plurality and alterity transforms human subjectivity and the implications cannot be grasped by any piecemeal reform of human rights or digital rights that only concerns the microlevel relationship between individual subjects and data-handling companies or state agencies.

This striking change in the basic human condition can be told in a way as entailed by the double inscription of the Frankenstein myth; that is, the loss of human rights encounters can be attributed to the technologies of digital surveillance and how they are put into practice, and then attributed to the failure of law which regulates the surveillance technologies and their use. But as discussed earlier, this linear way of problem-framing is reductive and fails to understand the social-embeddedness of both law and technology. By thinking of digital surveillance as a form of governing which removes human rights encounters, this study will consider how the existing practices and discourses of human rights law – for example the proceduralization of human rights projection and the subjectivation of individuals as passive and dependent rights-holders – have constituted the individual-institution relationship and provided conditions for removing the human rights encounter through the logic of surveillance-based governing. To see the loss of the

⁴³ Mireille Hildebrandt, “Profiling and the rule of law” (2008) 1:1 Identity Inf Soc 55 at 58.

human rights encounter as a joint accomplishment of law and surveillance technologies will help to critically assess some regulatory frameworks for digital surveillance which deal with and (re)create the situations of lost encounter.

4. Roadmap

In the first two parts of the thesis, I will describe the loss of the human rights encounter in the context of state and commercial data surveillance. The loss of the human rights encounter is treated as a phenomenon caused by the practice of surveillance technologies and the practice of law. I will use and expand on the scheme of the double inscription of the Frankenstein myth to enlighten the discussion. Part I will demonstrate the loss of the human rights encounter as a phenomenon made possible by certain practices of using digital surveillance technologies, and Part II will show how the taming of such technologies and their utilization by law perpetuate the loss of the human rights encounter.

As digital surveillance technologies have been applied to a wide range of fields, which all have various implicit and explicit implications on human subjectivity and governance,⁴⁴ I will only focus on those which have raised particular concerns for human rights in legal and political discourses. Chapter 1 of Part I focuses on the use of digital surveillance by state authorities. I choose targeted and mass surveillance programs by state intelligence services, surveillance technologies deployed in law enforcement and judicial decision-making, and surveillance technologies used for monitoring the provision of social benefits. I will use these examples to demonstrate how the existential conditions of the human rights encounter – an event that unites two parties in a particular time and space – are transformed radically and become increasingly unintelligible. I will also use terms as metaphors, such as “hunting,” “streamline” and “nudge,” to help think about the conditions which making avoiding human rights encounters possible.

Chapter 2 discusses commercial data surveillance. I will describe how data-dealing companies operate within the logic of what Shoshana Zuboff calls, “surveillance capitalism”, to datafy and digitize user behaviors and living environment to make enormous profits. The loss of the human rights encounter is manifested by the fact that many of these data-dealing companies

⁴⁴ See Lyria B Moses, Fleur Johns & Daniel Joyce, “Data associations in global law and policy” (2018) 5:1 Big Data Soc 1.

– notably data broker companies – are not consumer-facing at all, while their commercial activities could cause significant material impacts on people’s lives. I will describe the transformation of the existential conditions of the human rights encounter in the data broker industry and demonstrate the structural and systemic exclusion of individuals from the production and profit-making processes which arguably cannot be redressed by any forms of user consent. While I discuss state and commercial digital surveillance separately in Chapters 1 and 2, the nominal distinction should not conceal the fact that public authorities’ surveillance activities often resort to surveillance technologies developed in the private, commercial sectors for commercial purposes, which testifies to the, “voracious indifference, roving opportunism, and endless repurposing characteristic”,⁴⁵ of the new data analytical technologies used in those mass surveillance activities.

Part II discusses how mainstream reactions to digital surveillance have invoked law to regulate digital technologies and their use. Chapter 3 will show that, for both state and commercial digital surveillance, law intervenes to ensure the legality of surveillance activities and to revive basic values of natural justice – transparency and accountability of those activities. These are requirements embraced in modern human rights law when dealing with limitations on fundamental freedoms and have been extensively litigated before and elaborated by human rights courts in state surveillance cases. These requirements are also deemed as central in data protection legal regimes. I will survey the various jurisprudences of human rights and data protection and the recent data protection laws – most notably the EU General Data Protection Regulation – and describe how they articulate the requirements of legality, transparency and accountability.

The problem, however, is that these legal interventions, because they adopt a managerial approach, cannot possibly prohibit surveillance. While claiming individual rights to be essential, they seek to protect interests other than individual rights – for example, the efficiency and effectiveness of deploying police forces, or the development of the digital economy and digital market – and meanwhile phrase these different interests as compatible with each other. Chapter 4 argues that the positivist and managerial account of law exhibited in the legal interventions discussed in Chapter 3 detaches the requirements of legality, transparency and accountability

⁴⁵ *Ibid* at 2.

from their normative underpinnings. It can hardly redress the loss of the human rights encounter under ubiquitous digital surveillance and the structural power asymmetries in surveillance. More problematically, in some circumstances, the management of surveillance practices informed by formal legalism and bureaucratic rationality creates its own barriers of the human rights encounter, a typical problem for encounters with bureaucratic institutions. The law, hence, becomes monstrous.

As I have mentioned earlier, the double inscription of the Frankenstein myth is problematic. The purpose of writing Part I and Part II using this scheme is to demonstrate the impossibility of separating technology's elimination of the human rights encounter and law's elimination of the human rights encounter chronologically and logically in two steps. As will be shown in these two parts, despite their respective focuses, the discussions often allude to the coproduction and mutual-conditioning of surveillance technologies and law in the transformation of governing and the human rights encounter. The surpassing of the double inscription scheme will be summarized in the interim conclusion, which will enable a transition to Part III.

Part III explores alternative ways to understand the elimination of the human rights encounter in surveillance-based governing and its implications. Chapter 5 argues that the elimination of the human rights encounter is a joint accomplishment of surveillance practices and modern law. It is premised on a technical discourse of law, which is different from the technical discourse of law that reduces both law and technology to objects of a sovereign will, and sees law as playing a more proactive role and creating the frames of reference for human behaviors and human relations jointly with technology. Human behavior and relations are disclosed as socially intelligible by technolegal frames of reference. I will study the phenomenon of the transformation of the human rights encounter with a more socio-historical focus. I will argue that there is a process in modernization and political expropriation that replaces the more organic, personal encounters with impersonal individual-institution encounters which are rationalized by modern law and the technique of policing of modern states. This is a process where modern law (including human rights law) and surveillance practices are co-constitutive and together make possible telecommunicated and televised form of control and a particular logic of governing that flattens the plural and produces homogenous time, space and subjects.

Drawing on Foucault and Foucauldian scholarship on policing, I describe this logic of governing as pastoral liberalism and argue that it has an inherent aspect of pacifying and totalizing individuals. Recounting the larger socio-historical trajectory of the transformation of the human rights encounter helps to see current digital surveillance practices as derived from and reinforcing pastoral liberalism and its illiberal and totalizing aspect. This, in turn, helps better understand the stakes of surveillance-based governing, and also to critique current regulatory interventions on digital surveillance. Meanwhile, the illiberal aspect of pastoral liberalism is understood as part of a dilemma which is similar to the encouraging-inhibiting structure of law. While the illiberal and disempowering aspect of pastoral liberalism is augmented by surveillance-based governing, the emphasis on the dilemmatic character of pastoral liberalism and modern law invites investigation into the legal thoughts and practices that could resist totalization and enable individual empowerment, which will lead to Chapter 6.

In Chapter 6, this study moves from a descriptive and explicative project to an explicitly normative one. Whereas in previous parts, the human rights encounter (and its elimination) is treated as a simple, everyday social phenomenon, it is here developed into a notion that has profound normative implications. I will unpack this notion by explaining its theoretical underpinnings drawn from Levinas' ethics and Arendt's political theory and specifically explore how this notion can provide a valuable theoretical basis for human rights and the rule of law. The human encounter is about surprise, uncertainty and vulnerability which are not negative but basic conditions for constituting our subjectivity and the community. A normative notion of human rights encounter emphasizes this anarchic and infinite character of human encounter, one that always surpasses and disturbs the rationalized form of individual-institution encounters. I will argue that the consolidation of surveillance-based governance, which is technologically fundamentalist, amounts to the removal of human plurality and alterity and sterilizes human rights.

If human rights are seen as premised on chaotic and anarchic human encounters and if human encounters are accepted as an essential condition that we cannot afford to discard, how may we think about the political and legal institutions of human rights? Especially, if a case can be made that legal interventions in digital surveillance that adopt a positivist and managerial approach perpetuate the elimination of the human rights encounter, how do we reimagine the

role of law and how do we enact the liberating possibilities in the dilemma of encouraging-inhibiting structure of law? It seems that the discussions go back to the linear way of problem-framing and problem-solving that I try to avoid in previous sections of this thesis. But these questions cannot be avoided if the normative implications of human encounter are taken seriously. What Chapter 6 will do is not prescribe solutions but offer some preliminary ways of re-imagining legal institutions and law's engagement with surveillance technologies inspired by Levinas' and Arendt's work. There exists a valuable body of scholarship that recovers and intensifies the substantive conception of the rule of law, reasserting it as the weapon and locus for people's resistance.⁴⁶ Chapter 6 will engage with this work and provides further support for the normative notion of the rule of law with lessons drawn from Levinas' and Arendt's writings.

⁴⁶ E.g. Mireille Hildebrandt, "Governance, Governmentality, Police, and Justice: A New Science of Police?" (2008) 56 Buffalo Law Rev 557; E P Thompson, *Whigs and Hunters: Origin of the Black Act* (Penguin Books, 1977); Jeremy Waldron, "The Concept and the Rule of Law" (2008) 43:1 Ga Law Rev 1.

Part I

The Frankenstein Myth Part 1: Digital Surveillance and the Elimination of the Human Rights Encounter

Chapter 1. State Digital Surveillance and the Loss of the Human Rights Encounter

Part I of the thesis discusses the loss of the human rights encounter as a phenomenon mainly caused by the practice of digital surveillance. Chapter 1 focuses on the use of digital surveillance by state authorities and looks into four scenarios where digital surveillance operates and is involved in decision making. The first two scenarios involve surveillance operations by state intelligence authorities. From the outset, whatever consequences surveillance leads to, surveillance is by nature a covert and surreptitious activity. A successful surveillance operation is the one the target never learns of. It seems surveillance is all about distancing, camouflaging and avoiding a face-to-face encounter, although the observer and the observed are never really disconnected – the observer and the observed are seized by the unidirectional gaze of the surveillance party. It is also interesting to note that countersurveillance strategies are also often about avoiding, rather than directly initiating, an encounter. Hence, in instances of both surveillance and countersurveillance, there is a radical transformation of the existential conditions of the encounter understood as a participatory event in a specific time and space, with surveillance authorities. Moreover, the transformation of the encounter, properly understood, also takes the form of the untying of those conditions, in ways that dissolve the event of the encounter.

The third and fourth scenarios concern the involvement of digital surveillance in the administration of justice and the delivery of public services. Surveillance, or so-called data mining, becomes increasingly a necessary component of the functioning of these public institutions, such as police, courts, and welfare institutions, which seek to increase efficiency and the transparency of administration. The encounter is not just between individuals and surveillance authorities but primarily between individuals and the institutions which rely on surveillance for various aspects of their decision making, causing material effects on the daily lives of people.

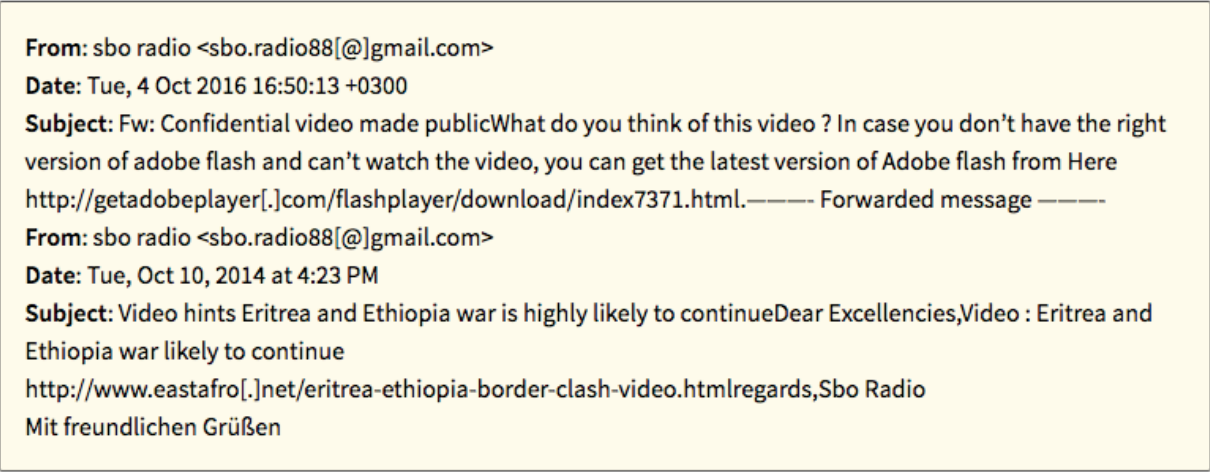
Before the introduction of digital surveillance and data analysis in the processes of governance, individuals' encounters with institutions have been already characterised by the power asymmetries between the two. There have been ways for individuals to become

empowered to encounter and address institutions and crack open the decision-making processes, for example, by asserting their rights to due process. The introduction of and reliance by governmental institutions on digital surveillance, profiling and big data analytics in the processes of decision making and administration changes the already very delicate conditions of encountering and addressing institutions. The transformation of the encounter in each scenario can be related to particular imageries of power relationship structures between people subjected to surveillance and state authorities.

1. Scenarios of state digital surveillance

Scenario 1: targeted surveillance by state intelligence authorities

In December 2017, the Citizen Lab at the University of Toronto published a report on the use of spyware by the Ethiopian government to target Ethiopian dissidents, mainly diasporic Oromia people who have been based outside Ethiopia since 2016.¹ One of the cases documented in the report is the targeting of Jawar Mohammed. Mohammed, the Executive Director of the Oromia Media Network, had circulated information about the government's use of violence against people in the Oromo region of Ethiopia. According to the report, Mohammed had received a number of malicious emails since October 2016.



From: sbo radio <sbo.radio88[.]gmail.com>
Date: Tue, 4 Oct 2016 16:50:13 +0300
Subject: Fw: Confidential video made publicWhat do you think of this video ? In case you don't have the right version of adobe flash and can't watch the video, you can get the latest version of Adobe flash from Here [http://getadobeplayer\[.\]com/flashplayer/download/index7371.html](http://getadobeplayer[.]com/flashplayer/download/index7371.html).----- Forwarded message -----
From: sbo radio <sbo.radio88[.]gmail.com>
Date: Tue, Oct 10, 2014 at 4:23 PM
Subject: Video hints Eritrea and Ethiopia war is highly likely to continueDear Excellencies,Video : Eritrea and Ethiopia war likely to continue [http://www.eastafro\[.\]net/eritrea-ethiopia-border-clash-video.html](http://www.eastafro[.]net/eritrea-ethiopia-border-clash-video.html)regards,Sbo Radio
Mit freundlichen Grüßen

Figure: An email sent to Jawar on October 4, 2016.²

¹ Bill Marczak et al, *Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware* (The Citizen Lab, 2017).

² *Ibid.*

The emails contained a link to a video. The link indicating eastafro[.]net looks very similar to the Eritrean video website eastafro.com. If a user clicks on the link to eastafro[.]net and is using an out-of-date Flash Player, the site will display a message asking the user to update their Flash Player. If clicked, or after 15 seconds, the user is redirected to a page on getadobeplayer.com, which offers the user a real Flash Player bundled with spyware. If the user downloads and installs the Flash Player update in order to watch the video, the spyware will be installed, which gives the spyware sender unauthorized access to the user's computer and allows monitoring of his or her activities and communications.

According to an analysis of the spyware by Citizen Lab, the spyware is called PC Surveillance System and was created for information collection from remote personal computers. By analysing and monitoring a public logfile on PC Surveillance System's command and control server and conducting internet scanning for over a year, Citizen Lab was able to attribute the targeting of Jawar Mohammed to the Ethiopian government and Cyberbit, an Israeli-based cyber security company which develops spyware and is marketed to intelligence and law enforcement agencies globally.

Whether Citizen Lab's findings are correct (bearing mind that attribution is always difficult in the cyber context), Mohammed's case exemplifies a fairly common surveillance practice in which government authorities track identified criminal suspects, political dissidents, activists, and journalists, etc., by gaining access to their targets' devices, then monitor and collect information from them. Monitoring can be realized by installing spyware on personal devices as in the Mohammed case. Government authorities can also track activities of devices by demanding certain data or information about targeted individuals from companies which provide telecommunication services or by demanding companies to provide "backdoor" access to specific devices.

Scenario 2: bulk data collection by state intelligence services

It has been reported since the Snowden Revelations in 2013 that the US government and its allies have been intercepting and collecting massive amounts of communications in real time with little geographical restraint. This raises the issue of bulk surveillance. Examples of bulk surveillance include the disclosed surveillance programmes conducted by the US government under Section

702 of the Foreign Intelligence Surveillance Act 1978, *i.e.* PRISM³ and Upstream,⁴ and the Tempora programme⁵ operated by the UK Government Communications Headquarters (GCHQ) under Section 8(4) of the Regulation of Investigatory Power Act 2000 (RIPA). Despite disputes over the exact details of these programmes, they are all characterised by the lack of pre-defined territorial, personal and thematic scope of data collection. Mass surveillance often finds its rationale in security and the identification and pre-emption of threats, and so targets of surveillance are not well-determined beforehand but need to be ascertained by ‘intelligence leads’ through the surveillance processes.

It is important to note that surveillance to a certain degree has long been regulated, tolerated or even encouraged domestically and internationally, which contrasts with some common claims about the legality vacuum of state surveillance activities.⁶ That state surveillance apparatuses are legally constituted and regulated can be demonstrated by briefly surveying states domestic legislation that entrust different surveillance authorities with different mandates.⁷ Surveillance for the protection of national security is often entrusted to secret service agencies or the military, and the mandates may be further detailed and divided in terms of geographical

³ From an internal NSA PowerPoint presentation, PRISM was described as a program by which the NSA and the FBI obtained the traffic of at least nine giant internet companies, and the materials collected include emails, chats (video and voice), videos, photos, stored data, voice over internet protocol, file transfers, video conferencing, notifications of target activity (including logins), and online social networking details. See Barton Gellman & Ashkan Soltani, “NSA Collects Millions of E-mail Address Books Globally”, *Wash Post* (14 October 2013), online: <https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html?utm_term=.46f442cb300e>.

⁴ Upstream was described as a programme for the ‘collection of communications on fibre cables and infrastructure as data flows past’. See *Ibid.*.

⁵ The Tempora programme has intercepted more than 200 fibre optic cables landing in the UK and has collected all data flowing through the tapped fibre-optic cables since 2011. See Ewen MacAskill et al, “GCHQ Taps Fibre-Optic Cables for Secret Access to World’s Communications”, *The Guardian* (21 June 2013), online: <<https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>>.

⁶ As Fleur Johns has described, vacuums are highly legalised and arguably the work of international lawyers and this is primarily about the legal constructions of non-legality. See Fleur Johns, *Non-Legality in International Law: Unruly Law* (Cambridge University Press, 2013). For the discussion on the uncertainty of legality of surveillance in public international law, see for example, Katharina Ziolkowski, “Peacetime Cyber Espionage - New Tendencies in Public International Law” in Katharina Ziolkowski, ed, *Peacetime Regime State Act Cyberspace Int Law Int Relat Dipl* (Tallinn: : NATO CCD COE Publication, 2013) 425. As for the legality vacuum of surveillance in domestic law, see Chapter 3.2 for further discussion.

⁷ *Foreign Intelligence Gathering Laws: Belgium, France, Germany, Portugal, Romania, Netherlands, Sweden, United Kingdom and European Union* (The Law Library of Congress)..

scope⁸ and types of intelligence.⁹ Whereas such frameworks are mostly set out for unilateral state surveillance, domestic law may also provide certain procedures, albeit in a much less detailed manner, for information sharing with surveillance agencies of other states.¹⁰ At the international level, information sharing, or the so-called intelligence liaison, can also be formalised as a state's international obligation imposed by international or regional organisations or treaties.¹¹

Although there exists some sort of legal framework regulating surveillance agencies and their activities, the problem with bulk digital surveillance is that it easily blurs the lines between different surveillance activities categorised in terms of purpose and scope in law. Among other things, the capacity to collect in real time massive amounts of data which have no link with territory makes the distinction between targeted and untargeted surveillance and that between internal and external surveillance unlikely to sustain. Both the UK and US governments deny that these programmes are “bulk” surveillance and explain that there is a selection and filtering process that determines the data to be picked up and examined by analysts. They also claim that this selection and filtering process fulfils the requirements of necessity and proportionality which are key to the protection of human rights.¹²

However, as long as the selection terms are not available to and understood by the public, the term “targeted surveillance” as understood by governments makes little sense to individuals. The distinction between internal and external surveillance is also arbitrary due to the lack of territorial connection between data and data subjects. For example, the UK RIPA defines

⁸ E.g. the UK Secret Service, also known as MI5, is a domestic intelligence agency, whereas the Secret Intelligence Service, also known as MI6, is a foreign intelligence agency. Their functions are separately provided for by the *Secret Service Act 1989* (UK) and the *Intelligence Service Act 1994* (UK).

⁹ E.g. the UK GCHQ (Government Communications Headquarters) is a signal intelligence gathering agency. Its function is defined by *Intelligence Service Act 1994*. See *Intelligence Service Act 1994* (UK), c13, s3(1).

¹⁰ E.g. According to the UK *Intelligence Service Act 1994*, the GCHQ operates under the control of a Director, who is appointed by the Secretary of State with the duty to ensure there are arrangements so that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings. See *Intelligence Service Act 1994* (UK), c13, s4(2)(a). The rules for requesting and handling unanalysed intercepted communications from foreign governments are set out further in the *Interception of Communications Code of Practice* issued by the UK government on 15 January 2016. See, *The Regulation of Investigatory Power (Interception of Communications: Code of Practice) Order 2016*, SI 2016/37.

¹¹ E.g. the obligations of exchanging information are laid down in Article 8 of the Statute of the International Atomic Energy Agency. *Statute of the International Atomic Energy Agency*, 26 October 1956, 276 UNTS 3 (entered into force 29 July 1957). See also Adam DM Svendsen, *Understanding the Globalization of Intelligence* (London/Basingstoke: Palgrave Macmillan, 2012) at 38–39.

¹² *10 Human Rights Organisations v the United Kingdom*, No. 58170/13, “The United Kingdom’s Observations on the Merits” (18 April 2016) at 30-33, paras 1.6-1.8.

“external communication” as a communication sent or received outside the British Islands.¹³ This is interpreted by the UK government as including when a person in the UK conducts a Google search on his or her internet browser, uses YouTube, or posts an item on a web-based platform such as Facebook or Twitter. In these scenarios the person is communicating with web servers based outside the UK and the communication will be viewed as external.¹⁴ The person, therefore, falls into a wholly different surveillance procedure for external communications. In addition to the geographical arbitrariness, it has also been pointed out that our conventional understanding that only the actual content of communication implicates the privacy right is unlikely to withstand the massive collection and analysis of communications data or metadata. This data is made up of information about communications and may include the source and destination of a communication, the time, duration and location of a communication, type of the device used, etc. Although not disclosing the content, the processing of communications data or metadata collected may even be more intrusive and more revealing than the content of communications.¹⁵ The Court of Justice of the European Union, hence, has observed that this data, “taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained.”¹⁶

In the first two scenarios (targeted surveillance by state intelligence authorities and bulk data collection by state intelligence services, respectively), the surveillance technologies are used in the absence of laws that protect individual rights, or despite existing regulations and laws, or are used to exploit and bypass existing legal frameworks. Each scenario demonstrates typical situations where technology can become problematic, even when justifications such as counterterrorism or the protection of national security are invoked.

¹³ *Regulation of Investigatory Powers Act 2000*, *supra* note 2, s20.

¹⁴ *Supra* note 12, at 146-147, para 4.69.

¹⁵ E.g. Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UNHRC, 27th Sess, UN Doc A/HRC/27/37 (2014), at 6-7, paras 19-20. Pieter Omtzigt, *Mass Surveillance*, AS/Jur (2015) 01 (Committee on Legal Affairs and Human Rights, Parliament Assembly of the Council of Europe, 2015) at 6, para 12.

¹⁶ *Digital Rights Ireland Ltd v. Minister for Communications and Others*, Joined Cases C-293/12 and C-594/12, [2014] ECLI:EU:C:2014:238, paras 26-27.

Scenario 3: digital surveillance in law enforcement

The previous two scenarios demonstrate a certain degree of exceptionality for several reasons: in the first scenario, targeted surveillance by installing spyware in the target's device would be considered illegal in many countries where the search of one's device needs specific authorization from a court; in the second scenario, intelligence authorities are usually shrouded in high secrecy and are subject to special legal and regulatory regimes. These surveillance authorities and their operations are closely engaged in the darkest side of state sovereignty and either are regulated with special legal regimes or are operating despite the law. However, digital surveillance is also increasingly used in the more common, day-to-day law enforcement and administration of justice.

Although state intelligence authorities, entrusted to protect national security, usually have far more resources and the capacity to conduct mass surveillance, it is increasingly the case that domestic law enforcement authorities rely on data mining and algorithms to generate crime patterns and to predict changes in crime patterns.¹⁷ Crime patterns involve an analysis of “who” is suspicious, “where” particular crimes are more likely to occur and “when”. The identification of crime patterns, to a significant degree, informs how the police should deploy and allocate manpower for the purpose of preventing the commission of crimes. Data involved in the identification of crime patterns typically includes the criminal statistics of a region as well as its demographic and geographic information. Recent criminology studies also suggest that data collected via social media could be indicative as well. For example, Twitter posts and corresponding geolocation data have been collected and analysed to map crime patterns, allegiance to extremist groups, and crime hotspots.¹⁸ In addition, it is interesting to note that data mining and crime pattern analysis are used not only for planning patrol operations but sometimes

¹⁷ E.g. Rosamunde van Brakel & Paul De Hert, “Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies” (2011) 20:3 J Police Stud 163; Lyria Bennett Moses & Janet Chan, “Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools” 37:2 UNSW Law J 643; Rik Peeters & Marc Schuilenburg, “Machine justice: Governing security through the bureaucracy of algorithms” (2018) 23:3 Inf Polity Int J Gov Democr Inf Age 267.

¹⁸ E.g. Matthew L Williams, Pete Burnap & Luke Sloan, “Crime Sensing With Big Data: The Affordances and Limitations of Using Open-source Communications to Estimate Crime Patterns” (2017) 57:2 Br J Criminol 320; Nick Malleson & Martin A Andresen, “The impact of using social media data in crime rate calculations: shifting hot spots and changing spatial patterns” (2015) 42:2 Cartogr Geogr Inf Sci 112.

also for tracking police staff member internally, directing and monitoring their performance of duty.¹⁹

Examples of so-called “intelligence-driven” policing include the PredPol (predictive policing) system used in many jurisdictions in the US and the Crime Anticipation System used in the Netherlands. The PredPol system is developed by a private company which claims it uses historical event datasets about crime type, location, and date and time to train a machine-learning algorithm to generate predictions. Predictions are displayed as red boxes representing 150×150-metres squared, which represent the highest-risk areas for each day and for the corresponding police shift. It is claimed that, for the protection of people’s privacy, no personal identifiable information, demographic, ethnic or socio-economic information is used for calculating predictions.²⁰ The Dutch system was developed in-house by the Dutch police. It divides maps of Dutch cities and districts in blocks also representing 125×125-metres squared and predicts hot spots and hot time periods. Different colours correspond to different crimes and the colour increases in intensity when the risk level for high-impact crimes increases.²¹ The Dutch system uses open demographic and geographical data and crime statistics gathered by the police force and processes them through algorithms to calculate the risk score of each city block.²² Both the US and Dutch systems do not focus on high-risk individuals as such, but inevitably certain indicators and the combination of them (such as the number of social benefits recipients in a zip code area, or the number of known offenders or suspects living in a certain area) make certain groups of people especially likely to be targeted. In addition to these systems for predicting hotspots and hot time periods, there is also a system that calculates people’s risk scores for committing crimes in the future. The risk scoring of individuals is usually combined with the identification of high-crime areas. The Los Angeles Police Department has been using the Los Angeles Strategies Extraction and Restoration program since 2011, a point system to rank

¹⁹ “Law Enforcement | PredPol Law Enforcement Intelligence Led Policing Software”, online: *PredPol* <<https://www.predpol.com/law-enforcement/>>; Peeters & Schuilenburg, *supra* note 17.

²⁰ *PredPol Law Enforcement Intelligence Led Policing Software*, *ibid*.

²¹ Serena Oosterloo & Gerwin van Schie, “The Politics and Biases of the ‘Crime Anticipation System’ of the Dutch Police” 12.

²² *Ibid*.

individuals to identify so-called “chronic offenders” (*i.e.*, violent repeat offenders and gang members) in crime hotspots.²³

In addition to predictive policing, a core aspect of the criminal justice system is also increasingly dependent on surveillance, profiling and data analytics. It has been reported that in the US, courts in several jurisdictions have adopted algorithms for decisions about bail, sentencing and probation.²⁴ For example, in 2013, the state of Wisconsin charged Eric Loomis with five criminal counts related to a drive-by shooting in the city of La Crosse. Loomis pleaded guilty to two of the less severe charges, “attempting to flee a traffic officer and operating a motor vehicle without the owner’s consent”, while the rest of the charges were dismissed but made available for the trial court to consider at sentencing. At the sentencing hearing, the court relied in part on the COMPAS (Correctional Offender Management Profiling for Alternative Sanctions, a software assessing recidivism risk developed by a private company, Northpointe) assessment and sentenced Loomis to six years of imprisonment and five years of extended supervision. This example of using algorithms in the sentencing process became well-known as Loomis challenged the trial court’s decision and argued it violated his due process rights because the COMPAS methodology used was a trade secret. The case was brought to the Wisconsin Supreme Court. The Court rejected his argument and held that as the COMPAS report was not the sole basis for the sentencing decision, the decision was sufficiently individualized because the trial court had the discretion and information necessary to disagree with the report’s assessment when appropriate.²⁵ Nevertheless, the Wisconsin Supreme Court required the presentencing investigation reports to include a written advisement to inform judges about the limitations of such assessments.²⁶

²³ 5 points if the individual is a gang member; 5 points if the individual is on parole or probation; 5 points if the individual had any prior arrests with a handgun; 5 points if the individual had any violent crimes on his rap sheet; 1 point for every “quality” police contact in the last two years. “How LASER Focus Cut Homicides in Crime-Prone L.A. District”, (7 August 2013), online: *Crime Rep* <<https://thecrimereport.org/2013/08/07/2013-08-reducing-gun-violence-in-la/>>; Craig Uchida et al, *Los Angeles, California Smart Policing Initiative: Reducing Gun-Related Violence through Operation Laser* (Bureau of Justice Assistance, 2012).

²⁴ Julia Angwin et al, “Machine Bias”, (23 May 2016), online: *ProPublica* <<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>>; George Joseph, “Justice by Algorithm”, (8 December 2016), online: *CityLab* <<http://www.citylab.com/crime/2016/12/justice-by-algorithm/505514/>>..

²⁵ *State v. Loomis*, 881 NW (2d) 749 (2016), para 109.

²⁶ The limitations the Wisconsin Supreme Court identified and required to be mentioned in the advisement include:

- The proprietary nature of COMPAS has been invoked to prevent disclosure of information relating to how factors are weighed or how risk scores are determined;

Although in this case, an algorithm-produced report was not the sole basis for the sentencing decision, there is nevertheless growing support for implementing algorithm programs in the US judiciary for more “objective” and “evidence-based” decisions.²⁷ Digital surveillance as such is not at the front-stage of the trend towards the “automation” of the administration of justice in the sense that judges themselves are not involved in surveillance. But digital surveillance that gathers massive amounts of information and produces the datafication of risk indicators form the necessary backbone for training algorithms used in the process of judicial decision-making.

Scenario 4: digital surveillance in the provision of public services

On an even broader scale, digital surveillance, data mining and profiling have also been deployed for the administration of public resources and the delivery of social benefits. Corruption, fraud, long processing times, non-claiming, undue payments, *etc.*, are typical problems in the administration and provision of social benefits. Technologies of digital surveillance and data analytics are claimed to address these problems, to increase the efficiency, transparency and equity of social benefits delivery and to reduce administrative costs. In light of such acclaimed benefits, there has emerged the largest biometric identification system in the world – India’s Aadhaar program, which launched in 2009. A central government agency, the Unique Identification Authority of India, collects and stores demographic and biometric data of each registered person and assigns each person a Unique Identification number. The purposes of the program are to eliminate fake and duplicate IDs, make verification easy and cost-effective, and,

-
- Because COMPAS risk assessment scores are based on group data, they are able to identify groups of high-risk offenders – not a particular high-risk individual;
 - Some studies of COMPAS risk assessment scores have raised questions about whether they disproportionately classify minority offenders as having a high risk of recidivism;
 - A COMPAS risk assessment compares defendants to a national sample, but no cross-validation study for a Wisconsin population has yet to be completed. Risk assessment tools must be constantly monitored and re-normed for accuracy due to changing populations and subpopulations.
 - COMPAS was not developed for use at sentencing, but was intended for use by the Department of Corrections in making determinations regarding treatment, supervision, and parole.

See *State v. Loomis*, *ibid*, at paras 66 and 100.

²⁷ William Ray Price Jr, *Chief justice delivers 2010 state of the Judiciary address* (Jefferson City, Missouri, 2010).

“provide good governance, efficient, transparent and targeted delivery of subsidies, benefits and services,” to the residents of India.²⁸

Such an identification system is just one preliminary step in the new data-driven public administration. More innovative programs use profiling and data mining to predict the probability of fraud, rather than just to detect fraudulent applicants. Digital surveillance and algorithms become essentially risk-management tools just as in Scenario 3 (digital surveillance in law enforcement). In France, the *Caisse nationale des allocations familiales* and the *Pôle Emploi* have been monitoring French welfare beneficiaries using data mining and algorithms and give beneficiary files risk scores calculated by various logistic regression models (logistic regression is a statistic model used to calculate the probability of certain events).²⁹ Information used in those models for risk identification includes one’s housing status, household composition, and the professional status of adults in the household. For example, the risk of undue payment is said to significantly increase when adult children live with the parents. Home checks will be performed on those whose files are flagged for high risk of fraud.³⁰

In Scenarios 3 and 4 (digital surveillance in law enforcement and digital surveillance in the provision of public services, respectively), digital surveillance, along with advanced data analytical tools, become a necessary component in the administration and functioning of public authorities. As will be discussed shortly, the use of these technologies transforms conventional encounters with institutions in many respects. It is also important to notice that the use of these technologies is deeply embedded in some classic conceptions about bureaucratic rationality and impersonality and that in practice they also exhibit some continuities with pre-existing measures of public administration. The most noted continuity is the intended or unintended bias introduced into algorithms because the input data are already discriminatory. For example, past crime statistics can be racially biased because a neighbourhood where the majority of residents are black people tends to attract more police. Naturally then, more offences will be detected and reported than in the areas where fewer police are deployed. Using such statistics to train

²⁸ “Vision & Mission”, online: *Unique Identif Auth India Gov India* <<https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/vision-mission.html>>.

²⁹ Vincent Dubois, Morgane Paris & Pierre-Edouard Weill, “Targeting by Numbers. The Uses of Statistics for Monitoring French Welfare Benefit Recipients” in Lorenzo Barrault-Stella & Pierre-Edouard Weill, eds, *Creat Target Publics Welf Policies Comp Multi-Level Approach*, Logic, Argumentation & Reasoning (Cham: Springer International Publishing, 2018) 93.

³⁰ *Ibid.*

algorithms will generate equally biased predictions that reaffirm pre-existing biases. Hence, despite the appeal of being evidence-based and objective, the so-called “digital offspring” of conventional bureaucratic procedures tends to reinforce rather than correct existing problems, confirm the existing categorisation of people and also reinforce the privilege of those who happen to belong to the categories that are not suspected.

Moreover, risk management strictly speaking is not just about external risks – such as, whether a crime is likely to happen, whether a defendant will flee before the trial, whether an offender will commit crimes again, or whether recipients of social welfare file false documents. Risk management also deals with internal risks, such as the quality of information collected, the reliability of the algorithm, and performance of duties by police officers or judges. Many proponents of such monitoring programs (without necessarily using the derogatory word “surveillance”) emphasize their benefits for managing these internal risk factors. For example, it is proposed that statistics of judges’ decisions in asylum request cases can be analysed to reveal judicial bias, which could then motivate certain reformative action to combat such bias.³¹ However, in practice, implementing such risk management programs in the administration of law enforcement and in the administration of social benefits usually ends up being equated with monitoring the external risk factors and targeting particular groups of people.³² That using data analysis to manage internal risk factors gets marginalized can also suggest the resistance from within the bureaucracy against potential scrutiny facilitated by digital surveillance. France’s recent ban of the use of data analysis regarding the behaviour of individual judges serves as an example of such resistance.³³

2. Transformation of encounters

2.1 Encounters with surveillance authorities: transformation and avoidance

As with other forms of surveillance – e.g. the old school ways of stalking, intercepting letters, and wiretapping telephone calls – encounter in digital surveillance is unidirectional. In those cases, there is still the possibility of the surveillance being discovered because the surveillance is

³¹ Malcolm Langford & Mikael Rask Madsen, “France Criminalises Research on Judges”, (22 June 2019), online: *Verfassungsblog* <<https://verfassungsblog.de/france-criminalises-research-on-judges/>>.

³² *Ibid* at 98.

³³ Langford & Madsen, *supra* note 31.

poorly executed, and the targeted people could directly confront the agents who have been listening or watching and recover a face-to-face encounter with the surveillance agents. The immanent possibility of exposure, however, has been dramatically reduced by digital surveillance technologies that enable more covert surveillance at a distance. Although it is possible to detect digital surveillance – for example, by checking a suspicious website link contained in an email and detecting spyware – it is significantly harder without the necessary technical expertise.

More importantly, digital surveillance mediates and transforms the existential and constitutive conditions for an event of encounter, which makes extremely difficult and unlikely the recovery of encounter by people who are targeted. As will be discussed throughout the thesis, the elimination of encounter, properly understood as a participatory and often conflictual event, amounts to the deprivation of people's capacity to confront and challenge the surveillance authority (public or private) to whom they are subjected. More seriously, when such elimination of encounter is incorporated into the practices of the judicial system, the inability to recover a human rights encounter means the inability of individuals to even remain legal subjects.

a. The amorphous state surveillance apparatus

The first two scenarios vary remarkably in terms of the surveillance capacities of state surveillance agencies. The Ethiopian government itself is under-equipped to track political dissidents outside Ethiopia, and so, is provided with the service by private companies; whereas the NSA or the GCHQ are capable of hiring or sub-contracting thousands of computer scientists, technicians and data analysts and developing surveillance technologies. Despite the different surveillance capabilities and scales of digital surveillance operations, in both scenarios, a state-of-the-art state surveillance apparatus augmented by digital technologies is a complex, technically and institutionally divided, and geographically fragmented actor-network. Despite pre-existing legal frameworks that give mandates to specific surveillance agencies, it seems that the state surveillance apparatus is increasingly becoming an amorphous creature deeply involved in the market of the global surveillance industry and actively engaged with private actors providing various cyber operation services all over the world. Certainly, such indeterminacy and the entanglement with non-state actors are not just phenomena of the surveillance apparatus, but

also a broader trend in governance by neoliberal, “cunning” states which, presenting themselves as weak, often contract out state functions and deny responsibilities.³⁴

To demonstrate the amorphous character of state surveillance apparatus, I will now focus on the state surveillance apparatus for bulk surveillance and demonstrate its extraordinary institutional and operational complexities using information from the Snowden Revelations, the litigation brought by human rights organizations and some reports from the Council of Europe. Bulk surveillance takes a series of steps – from the mass, real-time collection of data, selection and filtering of intercepted data, to reading and analysing selected data by analysts, and storing the data for a certain period of time before deletion.³⁵ Each of these steps may involve proxies such as subcontracted individual IT experts or private companies who provide technical assistance, as mentioned in the first scenario. Bulk surveillance also often requires collaboration with large tech companies (who may be willing or compelled) as exemplified by the NSA’s PRISM program.³⁶ Bulk surveillance may also involve collaboration with the surveillance agencies of other states when there is an enduring mutual interest or for a particular purpose of joint intervention.

This third way of constituting a surveillance network – intelligence collaboration – is claimed by governments as being of vital importance for risk identification and the protection of national security.³⁷ One infamous example is the UKUSA agreement about the gathering,

³⁴ Shalini Randeria, “Cunning States and Unaccountable International Institutions: Legal Plurality, Social Movements and Rights of Local Communities to Common Property Resources” (2003) 44:1 Eur J Sociol 27.

³⁵ An example is the UK’s surveillance regime under the Section 8(4) of RIPA. It is described as consisting of three stages: collection, filtering and selection for examination. Each of these stages contains assessments of the intelligence value for a communication and uses different analytical tools. It also describes how two distinct processes are applied: the stronger selector process whereby any communications which match the selectors are automatically collected, and the complex query process whereby GCHQ matches much more complicated criteria. See David Anderson, *Report of the Bulk Powers Review* (Independent Reviewer of Terrorism Legislation, 2016) at 22–25.

³⁶ One leaked document from Edward Snowden is a PowerPoint presentation from the NSA demonstrating its data collection from major US service providers in the PRISM program. Barton Gellman & Ashkan Soltani, “NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say”, *Wash Post* (30 October 2013), online: <https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?utm_term=.b3c3cb444959>; Glenn Greenwald & Ewen MacAskill, “NSA Prism Program Taps in to User Data of Apple, Google and Others”, *The Guardian* (7 June 2013), online: <<http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>>.

³⁷ E.g. *10 Human Rights Organisations v the United Kingdom*, No. 58170/13, “The United Kingdom’s Observations on the Merits” (18 April 2016), *supra* note 12, at 37.

exchange and analysis of foreign communication³⁸ and the ECHELON program under this agreement. In 2001 the European Parliament conducted an inquiry about this program and described it as, a “global system for intercepting communications”. It observed two features making it unusual: first, it had the capacity to carry out quasi-total surveillance, as the satellite receiver stations and spy satellites were able to intercept any communication (via email, telephone and fax) sent by any individual; second, it operated worldwide with cooperation proportionate to the capacities of each partner of the programme, each partner placing their interception system at its disposal, making joint use of the resulting information.³⁹

A more recent example is the project MUSCULAR revealed in the Snowden leaks of 2013. It is reported from the leaked NSA documents that the NSA and the GCHQ broke into Yahoo! and Google’s data centres by tapping their main communication links around the world and copying entire data flows across their fibre-optic cable networks.⁴⁰ The access points were located in the UK and the GCHQ placed all intake communications into a “buffer” for three to five days before they were deleted to reuse the storage space. From the buffer, tools built by the NSA were used to unpack and decode the special data formats used inside the cloud storage belonging to the two companies, and then a series of filters selected information from the data wanted by the NSA.

As mentioned earlier, joint-surveillance programmes, the so-called intelligence liaison, can be formalized as a state’s obligations imposed by international or regional organisations.⁴¹ A typical example is the obligations created by the UN Security Council Resolution 1373, which called on Member States to intensify and accelerate the exchange of information among states to

³⁸ The initial UKUSA agreement was signed on 5 March 1946 to continue a practice of signals intelligence cooperation since the Second World War throughout the Cold War. The UKUSA agreement was later joined by Australia, New Zealand and Canada (in total the Five Eyes). See Jeffrey Richelson, *The US Intelligence Community*, 7th edition ed (Boulder: Westview Press, 2016) at 369–371.

³⁹ See Gerhard Schmid, *Report on the Existence of A Global System for the Interception of Private and Commercial Communications (ECHELON Interception System) (2001/2098(INI))*, A5-0264/2001 (Temporary Committee on the ECHELON Interception System, European Parliament, 2001) at 23, para 1.6. While ECHELON generated outrage in Europe, the 9/11 attack in the US two months after the report of the European Parliament’s inquiry suggested that ECHELON was not as “all-powerful” as the media claimed, and the criticisms and recommendations to restrict the surveillance activities fell silent. Adam DM Svendsen, *Intelligence Cooperation and the War on Terror: Anglo-American Security Relations after 9/11* (New York: Routledge, 2009).

⁴⁰ Gellman & Soltani, *supra* note 36.

⁴¹ E.g. the obligations of exchanging information are laid down in Article 8 of the Statute of the International Atomic Energy Agency. *Statute of the International Atomic Energy Agency*, 26 October 1956, 276 UNTS 3 (entered into force 29 July 1957). See also Svendsen, *supra* note 11 at 38–39.

prevent the commission of terrorist acts.⁴² Following the adoption of the resolution, international intelligence cooperation was enhanced by the UK and US which helped countries like Kenya to build counterterrorism capacities and was also enhanced by the Counterterrorism Committee of the UN Security Council created by Resolution 1373.⁴³ So, the infrastructure of global surveillance is embedded in international cooperation among states.

Apart from formalized arrangements for intelligence cooperation, informal and sometimes unwritten agreements are equally, if not more commonly used to create intelligence liaisons.⁴⁴ Contracts with proxies and the deals with surveillance partners are often not subject to public scrutiny. For example, these arrangements are sometimes called, “arrangements below the waterline”. In the case *Liberty and others v GCHQ* before the UK Investigatory Powers Tribunal, the Tribunal described them as, “too confidential and sensitive for discussion in open court in the interests of preserving national security”.⁴⁵ The murky relationship with intermediaries and surveillance partners make it extremely difficult to ascertain how, from whom and when certain data are collected, selected or examined. The difficulties raised for judicial scrutiny will be discussed in Chapter 3.

Adding to the problems of institutional and processual secrecy and the fragmentation of state surveillance, bulk digital surveillance raises another question as to what to do with the large amount of raw materials collected. Digital surveillance relies on algorithmic decision-making to solve the problem of the overabundance of data. The collected data needs to be filtered and their salience and value have to be determined before their examination of the data. In a report by the UK Intelligence and Security Committee of Parliament in 2015, which reviewed the capacities of the UK intelligence agencies, the selection of intercepted communication was summarised. Two main processing systems were used. For the first processing system, the GCHQ first chose the

⁴² SC Res 1373, UNSC, 2001, UN Doc S/RES/1373, at 2 para 2(b). That international organizations impose the obligation of information sharing and is part of the reason why transnational surveillance per se is not illegal under international law although it is often denounced. Simon Chesterman, “Intelligence Cooperation in International Operations: Peacekeeping, Weapons Inspections, and the Apprehension and Prosecution of War Criminals” in Hans Born, Ian Leigh & Aidan Wills, eds, *Intell Coop Account* (Routledge, 2011) 124..

⁴³ Svendsen, *supra* note 39 at 40–41.

⁴⁴ Former CIA Inspector General, Frederic Hitz, says “formal intelligence liaison relationship between cooperating services are seldom reduced to writing, even between long-term allies. The less said the better is the norm.” Frederic Hitz, *Why Spy?: Espionage in an Age of Uncertainty* (New York: St. Martin’s Press, 2008)., cited in Svendsen, Svendsen, *supra* note 11 at 12.

⁴⁵ *Liberty and others v GCHQ and others* [2014] UKIPTrib 13_77-H, para 7.

particular “bearers”⁴⁶ to access and compared the communication flowing across those bearers against a list of “simple selectors”. These simple selectors were specific identifiers relating to a known target. And accordingly, any communications that matched the simple selectors were collected.⁴⁷ The second processing system applied “selection rules”, matching the data against more complicated criteria of three or four elements. This second system was targeted at communications across a smaller number of “bearers” considered as most likely to carry communications of intelligence interests.⁴⁸ The report claimed that:

By performing complex searches combining a number of criteria, the odds of a ‘false positive’ are considerably reduced. The system does not permit GCHQ analysts to search these communications freely (i.e. they cannot conduct fishing expeditions). The complex searches draw out only those items most likely to be of highest intelligence value. These search results – around *** items per day – are then presented to analysts in list form: it is only the communications on this list that analysts are able to open and read. They cannot open any communications which have not matched the complex searches. (This can be thought of as using a magnet to draw the needle out of a haystack instead of combing through the straw yourself.) Analysts then rank the communications on the list in order of intelligence value, in order to decide which ones to examine: they open and read only a very tiny percentage of the communications collected (around *** items per day) ...⁴⁹

While the report repeatedly emphasized the limited number of communications being examined in the end,⁵⁰ the crucial problems regarding what the selectors, selection rules and complex searches are, how they are designed and how the intelligence value of

⁴⁶ Each internet fibre cable carries a number of “bearers” which can carry up to 10 gigabytes data per second.

⁴⁷ Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and transparent legal framework* (2015) at 27–28.

⁴⁸ *Ibid* at 29.

⁴⁹ *Ibid* at 3–4.

⁵⁰ Similarly, in its report of February 2016, the UK Intelligence and Security Committee of Parliament stated that it remained of the view that, “the investigatory powers of the Agencies were authorised to employ were necessary and proportionate”. See Intelligence and Security Committee of Parliament, *Report on the Draft Investigatory Powers Bill* (2016) at 1.

the data is measured and ranked were unexplained.⁵¹ As will be seen later, essentially the same questions are raised in the cases of predictive policing and risk-management in the administration of justice and social welfare. The design of the algorithm often presumes certain normative preferences and judgments which are unknown not only to the public but also often to the users – the judges, the police officers or other bureaucrats.

Nevertheless, the report did give a hint: “In simple terms, [the system] can be considered as similar to the search results obtained from an internet search engine (like Bing or Google) ***. Just as with a normal web search, analysts will not examine everything – they must use their judgment and experience to decide which communications appear most relevant.”⁵² If this comparison is appropriate, it is fair to argue that the selection process is like a Latourian actor-network in which decisional agency is distributed among human agents and non-human actants, *i.e.* algorithms. When we use Google search, the search results are ranked by Google’s search algorithm which largely conditions our choices, even we as users may feel we are exercising our judgment and agency when clicking a link. The ranking may be inexplicable to the user and even to the algorithm’s developers. It has been observed that when the decision model is too complex and employing multi-layer neural networks, how the machine extracts and uses the ‘knowledge’ from the input data often becomes unexplainable.⁵³ So an analyst’s exercising of her or his judgment and experience does not mean she or he actually decides what communications will be examined. By describing the process as an actor-network, I do not intend to argue that surveillance agents have less decisional agency or

⁵¹ According to another report by the Independent Reviewer, David Anderson, examples of a, “strong selector”, include telephone number or email address. Complex queries combine a number of criteria, which may include weaker selectors but which in combination aim to reduce the odds of a false positive. What the weaker selectors are and how they are combined are not explained. David Anderson, *Report of the Bulk Powers Review* (Independent Reviewer of Terrorism Legislation, 2016) at 23–24, para 2.17. The report also mentioned that the UK Home Office has been developing filtering arrangements between multiple databases to speed up complex analyses on aggregated systems and were still at the stage of defining requirements before going to the design phase. The scope of the filtering arrangements was uncertain and will not be fully operational in the short term. David Anderson, *Report of the Bulk Powers Review* (Independent Reviewer of Terrorism Legislation, 2016) at 98, paras 6.26-6.28..

⁵² Intelligence and Security Committee of Parliament, *supra* note 47 at 31.

⁵³ Reuben Binns et al, “*It’s Reducing a Human Being to a Percentage*”: *Perceptions of Justice in Algorithmic Decisions* (ACM Press, 2018) at 2. An interesting example about how the machine learning process cannot be understood or predicted by the developers is an artificial intelligence system developed by Facebook, which diverged from its training and developed its own language. The researchers had to shut it down. See “Researchers Shut Down AI that Invented Its Own Language”, (21 July 2017), online: <<http://www.digitaljournal.com/tech-and-science/technology/a-step-closer-to-skynet-ai-invents-a-language-humans-can-t-read/article/498142>>..

even are not responsible for their actions. My point is that when an algorithm is used in the crucial task of selecting communications for examination and if we accept the UK government's argument that it is this act of selection that initiates surveillance, state surveillance becomes even more uncertain and unpredictable to individuals, and it is more difficult for individuals to experience and to recover an event of encounter.

In sum, the state surveillance apparatus has tremendous capacity for metamorphosis by subcontracting various surveillance tasks to proxies (individual computer scientists or private companies), or by obtaining backdoor access to the systems of large internet service providers, and by sharing information and techniques with surveillance partners. We also witness the distribution of decisional agency between surveillance agents and machines, which adds another important factor to the uncertainties of state digital surveillance operation.

b. The diffusion of the space of surveillance

The architectural feature of the internet which allows data to travel irrespective of territorial links contributes to the spatial transformation of surveillance. About ninety-nine percent of international communications travel through fibre-optic submarine cables.⁵⁴ As a result, a state which is well-situated as a major hub for international communication traffic can sometimes easily intercept large amounts of communications within the state's jurisdiction, and the distinction between internal surveillance and external surveillance is muted.⁵⁵ This is the case in the disclosed TEMPORA project conducted by the GCHQ since 2011. The GCHQ has attached intercept probes to more than 200 transatlantic fibre-optic cables where they land on British shores and carry data from telephone exchanges and internet services in North America to Western Europe.⁵⁶

⁵⁴ Alan Mauldin, *What the Internet looks like: Undersea cables wiring ends of the Earth* (2015).

⁵⁵ The highly problematic distinction between internal and external surveillances is exemplified by the UK RIPA. It defines, "external communication", as a communication sent or received outside the British Islands. *Regulation of Investigatory Powers Act 2000*, *supra* note 2, s20. This is interpreted by the UK government as when a person in the UK conducts a Google search on a browser, the person is having a communication with the web servers based outside the UK, and the communication will therefore be external. *10 Human Rights Organisations v the United Kingdom*, No. 58170/13, "The United Kingdom's Observations on the Merits" (18 April 2016) at 146-147, para 4.69.

⁵⁶ MacAskill et al, *supra* note 5.

Adding complexity to the architectural feature of global telecommunication, and more importantly, the spatial diffusion of digital surveillance is achieved through the transformation of the state surveillance apparatus as discussed above. Specific factors which contribute to the geographical expansion and fragmentation of state surveillance activities include: first, private actors that provide cyber operation services to the state are highly mobile and their existence and activities are often transnational; second, companies which own global platforms like Google and Yahoo! maintain multiple data centres on four continents and transmit data through their cloud network, increase cyber security risks and create new possibilities for bulk data collection; third, due to formal or informal cooperation agreements, a state surveillance agency can operate extraterritorially by establishing offices and facilities in partner states; fourth, also due to intelligence cooperation, a state can benefit from its surveillance partners, and unlike offering information to foreign agencies, receiving information that is willingly offered is subject to virtually no restrictions.⁵⁷

Each of the factors raises transparency issues. But the lack of transparency is not the only contributor to the spatial obscurity of state digital surveillance. The spatial diffusion of surveillance is a manifestation of the restructuring of the state surveillance apparatus that forms a “global value chain” of surveillance based on formal or informal arrangements. “Global value chain” describes the global-scale of the production and trade of goods or services,⁵⁸ which provides some interesting parallels with the chain of surveillance: Companies expand their operations internationally by outsourcing and offshoring production activities to different companies across a variety of locations and the production process is divided among a number of

⁵⁷ This is why a major concern is the circumvention of domestic constraints on interception by receiving intelligence materials from surveillance partners. In the case *Liberty and others v GCHQ and others*, the UK government detailed the highly restricted circumstances in which intelligence services would seek intercepted communication from a foreign government. After the IPT’s judgment of 5 December 2014, they published a set of rules for requesting and handling unanalysed intercepted communications from a foreign government in the current Interception of Communications Code of Practice, which requires the request to be necessary and proportionate. See Home Office, *Interception of Communications Code of Practice, Pursuant to section 71 of the Regulation of Investigatory Powers Act 2000* (London, 2016), ch 12. But these rules apply to the request of communications and leave unregulated the reception of communications offered by intelligence partners without making the request.

⁵⁸ E.g. The UNCTAD describes global value chains: “The fragmentation of production processes and the international dispersion of tasks and activities within them have led to the emergence of borderless production systems – which may be sequential chains or complex networks and which may be global, regional or span only two countries... [Global value chains] are typically coordinated by transnational corporations (TNCs), with cross-border trade of production inputs and outputs taking place within their networks of affiliates, contractual partners... and arm’s length suppliers.” See United Nations Conference on Trade and Development, *World Investment Report 2013: Global Value Chains: Investment and Trade for Development* (UN, 2013) at 122.

companies and geographically spread. The production process and value distribution are adjusted to and also change the capacities of the affiliated or contracted companies and the local social, legal, political and environmental circumstances. The patterns of global value chains thus continue to shift.

In state digital surveillance, there is a similar restructuring of the state surveillance apparatus by way of dispersing the production of intelligence across different locations to maximize data collection, reduce legal and institutional hurdles and optimize surveillance activities. The spatial dispersion of intelligence and surveillance is often claimed as being in response to the globalization of threats.⁵⁹ To recreate the space of cyber surveillance requires the identification of locations at each stage of surveillance, reconnecting locations and keeping track of any changes to them. This may be possible by demanding much greater transparency in each of these stages of surveillance. But the highly dynamic characteristic of state cyber surveillance, such as the rapid advancement of new surveillance technologies and the constantly shifting and evolving relationship with proxies or *ad-hoc* agreements with surveillance partners, pose enormous difficulties to recreate and ascertain the space of surveillance. As the space of surveillance becomes extremely uncertain, the question of “where do I encounter the surveillance authority?” is similarly unfathomable.

c. The manipulation of the time of surveillance

The transformation of the state surveillance apparatus diffuses not only the space but also the time of surveillance. As mentioned previously, digital surveillance takes a series of steps, each step taking place at a different time and space. The remapping of the space of digital surveillance also means the re-joining of different moments or periods to constitute the time of digital surveillance. Therefore, the reconstruction of the time and duration of digital surveillance is as artificial as the reconstruction of its space. Again, an illustrative example is the UK government’s claim that bulk data collection does not amount to bulk surveillance because the collected data will be filtered in the selection stage before being examined. While the argument emphasizes the guarantee of proportionality and necessity in the selection procedure, implicit in the argument is a unilateral imposition of and a very arbitrary creation of the time of surveillance.

⁵⁹ Svendsen, *supra* note 11 at 137.

The creation of the time of surveillance is unilateral because only the surveillance agents who choose from the filtered communications for examination can determine whether the clock starts ticking. It is unilateral also because the selection is a self-serving mechanism dealing with the overabundance of collected data from digital surveillance, which is unilaterally enforced on people in the first place and in its entirety. While the government's claim seems to suggest an identifiable moment of surveillance, it is arbitrary because the selection process involves many uncertainties, as described earlier. Moreover, it is not foreseeable what kind of communications will be deemed important or relevant, separately or combined with other information. The unilateral and arbitrary creation of the time of surveillance is related to what is called the "function creep" of digital surveillance – a situation where the use of data expands beyond the original purpose.⁶⁰

So, the selection and the determination of the intelligence value of data is not a one-time task but one that requires continual re-evaluation. The re-evaluation, such as recombining different datasets and re-matching them with different selection criteria, leads to the construction of a mosaic data profile of the individual. The result of the re-evaluation is unpredictable and unknowable to both the surveilled and the surveillant at the time of the initial collection of data.⁶¹ As the value of collected data are continually re-evaluated and the selection may take place at indefinite moments and use different methods, it is in theory possible to choose any data and determine if they are of some intelligence value at any point. Given the likelihood of selection at any point, it is fair to say that there is not much difference between the indefinite likelihood of surveillance and the permanent existence of surveillance. Ensuring the proportionality and necessity of the selection process, as would be required from a human rights point of view, makes little sense.

d. The post-humanist object of surveillance

The spatial and temporal diffusion of state surveillance deprives individuals of the capacity to initiate and recover an event of human rights encounter with state surveillance agencies by

⁶⁰ van Brakel & De Hert, *supra* note 17 at 179.

⁶¹ It is a common practice in commercial profiling. Companies can produce customer profiles using the data collected by them and can also combine the originally collected data with data bought from data brokers to create new profiles, or just by the data brokers for new profiles for the purpose of advertising. Frank Pasquale, *The black box society: the secret algorithms that control money and information* (Cambridge: Harvard University Press, 2015) at 32.

transforming the very subjectivity of individuals who have been surveilled. Digital surveillance produces and also utilises probabilistic knowledge, and underlying such practices is the post-humanist epistemic presumption that human mind and behaviours are convertible into numbers and digital patterns. This presumption may be scientifically difficult to repudiate,⁶² but when transposed into the operative rationale of state surveillance, it leads to the self-serving idea that the more data collected, the more becomes knowable and known. Strengthening surveillance capacities to hoover up more data becomes the default solution to the failure of crime or risk detection.⁶³ More importantly, what is also different from scientific inquiry of the complete laws of human behaviour is that state surveillance (and also commercial profiling) creates and re-imposes certain facts about people⁶⁴ and that it reproduces individual subjectivity. As will be discussed in more detail later, the creation and re-imposition of “dividual” (our digital representation)⁶⁵, combined with the new temporality of actuarial law enforcement and judicial practices, raise fundamental questions about what constitutes legal subjectivity.

Specific to bulk digital surveillance and the inability to recover a human rights encounter with surveillance agencies, is another important issue that the indefinite spatial and temporal diffusion of state surveillance makes everyone an indefinite object or victim of surveillance at anywhere and anytime. As digital surveillance is based on probabilistic knowledge, being a

⁶² E.g., Alan Turing responds to the argument that humans and machines are different because of the informality of human behaviour: ‘we cannot so easily convince ourselves of the absence of complete laws of behaviour as of complete rules of conduct. The only way we know of for finding such laws is scientific observation, and we certainly know of no circumstances under which we could say, ‘We have searched enough. There are no such laws.’ A M Turing, “Computing Machinery and Intelligence” (1950) 59:236 *Mind* New Ser 433 at 452.

⁶³ E.g., the UK Intelligence and Security Committee of Parliament has asked the GCHQ how useful bulk interception really is. The Committee found that the primary value of bulk interception was in the information associated with the actual content of communications, such as communications data and other information derived from content. The Committee was shown and satisfied that GCHQ’s bulk interception capacity is used primarily to find patterns or characteristics of online communications which indicate involvement in threats to national security. See *Intelligence and Security Committee of Parliament, Privacy and Security: A modern and transparent legal framework* (2015) at 32–33, paras 78–90. The utility of large amounts of data collection and sharing between state surveillance agencies is rarely questioned by human rights courts either. For example, in *Szabó and Vissy v Hungary*, the ECtHR accepted that “[t]he governments’ more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance – a practice, whose usefulness in combating international terrorism is, once again, not open to question...” see *Szabó and Vissy v Hungary*, No 37138/14 (12 January 2016), para 78.

⁶⁴ For example, predictive policing now uses algorithms which gather data about arrests, people’s affiliations, etc. But it is often not clear as to how the algorithms deal with variables such as the racial or ethnic composition of the community and the racial biases in policing and criminal sentencing. This raises serious concern about the amplification or justification of racial discrimination. See Eyal Benvenisti, “Upholding Democracy Amid the Challenges of New Technology: What Role for the Law of Global Governance?” (2018) 29:1 *Eur J Int Law* 9.

⁶⁵ Gilles Deleuze, “Postscript on the Societies of Control” (1992) 59 *October* 3 at 5..

victim of state surveillance also becomes probabilistic. It may be tempting to claim that everyone is a victim when there is permanent surveillance everywhere. Yet, victim is a relational status vis-à-vis not only the perpetrator, but also the people who are less vulnerable and suffer less, are less innocuous, are passive beneficiaries, or are uninterested third parties. While recent scholarship has started questioning the construction of ideal victim in various fields of international law, the critiques do not claim that criteria of victimhood are not necessary; rather they take seriously the issue of victim identification, the social and political construction of the criteria of being a victim and the practical implications on what we should do with international law.⁶⁶ To argue everyone is a victim would nullify the particularity of an event of human rights encounter in which a person can perceive who the oppressor is, and experience what the oppressor commits and make specific claims about his or her rights.

The problem of victim status has been raised in recent surveillance case law. Traditionally, subject to the limited function and authority of judicial bodies, not anyone who is afraid of being subject to surveillance can claim to be a victim before a court. The question is whether and to what extent someone needs to establish that s/he is subject to surveillance measures. One of the most restrictive notions is seen in the US where the claimant should establish that s/he has suffered an injury which is “concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favourable ruling.”⁶⁷ This can be contrasted with the UK RIPA, which established the Investigatory Power Tribunal (IPT) to hear allegations about interception of communication by *any* individuals against the UK intelligence services.⁶⁸ In the European Court of Human Rights (ECtHR), however, it is acknowledged that the applicant could not be reasonably expected to prove that information concerning his or her private life had been compiled and retained. Consequently, if the applicant alleges actual interception of their communications, it is sufficient that the existence of practices permitting secret surveillance be established and that there is a reasonable likelihood that

⁶⁶ E.g. Christine Schwobel-Patel, “Nils Christie’s ‘Ideal Victim’ Applied: From Lions to Swarms”, (5 August 2015), online: *Crit Leg Think* <<http://criticallegalthinking.com/2015/08/05/nils-christies-ideal-victim-applied-from-lions-to-swarms/>>; Christine Schwöbel-Patel, “Spectacle in International Criminal Law: the Fundraising Image of Victimhood” (2016) 4:2 *Lond Rev Int Law* 247; Giuseppe Maglione, “Embodied Victims: An Archaeology of the ‘Ideal Victim’ of Restorative Justice” (2017) 17:4 *Criminol Crim Justice* 401.

⁶⁷ See *Clapper v Amnesty International USA, et al*, 568 US 398 (2013), at 409, para.9.

⁶⁸ *Regulation of Investigatory Powers Act 2000*, *supra* note 2, s65.

information concerning private life is compiled and retained by the security services.⁶⁹ The ECtHR has also considered general complaints about legislation and practice permitting secret surveillance measures without the establishment of reasonable likelihood of specific interception of communications. In the recent *Zakharov* case, the ECtHR harmonised these two parallel approaches.⁷⁰ First, it argued that it will look into the scope of legislation permitting secret surveillance measures and examine whether the applicant can possibly be affected by it. A person can be “affected” by either belonging to a particular group targeted by surveillance legislation or because the legislation simply affects all users of communication services. Second, the ECtHR will examine the availability and effectiveness of domestic remedies. Whether a person can claim to be a victim of secret surveillance measures by the mere existence of surveillance legislation depends on whether effective domestic remedies are available. Thus, the ECtHR fundamentally changed the register of victim constitution: the victim is constructed through potentialities of rights-violation by the state, instead of through evidence of a direct violation.

The harmonization of the two parallel approaches is a departure from the tradition whereby the ECtHR generally speaking denies individuals the right to challenge a law *in abstracto*.⁷¹ As the individualization of both the risk to national security and the surveillance measures used to identify risk, the individualization of victim status also becomes unlikely, as the victim status is increasingly a matter of possibility rather than actuality – the construction of the victim itself becomes a probabilistic and virtual exercise. The ECtHR’s second factor, *i.e.* the availability of remedies at the national level, complicates its position regarding victim status. This second factor should be understood in light of the role of the ECtHR, which is deemed as subsidiary to human rights protections at the national level and the general procedural turn in the ECtHR’s assessment of states’ compliance with the convention.⁷² Therefore, the second factor is

⁶⁹ *Roman Zakharov v Russia*, No 47143/06 (4 December 2015), para 167.

⁷⁰ *Ibid*, para 171

⁷¹ *Kennedy v the United Kingdom*, No 26839/05 (18 May 2010) para 119; *Klass and others v Germany* (1978) ECHR (Ser A) 4, (1980) EHRR 214, para 33.

⁷² L R Helfer, “Redesigning the European Court of Human Rights: Embeddedness as a Deep Structural Principle of the European Human Rights Regime” (2008) 19:1 Eur J Int Law 125; “Procedural Review in European Fundamental Rights Cases edited by Janneke Gerards”, (March 2017), online: [Camb Core </core/books/procedural-review-in-european-fundamental-rights-cases/D7DCBD63D6480F8FA0F1FF91A34062B9>](http://CambCore.com/core/books/procedural-review-in-european-fundamental-rights-cases/D7DCBD63D6480F8FA0F1FF91A34062B9); Oddný Mjöll Arnardóttir, “The ‘procedural turn’ under the European Convention on Human Rights and presumptions of Convention compliance” (2017) 15:1 Int J Const Law 9.

not a standard that can be transposed intact to domestic courts and domestic courts should have their own standard of proof for victim status. Without understanding this point, the UK IPT in the *Human Rights Watch* case, distorting the ECtHR's approach, considered itself as providing effective remedies and required an individual claim to victim status to be able to show that, "due to his personal situation, he is potentially at risk of being subjected to" surveillance measures.⁷³ It therefore substantially limited the victim status that has been recognised by the RIPA.

The US Supreme Court's approach, mentioned earlier, is akin to the recovery of an event of human rights encounter. In seeking "concrete, particularized, and actual or imminent" injury, "fairly traceable to the challenged action" and "redressable by a favourable ruling", this approach tries to identify the spatial, temporal, subjective and material elements of the encounter by asking: whose injury, what is the injury, when and where did it happen (or is it going to happen, how soon), who cause(d) the injury. However, it does not take into account that cyber surveillance has transformed all elements of the encounter and has made them unascertainable. Redress seems to be the ECtHR's approach, which opens the possibility of granting victim status to, "all users of communication services". Arguably, the ECtHR's approach can initiate a judicial review of general surveillance practices and domestic surveillance legislations to access whether they respect basic principles of rule of law and democracy. It is not a redress to recover any specific human rights encounter of surveillance; rather, it acknowledges that the human rights encounter is irrecoverable.

2.2 Encounters with the institutions using surveillance for decision-making

Whereas encounters with surveillance authorities are mediated to the point of elimination in the first two scenarios (targeted surveillance by states' intelligence authorities and bulk data collection by states' intelligence services), the transformation of encounters in scenarios 3 (digital surveillance in law enforcement) and 4 (digital surveillance in the provision of public services) is a bit different. The encounter is not between individuals and surveillance authorities but primarily between individuals with bureaucratic institutions that rely on surveillance for their functioning. The encounter is not completely eliminated in scenarios 3 and 4 when public

⁷³ *Human Rights Watch Inc. et al. v Secretary of State for the Foreign & Commonwealth Office et al.* [2016] UKIPTrib15-165-CH, para 46.

authorities make decisions and impose them on individuals since police still patrol the street and home checks are still carried out to deliver social benefits. But crucial elements of the encounter are transformed, which significantly deepens the power gap between individuals and institutions.

In the legal encounters (or highly legalized encounters) in scenario 3 where digital surveillance is used in the administration of criminal justice, two elements become problematic. The first element relates to the temporality of encounter. While I have discussed previously that bulk surveillance makes the distinction between selected and permanent surveillance meaningless, here I draw attention to the collapse in surveillance-based decision-making of the usual time order from the past to the present and the future by which we experience events. Digital surveillance, as a form of simulation, offers the prospect of acting upon a subject in the present on the basis of what she is likely to do in the future, and that basis takes the form of probabilistic knowledge extracted from her behaviours in the past.⁷⁴ So, what the surveillance acts upon is not exactly the subject at the present time but her or his simulacrum in the future;⁷⁵ and by acting upon the simulacrum, surveillance closes the future and makes the future past.

When law enforcement and the justice system begin to rely on surveillance, the forward-looking-ness of surveillance raises a critical problem about the temporality of law's operation because legal reasoning and judgment are theoretically backward-looking.⁷⁶ based on liberal notions of individual autonomy and dignity and retributive ideology, judicial decisions that would determine the wrongfulness or blameworthiness of an act attribute legal responsibilities and decide punishment traditionally look at what a person has done in a given situation rather than what the person will do.⁷⁷ Certainly, sentencing decisions have long based the judgment on

⁷⁴ Writing about simulation of surveillance as a form of social control, an imaginary of absolute control, an ecstasy of control, William Bogard talked about the temporal orientation: 'Simulation is about the imagination of the "future-past," about projecting a future as something already over, ultimately, about mastery over time (speed and distance) ...' What I describe here is a kind of future "memory" of the technology of surveillance itself, what it "will have been" from the standpoint of its simulation (from the point of view in which the apparatus of surveillance looks back on the 'history' of its perfection as a mode of perceptual control).' William Bogard, *The Simulation of Surveillance: Hypercontrol in Telematic Societies* (Cambridge University Press, 1996) at 34.

⁷⁵ The problem of temporal orientation of simulation is also discussed by Jean Baudrillard, who wrote a series of articles about the Gulf War. The idea is that modern war is all about surveillance and preparation. As the global surveillance of geopolitical events and hyperreal military planning are continuous, a real war becomes just business as usual, a training ground, a simulation of the next war. See Jean Baudrillard, *The Gulf War Did Not Take Place* (Indiana University Press, 1995) at 49–50.

⁷⁶ Ronald Dworkin, *Law's Empire* (Harvard University Press, 1986) at 405.

⁷⁷ The backward-looking-ness is in adjudication in the sense that close attention is paid to what an individual has done in specific situation and is not to be confused with the temporality of judicial reasoning that announces the law.

the likelihood of recidivism, but the crucial decisions about guilt and responsibility are still about past events.⁷⁸ It is not just retributive justice but law's operation in a more general sense, understood as engaging in the distribution of rights and obligations, that deals largely with what has happened, in contrast to administration and governance. Administration and governance engage in the distribution of resources and risks, understandably adopts a more utilitarian and forward-looking perspective.⁷⁹

The second element is about individual subjectivity. As mentioned earlier, in surveillance and profiling, individuals are becoming “dividuals” and multiple simulacra which are implemented by various surveillance actors for different purposes. The digital simulacrum of an individual is created not just by using the information about her or his own traits, preferences and behaviours but also by using group profiles⁸⁰ which are increasingly generated by ubiquitous sensing devices (often non-intrusive) and use machine-learning technologies and algorithms to recognize group patterns.⁸¹ Group profiles are often non-distributive, which means that the properties of group profiles are based on comparisons of people within a group or comparisons of different groups. Hence, while group profiles can apply to individuals as members of the group, individuals do not necessarily have the properties associated with the group profiles.⁸²

In judicial decision making, surveillance and profiling change a fundamental condition of legal subjectivity. Normally, judicial decisions concerning one's rights and obligations are supposed to be individualized decisions based on individualized investigation.⁸³ The corollary to this is individual's right to be heard and right to contest judicial decisions.⁸⁴ If a decision is made primarily by matching an individual with certain patterns or group profiles rather than her or his

The latter engages in the interpretation of legislations or case law which cannot be entirely a backward-looking activity. *Ibid* at 225; Neil MacCormick, *Legal Reasoning and Legal Theory* (Clarendon Press, 1994) at 75.

⁷⁸ Melissa Hamilton, “Adventures in Risk: Predicting Violent and Sexual Recidivism in Sentencing Law” (2015) 47:1 *Ariz State Law J* 1 at 43.

⁷⁹ Robert Stuart Lorch, *Democratic Process and Administrative Law* (Wayne State University Press, 1969) at 26–34; Helmuth Heisler, ed, *Foundations of Social Administration* (London and Basingstoke: Macmillan Press LTD, 1977).

⁸⁰ Mireille Hildebrandt, “Who is Profiling Who? Invisible Visibility” in Serge Gutwirth et al, eds, *Reinventing Data Prot* (Springer, Dordrecht, 2009) 239 at 243.

⁸¹ Angelos Yannopoulos, Vassiliki Andronikou & Theodora Varvarigou, “Behavioural Biometric Profiling and Ambient Intelligence” in Mireille Hildebrandt & Serge Gutwirth, eds, *Profiling Eur Citiz* (Dordrecht: Springer Netherlands, 2008) 89.

⁸² Anton Vedder, “KDD: The challenge to individualism” (1999) 1:4 *Ethics Inf Technol* 275 at 277.

⁸³ Hamilton, *supra* note 78..

⁸⁴ E.g. *International Covenant on Civil and Political Rights*, 19 December 1966, 999 UNTS 171 art14 (entered into force 23 March 1976); *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 UNTS 221 art 6 (entered into force 3 September 1953).

personal situation, the individual concerned will not be able to challenge the validity of information beyond her or his knowledge or control. This is, as we have seen, what was raised in the *Loomis* case. While the Wisconsin Supreme Court held that the trial court's sentencing decision was sufficiently individualized, ubiquitous surveillance and the perceived objectivity of the algorithmic-generated assessment remain fundamentally challenging for a traditional conception of legal subjectivity.

In scenario 4 (digital surveillance in the provision of public services), the human rights encounter with institutions which provide social benefits and administer social resources, the temporality and subjectivity of legal order are of relatively less concern because it is accepted that, unlike the judiciary,⁸⁵ the administration of the welfare state deals with population and distributes resources in a forward-looking, cost-effective way.⁸⁶ But this does not mean that individualized encounter with the institution is irrelevant. Due process rights are equally important in administrative law, which for individuals are central to the process of having an encounter with bureaucratic institutions.⁸⁷ However, the human rights encounter here is also being reconstituted by the deployment of digital surveillance and big data analytics. The most observable change is that when such risk-management tools, believed to be objective, are used for planning various monitoring activities (e.g., patrols, home checks, etc.), the discretion of the street-level officials is considerably reduced.⁸⁸ This suggests a change in decision making from individual professional judgment to algorithm-based judgment that redistributes decisional agency.⁸⁹

Although this change is sometimes celebrated for reducing the impact of individual subjective bias and increasing the transparency of decisions made⁹⁰ (meaning evidence-based),

⁸⁵ Cf. Law and economics consider precisely the opposite that “the judicial process operates as a machine for allocating costs and profits, and for producing cost-benefit calculations.” Alain Supiot, *Governance by numbers: the making of a legal model of allegiance*, translated by Saskia Brown (Oxford; Portland: Hart Publishing, 2017) at 131.

⁸⁶ Lorch, *supra* note 79 at 26–34.

⁸⁷ D J Galligan, *Due Process and Fair Procedures: A Study of Administrative Procedures* (Oxford University Press, 1997).

⁸⁸ Hence, in practice, it is not always welcomed by the street-level bureaucrats especially when risk-management tools can be adapted to monitor their behaviours. Tom Bullock, “Big Data And Bad Cops: Can An Algorithm Predict Police Misconduct? (Part 2)”, (24 August 2016), online: *WFAE* <<https://www.wfae.org/post/big-data-and-bad-cops-can-algorithm-predict-police-misconduct-part-2>>..

⁸⁹ Peeters & Schuilenburg, *supra* note 17; Hamilton, *supra* note 73 at 6–7; Mark Bovens & Stavros Zouridis, “From Street-Level to System-Level Bureaucracies: How Information and Communication Technology is Transforming Administrative Discretion and Constitutional Control” (2002) 62:2 Public Adm Rev 174.

⁹⁰ This is itself a questionable claim because algorithm often incorporates subconscious biases, as mentioned earlier.

human agency in decision-making, in that a professional can reason and explain to others her or his decision, especially to the individual concerned, is a critical aspect of the human rights encounter with bureaucratic institutions. This displacement of human agency raises a serious problem. This is not to say that man-made decisions are necessarily contested in human rights encounters, but that man-made decisions are contestable when they are explained and justified to the others. So, when decisional agency is redistributed in an inexplicable actor-network, not just that of individuals but also of officials or judges who read the report of the risk-management system would often be unable to understand it,⁹¹ not to say that the methodologies used in the programmes are often patented or trade secrets. The inability to understand a decision does not necessarily mean that the decision cannot be challenged; but at least it seriously restricts the means of contestation and resistance.⁹²

3. No face-to-face encounters here: imagery of surveillance and the surveillance-enabled encounter

Having discussed the transformation of the constitutive conditions of the human rights encounter in various scenarios of digital surveillance, I now want to demonstrate the structural relationship between individuals and state authorities deploying digital surveillance by suggesting alternative imageries to that of the face-to-face encounter. Just a quick note, as mentioned earlier, the human rights encounter with institutions is not face-to-face literally, because bureaucratic institutions are supposed to be impersonal and multi-layered entities. But face-to-face encounter provides a way for thinking about the situation of addressing the other and being addressed by the other (the normative significance of this metaphorical face-to-face will be further explored in Chapter 6).

⁹¹ E.g. In a nationally distributed survey in the US about judges' attitudes toward risk assessment tools that predict someone's likelihood of recidivism, some judges were especially ambivalent about the transparency and accuracy of the assessment tools, because they "are often only provided summary information indicating an offender is at low, medium or high risk to reoffend" but often not provided with more detailed and specific information and data needed to target sentencing condition." Jordan Hyatt & Steven L. Chanenson, "The Use of Risk Assessment at Sentencing: Implications for Research and Policy" (2016) Villanova LawPublic Policy Res Pap No2017-1040 at 10.

⁹² For this reason, as will be discussed in the next Part, the European data protection law requires the right to information and human intervention when a decision involves automated processing. EU, *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*, [2016] OJ, L119/1, arts13(2)(f), 14(2)(g) and 15(1)(h).

3.1 Panopticon and hunting

Due to the inherent covert nature of surveillance activities as shown in scenarios one and two, the encounters that happen in surveillance are the opposite of the imagery of face-to-face encounter. We may think of some common imagery of surveillance. One such example is the famous Panopticon designed by Jeremy Bentham. Prison inmates are surveilled and controlled without having direct encounters with the prison guards. Being unable to see the guards in the inspection tower, inmates internalize the control that they are subjected to and change their own behaviours through the mere possibility of being watched. Another image of surveillance is hunting.⁹³ There are two common strategies of predation – pursuit predation and ambush predation; both of them need surveillance for detection and deception.

Encounter still happens in hunting but is diametrically different from the face-to-face encounter we have talked about. Hunting is a unilateral encounter aimed at the avoidance of the dyadic face-to-face encounter. Either the predator observes the tracks of a hiding or fleeing prey, detects a wanted prey among a flock, watches and approaches the prey discreetly, maybe wearing camouflage, and waits for the time to strike; or the prey sees the predator and immediately runs away. A successful escape would require the prey to adopt a certain logic and strategies of the predator, to foresee the pursuit of the predator and to cover its own tracks.⁹⁴ Both the predator and the prey avoid a direct face-to-face encounter. The predator needs to wait for or create the ideal circumstances that ensure a capture. Very often, the predator (or the hunter) uses proxies such as hunting dogs to mediate or even completely eliminate its direct encounter with the prey. The mediation of the encounter by using proxies also ensures that no danger can be posed to the safety of the predator by the prey.⁹⁵ For the prey, avoidance of encounter is of course of deadly importance, as a face-to-face encounter will put an end to the hide and seek game and turn into a life-or-death battle. For both the predator and the prey, the avoidance in

⁹³ E.g. UK government describes a case where bulk interception of communication is used: “[t]he triggering of a manhunt for a known terrorist linked to previous attacks on UK citizens”. See *ibid*, at 50.

⁹⁴ By covering its own traces and predicting the pursuit of the predatory, the prey stops being merely the object of the predator but obtains certain freedom and subjectivity. See Grégoire Chamayou, *Manhunts: A Philosophical History*, translated by Steven Rendall (Princeton University Press, 2012) at 70–71.

⁹⁵ *Ibid* at 67. The mediation of encounter which ensures that the predator never risks his own life is seen in some discourses in the US as being about the benefits of developing and using autonomous weapons and drones for reducing the number of casualties of American soldiers. E.g. Jeremy Seahill, “Find, Fix, Finish”, (15 October 2015), online: *The Intercept* <<https://theintercept.com/drone-papers/find-fix-finish/>>.

hunting is in fact an exercise of power by manipulating time and space or by mimicking the behaviours of the other.

The Panopticon is an image of surveillance within a relatively confined institution, whereas the imagery of hunting seems appropriate as a way to describe surveillance activities when the targets are geographically scattered, mobile and at a distance. Both display the key feature of exercising control by creating certain kinds of dissociation between the surveillance agent and the targeted subject. Distance is created to interrupt or block a direct encounter, and control is made possible precisely because of such dissociation. With the Panopticon, dissociation is produced by the architectural design of the building: the inspection tower at the centre of the building directs a spotlight, so everyone in cells can be clearly seen from the tower but they cannot see the observer inside the inspection tower.⁹⁶ While the Internet as such does not have the central control and the exposure of data and the exposure of physical bodies may generate different reactions from people (e.g., the exposure of data may not lead to the internalization of control which happens in the case of the exposure of physical bodies), the Panopticon is still a useful metaphor. The Snowden Revelations show that states conducting mass surveillance programmes have the capacity and possibility to read any data of any person, even as the surveillance apparatus remains largely in the dark.

In hunting, dissociation is produced either by hiding and camouflage which creates a false sense of distance or, by initiating a different encounter through intermediaries. Deception is evident in the *Jawar Mohammed* case (Scenario 1) and many other cyberattack cases where the messages sent to the target are specifically crafted to interest them and spyware impersonates legitimate websites or software in order to obtain the target's trust. As with intermediaries in hunting encounters, the use of proxies is also especially common in surveillance and the larger field of cyber security.⁹⁷ We have seen individuals or private companies serving as proxies for

⁹⁶ Another example is the case *FBI v Apple* over whether Apple should help the FBI unlock Syed Rizwan Farook's cell phone. The gunman was shot dead in the 2015 San Bernardino mass shooting. It turned out that the FBI paid hackers \$900,000 USD to crack the cell phone. Ellen Nakashima, "FBI paid professional hackers one-time fee to crack San Bernardino iPhone", (12 April 2016), online: <https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html?noredirect=on&utm_term=.9f390be41c63>; CNBC, "Dianne Feinstein reveals FBI paid 900000 to hack into killers iphone", (5 May 2017), online: <<https://www.cnbc.com/2017/05/05/dianne-feinstein-reveals-fbi-paid-900000-to-hack-into-killers-iphone.html>>.

⁹⁷ Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power*, 1st ed (Cambridge University Press, 2018).

governments (as in the *Jawar Mohammed* case) and major internet service providers and global platforms that willingly or unwillingly facilitate the UK and US's bulk data surveillance. These companies rarely admit in public any such arrangements with surveillance agencies and have demonstrated care regarding customer data and privacy, sometimes even openly defying a government's requests, an example being the high-profile case of *Apple v. FBI*. However, acclaimed commitment to protecting customer data and privacy may also be a great camouflage for their intermediary status in encouraging users' trust and continued usage,⁹⁸ which further mediates the unilateral encounter of surveillance agencies with surveilled people.

It is also worth noting the mimetic character of the power relationship in hunting (and hence, surveillance): people who are subject to surveillance or who are afraid of being subjected to surveillance adopt strategies of counter-surveillance and also contribute to the dissociation and avoidance of encounter with surveillance agencies. Except for political activism that directly demands tighter protection of personal data from states, counter-surveillance is largely about hiding, anonymizing, disengaging, and circumventing surveillance rather than directly confronting it.⁹⁹ As mentioned earlier, a prey needs to learn and internalize some of the plans and logics of the predator to successfully flee. It is through this dialectical process of gaining the perspective of the predator and intellectually mastering some of their hunting strategies that a prey stops being a mere object of hunting, develops some freedom and recovers its subjectivity.¹⁰⁰

So, some people who have or can obtain more knowledge about some aspects of digital surveillance, such as the logic used in algorithm-based profiling, can try to "game the algorithm" or even counter-optimize the system of profiling by providing false information, such as

⁹⁸ It is reported that while Apple resisted the FBI's order, it ultimately did submit to the Chinese authorities' security reviews and the requirement to store the users data generated in China on China-based servers. See David Pierson, "While It Defies U.S. Government, Apple Abides by China's Orders — And Reaps Big Rewards", online: *latimes.com* <<http://www.latimes.com/business/technology/la-fi-apple-china-20160226-story.html>>. With the adoption of China's Cybersecurity Law on 1 June 2017, tech companies are required to cooperate with Chinese public security and national security authorities and provide unspecified technical support to the authorities upon request, in addition to the requirement of data localization and security reviews. See *Cybersecurity Law of the People's Republic of China*, 7 November 2016 [*Cybersecurity Law of the People's Republic of China*], articles 23, 28 and 37.

⁹⁹ Lina Dencik, Arne Hintz & Jonathan Cable, "Towards data justice? The ambiguity of anti-surveillance resistance in political activism" (2016) 3:2 Big Data Soc 1.

¹⁰⁰ Chamayou, *supra* note 94 at 70–71.

locations or birthdays, to achieve their desired profiling results.¹⁰¹ However, counter-surveillance practices are necessarily restricted due to the asymmetry of knowledge about the surveillance black box and technological expertise between the surveillance apparatus and those surveilled. For most people, confrontation by way of gaming the system is often not possible and the more common practices of counter-surveillance include taping over laptop cameras and microphones, encrypting communications by using tools such as Virtual Private Network (VPN), or completely quitting services with poor data protection records. The main logic of counter-surveillance, even in the case of falsifying one's information to game the system remains avoidance rather than confrontation, even if such practices entail many inconveniences.

Some research about undocumented immigrants in the US provide an interesting analogy for avoiding encounter. Counterintuitively, undocumented immigrants do not always report fearing deportation, whereas documented immigrants may report being more concerned about deportation.¹⁰² The seeming contradiction between the perception of risks of deportation and the degree of the precariousness of immigration status can be explained by the fact that involvement in the state's immigration system exposes the immigrant, even while granted legal status, to the gaze of the state and the possibility of his or her status being revoked (due to policy changes).¹⁰³ Remaining undocumented offers some sort of invisibility, protection and freedom, which some immigrants weigh as more significant than the rights and benefits provided by the immigration regime to documented immigrants.¹⁰⁴ The analogy made here is about people using strategies of avoidance and creating anonymity and distance as a form of self-protection against the omnipresent state rather than confronting the state and demanding the state fulfil human rights obligations, forgoing state protection at the same time. Again, the difficult problem is that such avoidance in counter-surveillance is radically contrary to the image of human rights encounter (a

¹⁰¹ Lilian Edwards & Michael Veale, "Slave to the Algorithm? Why a 'Right to Explanation' Is Probably Not the Remedy You Are Looking For" (2017) 16:1 Duke Law Technol Rev 19 at 63; Joshua A Kroll et al, "Accountable algorithms" (2017) 165:3 Univ Pa Law Rev 633 at 654.

¹⁰² Asad L Asad & Eva Rosen, "Hiding within racial hierarchies: how undocumented immigrants make residential decisions in an American city" (2018) J Ethn Migr Stud, online: <<https://doi.org/10.1080/1369183X.2018.1532787>>.

¹⁰³ Such uncertainty concerning governmental policy becomes evident in the case where the US Trump Administration declared to end Deferred Action for Childhood Arrivals which had granted certain illegal immigrants work permits and made allegedly 800,000 DACA recipients face deportation. Michael D Shear & Julie Hirschfeld Davis, "Trump Moves to End DACA and Calls on Congress to Act", *N Y Times* (20 January 2018), online: <<https://www.nytimes.com/2017/09/05/us/politics/trump-daca-dreamers-immigration.html>>.

¹⁰⁴ Asad & Rosen, *supra* note 102.

conflictual encounter, for example when individuals subjected to control of police directly challenge and resist police violence). I will revisit the strategies of avoidance and subjectivity of the prey in Chapter 6, to discuss the normative implications of the absence of the human rights encounter.

3.2 From hunting to streamlining a loop

Although the imagery of tracking down and hunting is more specific to people's relationship with surveillance authorities, it is also relevant to the relationship between the individual and the institution which relies on surveillance for its regulatory function. In the case of delivering welfare benefits, a fraudulent recipient is primarily detected through risk scoring rather than home checks and interviews. These street-level, human encounters are still important but become secondary and happen after a risk management system flags a recipient. Hence, technologies of surveillance and data analytics make possible the dissociation between the official and the recipient both temporally and geographically. This dissociation and distance are even more striking when monitoring is planned at the national level where nationwide data mining is conducted or various datasets from municipalities are collected. However, for the individuals concerned, the sense of distance from the institution is false, because as people are datafied and transformed into digital simulacra, they become closely reconnected with monitoring authorities, despite their feeling of isolation from those authorities.

Nevertheless, it seems that an important feature in the transformation of the human rights encounter in scenarios 3 (digital surveillance in law enforcement) and 4 (digital surveillance in the provision of public services) is not quite addressed by the imagery of hunting – that is, the distribution of resources. Risk management that detects crime hotspots and hot time period or rank people's likelihood of recidivism or fraud is essentially about cost-effective distribution of police manpower, judicial resources and other public resources. Hunting as such is insufficient to describe this critical aspect and perhaps more explicit reference to actuarial economics is needed. While this is beyond my capacity and I do not plan to engage with law and economics in this study, I want to draw attention to one extreme case of the automation of the justice system that seems to manifest this type of governance by numbers. The case is about the enforcement of traffic regulations. Over the past three decades, the way traffic offences are dealt with has

gradually moved from their being individually investigated by police officers (and perhaps leading to prosecution for criminal charges), to the automated issuance of fines after a licence plate is recorded by a camera.¹⁰⁵ A person can, of course, dispute a fine with the enforcement authority and hence initiates an encounter with the institution after receiving a fine. But such an encounter is very different from the one where a person can confront a police officer who pulls his or her vehicle over on the spot and ask the officer to make more contextualized and individualized decisions.¹⁰⁶ In most cases, it is observed that people pay fines immediately, in which case no human encounter happens at all and the individual encounter with the institution is minimal.¹⁰⁷ This situation suggests a relationship different from hunting. A supposedly conflictual encounter of law enforcement becomes some sort of a processing machinery which is designed to reduce transaction costs for both individuals subject to it and the law enforcement institution. From an extremely restricted technical perspective, cost-effectiveness for law enforcement means fewer police on the street, more surveillance cameras, more computerized and networked processing of traffic photographs (which are increasingly cheap), and increased compliance with traffic rules by the general public. For people, cost-effectiveness means minimum trouble and time spent dealing with the police. Such streamlining of regulation and compliance suggests, however, a fundamental lack of mutual engagement between the ruler and the ruled in which fundamentally normative questions about efficiency and social costs can be raised and addressed with less mediation or translation by technical experts.

Of course, a large part of the current judicial system has not become an automated processing machinery and human intervention in public administration is still a necessary component.¹⁰⁸ One can also imagine that there could be some resistance from within the judicial

¹⁰⁵ Mark Bovens & Stavros Zouridis, "From Street-Level to System-Level Bureaucracies: How Information and Communication Technology is Transforming Administrative Discretion and Constitutional Control" (2002) 62:2 Public Adm Rev 174 at 179.

¹⁰⁶ The inability to recover an encounter where the alleged traffic offence is committed in a *post facto* encounter with authorities is vividly illustrated in an Argentinian movie, *Relatos Salvajes*.

¹⁰⁷ Bovens & Zouridis, *supra* note 105 at 179.

¹⁰⁸ For example, in the case of traffic law enforcement, some jurisdictions in the US have banned automatic surveillance systems. In Iowa City, an ordinance was adopted in 2013 which prohibits the use of "any automatic traffic surveillance system or device, automatic license plate recognition system or device, or domestic drone system or device for the enforcement of a qualified traffic law violation, unless a peace officer or Parking Enforcement Attendant is present at the scene, witnesses the event, and personally issues the ticket to the alleged violator at the time and location of the vehicle". Lisa Vaas, "Politicians in Iowa City reluctantly pass ban on drones, automatic traffic surveillance", (6 June 2013), online: *Naked Secur* <<https://nakedsecurity.sophos.com/2013/06/06/iowa-ban-drones-traffic-surveillance/>>.

system and public administration against automation, because putting aside fundamental questions about justice and individual rights, automation arguably signifies a power shift from individual professionals to data scientists and programmers.¹⁰⁹ Such an extreme case as shown with the automation of traffic regulation enforcement illustrates the transformation of legal encounters and the streamlining of enforcement and compliance. It is also very useful for understanding and framing questions about what is at stake in the trend towards actuarial justice and actuarial public administration.

4. Summary

In this chapter, I used four scenarios of state digital surveillance to discuss how surveillance transforms individual-institutional encounters. The apparatus of state digital surveillance is described as a highly amorphic Frankenstein creature (different agents and machines are “stitched” together), which accordingly leads to the diffusion of the space and time of surveillance. Digital surveillance also fundamentally changes individual subjectivity. While post-humanist subjectivity has been celebrated by Donna Haraway as liberating, powerful and transgressive,¹¹⁰ what I emphasize is how the opposite can also be true; that is, state surveillance based on the post-humanist presumption can make individuals more controllable and make the control less visible. The growing invisibility of control is then discussed with a few imageries of the surveillance-enabled encounter – i.e., Panopticon, hunting and streamline – which aim to visualize the power structure in the context of state surveillance. These imageries help to highlight the radical lack of mutual engagement in surveillance and the peculiar subjectivation of individuals subjected to surveillance. These features of surveillance will be revisited in Part III.

¹⁰⁹ Jay R Galbraith, “Organizational Design Challenges Resulting From Big Data” (2014) 3:1 J Organ Des 2.

¹¹⁰ Donna Haraway, “A Manifesto for Cyborgs: Science, Technology, and Socialist-Feminism in the 1980s” (1985) 15:2 Social Rev 65.

Chapter 2. Commercial Digital Surveillance and the Loss of the Human Rights Encounter

1. Introduction

In Chapter 1, I demonstrated the features of state-of-the-art surveillance by the state and its elimination of the human rights encounter. As mentioned previously, the state surveillance apparatus relies significantly on and appropriates surveillance and information technologies developed in the private sector. The tremendous surveillance capacities developed by tech companies such as Google are envied by every state security/secret agency. Google's use of big data analytics for generating revenue and profit also epitomises a new business model centred around digital surveillance and data analytics to which everyone is subjected to in quotidian life.

Unlike state secret surveillance, which immediately poses questions about human rights, legality and democracy, commercial data surveillance has, at least before the Cambridge Analytica scandal, often been presented as innocuous and even beneficial as it delivers more customised products and services, saves people time and enhances the consumer experience. It is even believed that commercial data surveillance can improve people's behaviour and lifestyle. For example, people whose data show that they are prone to obesity may receive more healthy-eating ads and gym membership promotions than fast-food restaurant coupons. It seems as long as these data-driven companies deal with data carefully and function as a proper fiduciary, their invasive and disturbing practice can generally be tolerated. There is an increasing body of literature critiquing this new, data-driven business model and its social and political implications. The problem is not only and not primarily about possible data breaches and violation of privacy rights. The problem is also about the structural power imbalance between those who control the data surveillance process and those who are subjected to it. This imbalance is inherent in the activity of social sorting, which leads to customized products and services and more seriously to discriminatory and unjust treatments, affecting everything from insurance premiums to employment opportunities. As discussed in Chapter 1, the transfer of surveillance technology

from the private to the public sectors is very common.¹ In addition, what has been long considered as traditional state functions are now performed by private actors. The impact of power asymmetry in commercial digital surveillance spills over to all aspects of people's private, social and political lives and is also directly related to the transformation of the human rights encounter discussed in Chapter 1.

Some observations made in Chapter 1 regarding the transformation of encounter are also present here: Briefly speaking, in terms of the imagery of surveillance (i.e. avoiding rather than confronting), commercial data surveillance is also in nature unilateral and predatory,² and often covert and deceptive.³ In terms of the transformation of the constitutive conditions of an encounter, commercial digital surveillance also relies on the epistemic presumption that a person's past behaviour has patterns and can be observed and extracted into a form of knowledge based on which decisions can be made, and therefore transforms the subjectivity of those who are subjected to surveillance. In commercial data surveillance, the global value chain of data is perhaps even more complicated and unknown to people whose data are constantly being assembled and reassembled into digital personas. There is a similar transformation in the context of commercial data surveillance that avoids and eliminates the human rights encounter.

It is, however, not sufficient to say that these observable similarities regarding the transformation of the human rights encounter between commercial and governmental surveillance are inherent to the technological characteristics of surveillance. Technology and its application present certain characteristics because of the particular logics leading to their deployment. In Chapter 1, there is a new logic of governance that co-evolves with surveillance

¹ For example, in 2012, the Obama administration launched an initiative of big data research and development worth \$200 million that covered a wide range of matters from health care to energy to defence. The White House, "Obama Administration Unveils 'Big Data' Initiative: Announces \$200 Million in New R&D Investments", (29 March 2012), online: <<https://obamawhitehouse.archives.gov/the-press-office/2015/11/19/release-obama-administration-unveils-big-data-initiative-announces-200>>; Nancy Scola, "Obama, the 'big data' president - The Washington Post", (14 June 2013), online: <https://www.washingtonpost.com/opinions/obama-the-big-data-president/2013/06/14/1d71fe2e-d391-11e2-b05f-3ea3f0e7bb5a_story.html?utm_term=.050d06cc9c61>.

² Shoshana Zuboff describes Google's repeated method of data extraction, as exemplified by its Street View, "[t]his *modus operandi* is that of incursion into undefended private territory until resistance is encountered," and the practices are designed to be undetectable or at least obscure. When encountering resistance, it exhausts its adversaries in court or pay fines that represent a negligible investment for a significant return. Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization" (2015) 30:1 J Inf Technol 75 at 78–79.

³ E.g., Web tracking technologies such as cookies and web beacons are often designed to be invisible and are secretly installed. Company privacy policies that describe the practice of data collection and processing often contain overly ambiguous terms and are often changed without notifying users.

technologies that transform the human rights encounter. In this Chapter, I will re-visit some of the similarities in the transformation of the human rights encounter in light of the more specific characteristics and logics of commercial digital surveillance. It is important to consider the logics of commercial digital surveillance whether one adopts a Marxist based-superstructural theory or not. Because of the complex entanglement between public authorities and private, commercial sector in governing people's socioeconomic and political lives, as well as the de facto domination by a few tech giants that structure and regulate the digitally-mediated world, the deployment of commercial digital surveillance and its specific features subject to some market logics need to be examined.

The power imbalance in commercial digital surveillance co-evolves with a new form of predatory capitalism – what Shoshana Zuboff has called “surveillance capitalism”⁴ (also called “digital surveillance economy”⁵), – and its new logics of accumulation. Drawing on critical studies about the new surveillance-based economy, I will demonstrate how such structural power imbalances underpinned by the new logics of capital accumulation has made impossible the human rights encounter in which people can directly confront data-driven multinational corporations and bring up human rights claims. Hence, the consequence is that any legal and regulatory regimes that maintain an idealized image of the liberal subject and protect privacy and personal data will still be seriously insufficient to address the structural and systemic disempowerment and alienation of people.

Drawing on critical studies of surveillance capitalism, I will look closely into two main aspects of the structural impossibility of the human rights encounter. First, a new form of production (capital input) monetizes the individual's data rather than their labour in the workplace. The monetization and extraction of value are less obvious to individuals and most people do not think they are unpaid by Google or Facebook for their everyday online activities (especially when many of these activities happen in the time and space of leisure and domicile).⁶

⁴ Zuboff, *supra* note 2.

⁵ Mark Andrejevic, “The Big Data Divide” (2014) 8 Int J Commun 1673 at 1678.

⁶ There is a problem with the character of labour people perform on social media. Cf. Andrejevic argues that as markets in personal data become lucrative, people's digitally-mediated, immaterial activities should be acknowledged as economically productive labour, and that the value captured by the companies which control the information-gathering technologies and databases can be considered as a form of exploitation. Mark Andrejevic, “Surveillance in the Digital Enclosure” (2007) 10:4 Commun Rev 295 at 313–315. See also, Doug Laney, “To Facebook You're Worth \$80.95”, (3 May 2012), online: *Wall Str J* <<https://blogs.wsj.com/cio/2012/05/03/to-facebook-youre-worth-80-95/>>.

So, it is quite unlikely that users of internet services would confront the companies of global platforms as workers used to do in sweat factories and demand a fair share of the profits. Second, the value exchange of people's data is between commercial entities (capital output), rather than between companies and people as consumers. This is vividly exemplified in the data broker industry, an industry entirely based on the value extraction and exchange of peoples' data. This process of the value extraction and exchange is the backbone of the digital surveillance economy, but it is shrouded in a great deal of secrecy. In both aspects, people are systematically excluded from the monetization and the value extraction of data, because data production is presented completely as a technological matter and does not engage directly with people who are datafied and surveilled. In addition to this structural exclusion is of course the fact that people are unable to access information and understand the processes of data production and monetization in the digital surveillance economy. Above all, in surveillance capitalism, people are no longer labourers or consumers in the market, but are transformed into raw materials; people as individuals become products of the market. This transformation is profound. In traditional capitalism which is dependent on people's labour and consumption and is hence socially-embedded, people can confront the company and make claims about their socioeconomic and also political rights.⁷ Yet, in surveillance capitalism which largely kicks individuals outside the processes of production and accumulation, people face enormous structural difficulty to initiate encounters with the large scale players of the market.

Going from economic exploration back to the consideration of governance and power, I will show that the change of the two structural factors (capital input and capital output) in surveillance capitalism not only removes conditions for encounter with companies (which are often multinational corporations), but has serious implications for the forms of control and regulation that they exercise. In other words, it is not just that people are unable to confront data-handling companies and contest being alienated from their data and the exploitation of their data; it is also that people become more controllable and in fact controlled by the nudging of the surveillance economy. This control by nudging can also be somewhat easily exported to or imported by public administration and even the administration of justice systems discussed in Chapter 1. In the sense that this new type of control and governance is based on surveillance, it

⁷ Wolfgang Streeck, *Buying Time: The Delayed Crisis of Democratic Capitalism* (Verso, 2014) at 14–16; Steven Lukes, *Moral Conflict and Politics* (Oxford: Clarendon Press, 1991) at 175.

does not quite matter whether it is public authority or private companies which conduct surveillance. The transformation of critical conditions of encounter by the logic of surveillance capitalism can provide a new perspective for understanding the transformation of encounter discussed in Chapter 1, even if one does not accept Marxist base-superstructure theory.

2. The logic of surveillance capitalism and the impossibility of encounter

2.1 Google's story

It is itself an interesting paradox that many digital economy initiatives started with some measure of anti-capitalist, social-oriented or egalitarian ethos, with the aim of increasing social and economic inclusivity, encouraging innovation, sustainable development, and of improving the quality of life. Nevertheless, the current default form of digital economy – “surveillance capitalism” – exhibits serious democratic and human rights deficits in its logic and structure. To understand better how the default form came into being, it is necessary to make a detour briefly to Google's discovery of its basic formula which laid down the basics for surveillance capitalism.

For any of the early internet start-ups which subscribed to the visions of early cyber liberalism, surviving under the increasing pressure of making profits in the market was a daunting task. In its early days, Google was against the search model funded by advertisers and considered it “inherently biased towards the advertisers and away from the needs of the consumers”.⁸ Its solution was an algorithm by which a search result would be ranked according to its importance to users rather than advertiser funding.⁹ The problem was that if Google continued to offer a user-facing web browser only, then simply generating better search results would not produce profits, because users' value would be depleted once Google improved search results for its users. As Zuboff describes, it would be a self-contained circle in which value generated by users was reinvested to improve users' experience and nothing was left to be turned into capital.¹⁰

⁸ Sergey Brin & Lawrence Page, “The Anatomy of A Large-Scale Hypertextual Web Search Engine” (1998) 30:1–7 *Comput Netw ISDN Syst* 107.

⁹ *Ibid.*

¹⁰ Shoshana Zuboff, “Google as a Fortune Teller: The Secrets of Surveillance Capitalism”, *FAZNET* (3 May 2016), online: <<http://www.faz.net/1.4103616>>.

The shift Google made then was to capitalize users' data with a different advertising model that, like a matchmaker, provided ads that could be useful, interesting and informative for users. In early 2002, Google launched its AdWords advertising service. It was designed as an auction system where advertisers bid for slots on search result pages to show their ads. Every time a query was made in Google web search, Google ran an auction. Advertisers bid on a price for each time a user clicked on the ad when queries using specific keywords were made. However, slots for ads were not given to advertisers based on their auction bid. Matchmaking needs to be accompanied by quality control – to ensure that the ads are true and high-calibre matches for users' searches.¹¹ This was done with the help of Google's sophisticated analytical tools that measured (1) the quality of the landing page for an ad, (2) the relevance of the ad to the search terms or keywords, and above all, (3) the percentage of times users actually click on a given ad which appeared on a result page.¹² The latter two factors were largely based on analyses of users' behavioural data which Google already held in great quantity, and therefore matchmaking as such did not create additional cost for Google. The ad rank would then be determined by multiplying an advertiser's bid with real-time evaluation of these three factors related to ad quality, and slots would be given based on the ad rank.¹³

An additional innovation of Google's ad auction was that the winner of each auction would pay the amount bid by the advertiser with the next-highest offer.¹⁴ The principle is that the winner would pay the minimum amount necessary to maintain its position.¹⁵ Combining the bid price with the quality score of the ad, Google's Chief Economist Hal Varian illustrated how to determine the amount that advertiser actually had to pay to Google with a simple equation: $P_1 = \frac{b_2 \times Q_2}{Q_1}$ (P_1 is the actual price that advertiser no.1 pays; Q_1 is its quality score; b_2 is the second-highest offer compared with the offer of advertiser no.1; Q_2 is the quality score of the advertiser

¹¹ Steven Levy, "Secret of Googlenomics: Data-Fueled Recipe Brews Profitability", *Wired* (22 May 2009), online: <<https://www.wired.com/2009/05/nep-googlenomics/>>.

¹² *Ibid*; "Using Quality Score to Guide Optimisations: Google Best Practices", online: *Google Ads Help* <<https://support.google.com/google-ads/answer/6167123>>.

¹³ note 12.

¹⁴ Levy, *supra* note 11.

¹⁵ Hal Varian, *Introduction to the Google Ad Auction*, online: <https://www.youtube.com/watch?time_continue=355&v=a8qQXLby4PY>.

with the second-highest offer). As the equation shows, if the quality score of advertiser no.1 increases, they would pay less.¹⁶

Hence, Google has created an ecosystem that makes the advertisers, the users and Google all happy. The ads are no longer annoying but rather, useful and relevant to the users; the advertisers get their ads through to the targeted audience, and as the relevance and clicks of their ads increase, their cost decreases; Google is content as it has found a sustainable means of generating revenue and profit. The more Google is used, the more users' data Google collects, and the better matching it can do, which leads to more usage, and so on. This shift by Google rediscovered the value of users' data, which allowed it to re-pay their investors and also gave rise to the surveillance-based big data business model that recognizes consumer patterns, predicts future consumer behaviours and makes decisions based on identified patterns and predictions. As the business grew, Google's data source has gone far beyond users' web searches and has extended to wearable technology, surveillance cameras, drones, satellites and other sensors in smart machines. The rapid expansion of its surveillance programmes at a global scale forces people in different societies to buy in Google's world vision, which is described as "infrastructure imperialism" by Siva Vaidhyanathan.¹⁷

Google's story is a text-book example of business model revolution. Before becoming Google's Chief Economist since 2002, Hal Varian taught at the business school at University of California, Berkeley and co-authored with Carl Shapiro a popular business school textbook on information economy.¹⁸ In it, they argued that while information overload would lead to scarcity of customer attention, the internet had the potentials to direct customer attention and match it with suppliers,¹⁹ an idea also seen in Bill Gate's frictionless capitalism.²⁰ The strategy of personalized and targeted advertising and the principle of customer analysis were paramount and would be much easier to implement with internet technologies.²¹ Google has carried out these

¹⁶ *Ibid.*

¹⁷ Siva Vaidhyanathan, *The Googlization of Everything: (And Why We Should Worry)* (University of California Press, 2012) at 109.

¹⁸ Carl Shapiro & Hal Varian, *Information Rules: A Strategic Guide to the Network Economy* (Harvard Business Press, 1998).

¹⁹ *Ibid* at 6–9.

²⁰ Bill Gates, Nathan Myhrvold & Peter Rinearson, *The Road Ahead* (New York: Penguin Books, 1996) at 181 ("Internet will extend the electronic marketplace and become the ultimate go-between, the universal middlemen.").

²¹ Shapiro & Varian, *supra* note 18 at 35–36. Similarly, Bill Gates had envisioned that advertisers access customers would not happen through billing and registration but by "software agents" which persuade customers to fill out a

ideas successfully. But the underlying principle is that people's attention is valuable and can be traded for revenue, profit and market-share and organized with business partners.

Therefore, in rediscovering the value of users' data, Google has also dragged users to a complicated market mechanism where people, once transformed into data and digital patterns, are not players in a relationship of value exchange but, as many critics have observed, are Google's products and assets.²² The concept of human rights is alien to and incompatible with the picture of this business model. This deep normative fault line was expressed in Varian's business textbook which claimed that marketing strategies should "bribe" and "induce" users to give them information.²³ Indeed, Google often treats human rights concerns raised against its surveillance and datafication programs as merely a technical issue, avoiding genuine rights discussions. This is seen in the Google Street View example,²⁴ mentioned in the introductory chapter. In countries which prohibit taking pictures of people without their permission, Google's solution of blurring people's faces and license plate numbers upon individual request avoids the questions such as why surveillance cameras can be installed in the first place and why Google can assume its conception of privacy and free speech can operate worldwide.

2.2 Structural impediments of the human rights encounter in surveillance capitalism
Google's change from operating a user-facing, self-sufficient circle to a tripartite profit-making ecosystem is described by Zuboff as the discovery of the "behavioural surplus"²⁵ which has profoundly changed the economy. The importance of user behavioural and environmental information goes beyond sales and marketing to basically every aspect of business practices from research and development of products to supply chain management.²⁶ In the big data era,

questionnaire that, "might include all sorts of images in an effort to draw subtle reactions out of you (customers). Your agent might make the process fun by giving you feedback on how you compare with other people." Gates, Myhrvold & Rinearson, *supra* note 20 at 191.

²² E.g. Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads* (Knopf Doubleday Publishing Group, 2017); Pernille Tranberg & Steffan Heuer, *Fake It: Your Online Identity Is Worth Gold. Guide to Digital Self Defense* (Art People, 2012).

²³ Shapiro & Varian, *supra* note 18 at 35–36.

²⁴ *Ibid* at 99–111.

²⁵ Zuboff, *supra* note 10.

²⁶ For the use of big data in business sectors, see survey: PwC, "In which areas are you using big data analytics today? In which additional areas will your company use data analytics in five years?", (2016), online: *Statista* <<https://www.statista.com/statistics/549712/worldwide-survey-use-of-data-analytics-by-business-area/>>.

which is often characterised by 3Vs – high volume, velocity and variety²⁷ – the challenge, then, is to find out useful information among overly abundant information and get value from it.²⁸ The notion of big data also claims to solve the challenge of data explosion: big data not only means large datasets or collection and consolidation of data from different sources, but also refers to the advanced techniques of data processing, analysing and sense-making, specifically to find patterns and correlations in the data.²⁹

More importantly, big data allows for the recognition of un-anticipatable and persistent patterns or correlations,³⁰ based on which marketing decisions can be made that create an edge over the competitors in the market. Un-anticipatable, because the patterns or correlations can hardly be explained or understood with reason. Persistent, because it seems objectively discerned by big data. As the promise of big data is precisely about discerning un-anticipatable patterns for exploiting niche markets, the technology begs for more data, and the data can be structured, semi-structured or unstructured from various sources.³¹ The logic is self-fulfilling and self-stimulating: the more data is available, the more we know about the world (except knowing here does not equate to comprehension), and the better decisions we make. It requires and legitimises ever more pervasive and invasive surveillance. Big data, initially applied in physical sciences, has become a mantra for the private sector as well as government agencies. Surveys also show a steady increase of the big data market size and revenue at a global level, which is projected to reach \$103 billion by 2027,³² and increasing investments in advanced analytics and big data initiatives in enterprises.³³

²⁷ E.g. Paul Zikopoulos et al, *Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data* (McGraw-Hill, 2011) at 5.

²⁸ E.g. Jacobs argues that the pathologies of big data are primarily those of analysis. Adam Jacobs, “The pathologies of big data” (2009) 52:8 *Commun ACM* 36 at 39.

²⁹ danah boyd & Kate Crawford, “Critical Questions for Big Data: Provocations for a cultural, technological, and scholarly phenomenon” (2012) 15:5 *Inf Commun Soc* 662 at 663; Svetlana Sicular, “Gartner’s Big Data Definition Consists of Three Parts, Not to Be Confused with Three ‘V’s”, (27 March 2013), online: *Forbes* <<https://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/#6106aeca42f6>>.

³⁰ Andrejevic, *supra* note 5; boyd & Crawford, *supra* note 30 at 668.

³¹ Zikopoulos et al, *supra* note 28 at 16.

³² Wikibon SliconANGLE, “Forecast of Big Data market size, based on revenue, from 2011 to 2027 (in billion U.S. dollars)”, online: *Statista* <<https://www.statista.com/statistics/254266/global-big-data-market-forecast/>>.

³³ *Big Data Business Impact: Achieving Business Results through Innovation and Disruption* (New Vantage Partners LLC, 2017).

Like many technological breakthroughs, big data has generated considerable enthusiasm in the business sector. It is commonly described as the “new oil” or “new gold mines”.³⁴ Combined with terms such “data mining”, they create a misleading impression that data already exist and wait to be gathered. In fact, unlike gas or rare earth, data are artificially created in a largely unilateral, covert and often predatory way. The creation of data requires putting in place surveillance devices and analytical programs around people’s living environment and offering people the services, sometimes for free, which monitor and track their behaviours often without the knowledge and consent of the people being monitored. The creation of data, thus, is not only a conversion of people and their lives into data whose meaning can be decoded by digital semiotics. It also transforms people from consumers into “human natural resources” that are capitalizable.³⁵

One structural barrier of the human rights encounter is caused by the new means of production and especially the artificiality and enclosure of the production of data and people’s digital personas. While we may think of information such as email as our own creation, data about such information is simultaneously generated by us using programs and devices to write and send emails. This data is not naturally owned by people but produced by the technologies owned by the companies who claim title of (often expressed in its terms of use) and capitalise the data. People have little knowledge and control over the process in which such data and their digital personas are generated. In this sense, there is a critical transformation of conditions of encounter: the collection of people’s data is different from, say, taking away a farmer’s land,³⁶ a classic example of Marxist “accumulation by dispossession”.³⁷ In the latter case, the farmer is deprived of his or her means of production by a forceful transfer of the titles to the exiting assets in a specific event of encounter with the land grabbing company or state. In the former, data and their value are artificially created and reified by tech companies in the first place, and people

³⁴ E.g. Klaus Schwab et al, *Personal Data: The Emergence of a New Asset Class* (World Economic Forum, 2011).

³⁵ Zuboff, *supra* note 10.

³⁶ Cf. Andrejevic, *supra* note 6. Andrejevic describes the privatization of information resources and databases as “digital enclosure”, which prevents people from accessing their personal data, and argues that digital enclosure parallels the historic land enclosure movements in England that separated producers from the means of production.

³⁷ Cf. Jim Thatcher, David O’Sullivan & Dillon Mahmoudi, “Data colonialism through accumulation by dispossession: New metaphors for daily data” (2016) 34:6 *Environ Plan Soc Space* 990. Thatcher et al. apply David Harvey’s notion of “accumulation by dispossession”, which theorizes the continuation and proliferation of primitive accumulation in contemporary global capitalism to the big data economy which “colonializes” everyday life. But unlike “everyday life”, which people own and presumably have control of, both data and the title of data are fabricated by companies which develop and control information technologies.

have never possessed it as tangible or intangible property and never had a say in the production of data. There is no encounter of dispossession or deprivation insofar as such an encounter presumes pre-established ownership over pre-existing asset,³⁸ because when people use their services, the data generated from the activity are simultaneously collected by service providers. If people reject the terms of use and refuse to use the services or devices, their data will not be created at all and hence cannot be owned by anyone. This paradox manifests one critical condition of structural impediment – the asymmetry of control over the information infrastructure and digital technologies which prevents people from making human rights-based claims over their data in the big data economy.

Just a quick note here: that people are excluded from the data production process also makes the post-humanist subjectivity – whether we call it cyborg or dividual – problematic. It is tempting to consider individual subjectivity in a hyper-connected and digitised world should include the digitalized form of existence of individuals. For example, my digital persona on Facebook should be considered as part of me. However, the constitution of the digital persona is a process of representation of which the means owned and controlled by the tech companies. Hence, my dividual subjectivity is again mediated and I either am not aware of the mediation or have no control of it. To recall Chapter 1, post-humanist subjectivity in the context of ubiquitous surveillance could be more controllable.

To come back to the problem of metaphor. The commonly used metaphors are misleading in another way. Oil and gold cannot be reused and reproduced, and dusts and dirt have absolutely no value and are simply discarded. With big data technology, data can be repurposed, recombined, repackaged and reused multiple times, and therefore retained indefinitely, for the discovery of unknown patterns and there is no definite exhaustion of data's value. The non-exhaustibility of the value of data demonstrates its artificial and speculative characteristics. As will be seen shortly, these features are also the reason that the data broker industry has been so lucrative. Here again, people are structurally excluded from the process of the creation and monetization of data.

³⁸ E.g. Maurice Dobb, *Studies in the development of capitalism* (International Publishers, 1964) at 178. [“...when one speaks of accumulation in an historical sense, one must be referring to the ownership of assets, and to a transfer of ownership, and not to the quantity of tangible instruments of production in existence.”]

Interestingly, there is meanwhile another commonly used term that sounds precisely the opposite to the metaphors of new oil and new gold mines. The raw, unstructured data used in big data analysis is also often called “data exhaust”. They are the data generated as by-products from people’s digitally mediated activities, such as files generated by web browsers, cookies, log files, etc. Once analysed, they can reveal detailed information about a person’s habits and preferences.³⁹ With the big data enthusiasm, there is no shortage of tutorials in the popular press about how to turn data exhaust into a competitive edge.⁴⁰ The problem with the term “data exhaust” is not just that it is ironic. Zuboff compares it with terms such as “heathens,” “infidels” “primitive” and “vassals” that labelled the lands of North America in the time of colonization. These are “ideological filters” which put the objects of extraction and monetization outside moral consideration and make such activities less contestable.⁴¹ “Data exhaust,” therefore, is a problematic term not only because it is misleading with respect to the value of the data. More importantly, it suggests that the big data economy is entirely a technological matter and therefore politically and socially neutral. Before the discovery of behavioural surplus, the term may have been appropriate to describe the early state of the data analytics and technologies when purely user-facing services did not utilise the by-product data. But over time, as such by-product data generates surplus values, “data exhaust” creates a discursive and conceptual barrier to the questioning of the implications of the big data economy on people’s lives from political, moral and human rights perspectives.

The problem with the commonly used metaphors and terms related to big data analytics are symptomatic of the self-fulfilling and totalising logic of the digital surveillance economy. The logic subjects every person and every aspect of human life to the mythical representation and superimposition of data and renders them commercially exploitable, excluding people’s active engagement from the process of data production and manipulation. By serving people’s present preferences and fabricating people’s future needs, the totalising loop also reconstitutes

³⁹ E.g. Pierre Laperdrix, Walter Rudametkin & Benoit Baudry, *Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints* (San Jose, CA: IEEE, 2016).

⁴⁰ E.g. Tim McGuire, James Manyika & Michael Chui, “Why Big Data is the new competitive advantage •”, (August 2012), online: <<https://iveybusinessjournal.com/publication/why-big-data-is-the-new-competitive-advantage/>>; Dave O’Donovan, *Harnessing the Data Exhaust Stream: Changing the Way the Insurance Game is Played* (Accenture, 2016).

⁴¹ Zuboff, *supra* note 10; Zuboff, *supra* note 2 at 79.

individual subjectivities and social relations that fit into the logic of value extraction and accumulation of the digital surveillance economy.

Moreover, the belief in data-driven knowledge production displaces other forms of knowledge and other methods of learning, experimenting and theorizing. For example, Chris Anderson proclaimed, “the end of theory”, in the age of big data.⁴² In business practices, this means that the surveillance-based data-driven model expels other non-data-driven, non-techno-fundamentalist business practices and the exploration of those practices that do not preclude the participation of people. As the technology is quite easy to be transposed to the public sector and as the private sector has been performing many significant public functions, it is important to critique the business model from the more normative and broader perspectives of democratic legitimacy and human rights – e.g., the right of access to information, the notion of information self-determination and the right to participate in political and public affairs.

2.3 The example of the data broker industry and the structural barriers of the human rights encounter

In the digital surveillance economy, artificially created data and people’s digital personas in a largely enclosed fashion mediate the relationship between companies and people. Such mediation prevents people from encountering the parties with whom their value is exchanged and converts people into the raw materials and products of the data-driven companies. The structural asymmetry and commodification of people are exacerbated by the data broker industry which is completely divorced from people’s labour and consumption and therefore does not need people’s active engagement at all. Data broker companies collect information about people from various sources, process it and sell it to their client companies for a variety of purposes. In 2013, the *Financial Times* created a calculator to determine the dollar value of a person’s personal data

⁴² Chris Anderson, “The End of Theory: The Data Deluge Makes the Scientific Method Obsolete”, (23 June 2008), online: *WIRED* <<https://www.wired.com/2008/06/pb-theory/>>. [“This is a world where massive amounts of data and applied mathematics replace every other tool that might be brought to bear. Out with every theory of human behaviour, from linguistics to sociology. Forget taxonomy, ontology, and psychology. Who knows what people do what they do? The point is they do it, and we can track and measure it with unprecedented fidelity. With enough data, the numbers speak for themselves.”]

and it suggested that average person's data are often sold for less than a dollar.⁴³ With the big data hype and the internet of things, more data are made available and collected by companies which package them into valued products.⁴⁴ The business of data broker has become a multibillion-dollar industry and the market size is expected to continue expanding significantly in the coming years.⁴⁵

The data broker industry is almost completely non-people facing. Starting with the data acquisition, data broker companies typically do not acquire people's data from direct interaction with people themselves.⁴⁶ According to a report made by the US Federal Trade Commission on nine major data brokers in 2014, the sources of data fall into three categories: (1) government sources, such as the US Census Bureau which provides demographic and geographic information of a particular area; (2) other publicly available sources, including telephone and other directories, press reports, and information posted on the internet; and (3) commercial sources, such as retailers and catalogue companies, registration websites, and financial service companies that offer detailed transaction-specific consumer data.⁴⁷ Data broker companies acquire data by buying them from companies, government agencies or other data brokers, trawling public information such as court records and census data, and running programs – the so-called web

⁴³ Emily Steel, "Financial worth of data comes in at under a penny a piece", (12 June 2013), online: *Financ Times* <<https://www.ft.com/content/3cb056c6-d343-11e2-b3ff-00144feab7de>>; Emily Steel et al, "How much is your personal data worth?", (12 June 2013), online: <<https://ig.ft.com/how-much-is-your-personal-data-worth/>>.

⁴⁴ E.g., Acxiom, one of the largest data broker companies, claimed to retain over 3,000 pieces of information for nearly every adult consumer in the US, provide multi-sourced insight into approximately 700 million consumers worldwide, and manage over 15,000 databases and process about 13 trillion transaction per quarter for clients. See *Acxiom Corporation Annual Report 2014* (Acxiom, 2014) at 8.

⁴⁵ E.g., According to a market study done by Transparency Market Research, the compound annual growth rate of the global data market will increase by 11.5% between 2017 to 2026. The pay-per-use paid segment is expected to surpass a market valuation of \$163,802.3 million by 2026. Transparency Market Research, "Data Broker Market is expected to surge at 11.5% CAGR between 2017 & 2026 - TMR", (7 December 2017), online: *GlobeNewswire News Room* <<http://globenewswire.com/news-release/2017/12/07/1247221/0/en/Data-Broker-Market-is-expected-to-surge-at-11-5-CAGR-between-2017-2026-TMR.html>>.

⁴⁶ According to a report on the data broker industry by the US Senate Commerce Committee in 2013, some data brokers obtain information directly from consumers through online and offline marketing surveys, such as warranty cards and sweepstakes entries which ask detailed questions about household, demographics, income levels, shopping preference and other personal matters. The surveys disclose to consumers that the information they provide may be shared for marketing purposes, but the surveys generally do not indicate that they are affiliated with a specific data broker. Office of Oversight and Investigations Majority Staff, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, Staff Report for Chairman Rockefeller (Committee on Commerce, Science, and Transportation, 2013) at 18.

⁴⁷ Edith Ramirez et al, *Data Brokers: A Call for Transparency and Accountability* (Federal Trade Commission, 2014) at 11–15. See also, Office of Oversight and Investigations Majority Staff, *supra* note 47 at 15–21.

crawlers – to systematically browse and capture data on the internet.⁴⁸ Data brokers and their data sources often have contractual relationships that determine the ownership of the data, its use for a defined time period and the right to resell the data. Rarely do those contracts contain provisions requiring the company which gathers and holds consumer data to notify the consumers of the sharing of the data or to provide consumers with the choice to opt out, not to mention to obtain consumers’ prior consent to such use of their data.⁴⁹

Once acquired, data is developed into various products to be sold to the client companies for marketing and other purposes such as identity verification and fraud detection. Products can be both the actual, raw, unstructured data from data sources or processed data, such as that inferred from raw data and structured data segments. Structured data segments can be categories of people who are shown by raw and derived data elements to display similar characteristics, or predictive patterns such as scoring of consumer behaviour based on the data of a subset of consumers. The structured data segments are highly attractive and valued in the market because they are the most informative for decision-making or can be put directly into marketing practices. Data broker companies such as Acxiom are investing heavily in data analytics that can infer missing information, derive insights and form models for prediction.⁵⁰

Data brokers have an interest in ensuring the quality of the data products, since inaccurate data and poorly inferred data or digital patterns may lead to wasted marketing expenses which could cause complaints from their client companies or even the loss of clients. Quality control of data products does not mean people can have access to their data, correct wrong or inaccurate information about them, or opt out of the use or sharing of their information. People rarely have such opportunities to engage in data production. The exception is credit bureaus. Under the US Fair Credit Reporting Act, people have the right to inspect their records and demand

⁴⁸ Ramirez et al, *supra* note 48 at 17; Matthew Crain, “The limits of transparency: Data brokers and commodification” (2018) 20:1 New Media Soc 88 at 90.

⁴⁹ Ramirez et al, *supra* note 48 at 16–17.

⁵⁰ E.g., in Acxiom’s 2017 annual report, it observes that with the explosion of data, most client companies are unable to derive valuable information regarding their business and the market and it is increasingly difficult to attribute marketing expenditures to a measurable outcome. Wasted marketing spending is caused by the fragmented ecosystem of brands, data providers, marketing applications, media providers and agencies involved in the marketing process but operate without cohesion. See *Acxiom Corporation Annual Report 2017* (Acxiom, 2017) at 6.

corrections,⁵¹ although in practice it remains very difficult to actually get the records corrected.⁵² Since the Act was passed in 1970, most businesses in the current data broker industry are not covered by the Act and even the data products may strongly resemble credit scorings.

More importantly, unlike credit bureaus and credit scoring, the existence and business activities of most data broker companies are invisible and unknown to consumers. Even companies which allow consumers to access their information or opt out of the use of their information, usually display such options in the privacy policy on their website,⁵³ people cannot effectively exercise their rights as long as they do not know these companies are using and benefiting from their information.⁵⁴ Moreover, individually verifying the accuracy of consumer data matters little for the purpose of quality control of the data broker company's products because they are dealing with massive amount of raw data, derived data and data segments. The solution to the issue of data quality is once again technical, and hence feeds back again to the self-serving logic of totalization: investing in advanced analytical programmes and enlarging databases for validating the data and deriving inferences.⁵⁵

Clients of data brokers include a wide range of enterprises such as financial services, insurance, retail, healthcare, travel, information and communication services, as well as government and the non-profit sector. As data brokers seek to maintain long-term relationships with client companies and clients seek more informative data to enhance their business, the client companies are also often the data sources for data brokers by way of cooperative arrangements.⁵⁶ Hence, the data broker industry creates an ever-expanding loop that benefits both data brokers and their source/client companies. People (as consumers or labour) are totalized and become human natural resources to support the self-reproducing loop.

⁵¹ *Fair Credit Reporting Act*, 15 USC §1681 (1970).

⁵² Frank Pasquale, *The black box society: the secret algorithms that control money and information* (Cambridge: Harvard University Press, 2015) at 22–23.

⁵³ E.g., Ramirez et al, *supra* note 48 at 42–43.

⁵⁴ There is a similar problem in state surveillance due to the covert and unilateral characteristics of surveillance practices. The accessibility of domestic surveillance law is questionable when people are not made to know about the existence of secret surveillance. See Part II, Chapter 3(1).

⁵⁵ E.g., Acxiom offers its Audience Solutions products to client companies to validate the accuracy of their data. It includes InfoBase, which contains 1,500 demographic, socio-economic and lifestyle data elements and thousands of predicative models, and AbiliTec which is an identity resolution technology that helps client companies recognize individuals and households using different input variables and connect identities online and offline. See note 51 at 9.

⁵⁶ Office of Oversight and Investigations Majority Staff, *supra* note 47 at 16.

This loop puts a number of barriers into the structural difficulties of the human rights encounter in the digital surveillance economy. Whereas Google and Facebook’s data surveillance activities have been made known for some time and they have encountered some resistance from the public,⁵⁷ the data broker industry has largely remained invisible to people. The available governmental investigative reports so far show how difficult it is to probe into the “dark underside” of the data-driven economy,⁵⁸ and the task of confronting the data brokers is more formidable for individuals. Collective action is possible. In November 2018, over 50 individuals’ access requests were gathered by an NGO – Privacy International – which launched complaints against seven major data brokers before data protection authorities in the UK, Ireland and France. It remains however, that to reveal the full picture of data broker activities and to establish detailed violations of people’s privacy and data protection rights is extremely challenging and perhaps beyond the capacity of even the best-resourced civil society groups.⁵⁹

The black box characteristics of the data broker industry resemble those of the state intelligence liaisons discussed in the previous section, in the sense that both cite the laws that grant them considerable secrecy. Whereas for state intelligence liaisons, surveillance agencies rely on national security clauses and “third-party rule” (discussed in Chapter 3) to prevent public scrutiny,⁶⁰ data brokers claim that their sources of data and client identities are their proprietary

⁵⁷ E.g. Electronic Privacy Information Center & Consumer Privacy Organizations, *Letter to Federal Trade Commission, Re: How tech companies nudge users to choose less privacy-friendly options* (2018), online: <<https://thepublicvoice.org/wp-content/uploads/2018/06/FTC-letter-Deceived-by-Design.pdf>>; EPIC, *In re: Facebook, Inc. Internet Tracking Litigation* (Electronic Privacy Information Center, 2018), online: <<https://www.epic.org/amicus/facebook/davis/>>.

⁵⁸ Katy Bachman, “Senate Commerce Report Says Data Brokers ‘Operate Behind a Veil of Secrecy’”, (18 December 2013), online: *Adweek* <<https://www.adweek.com/digital/senate-commerce-report-says-data-brokers-operate-behind-veil-secrecy-154579/>>.

⁵⁹ Privacy International requests the data protection authorities of these three countries to conduct a full investigation over the activities of the seven data broker companies and also any necessary further investigations that will protect individuals from wide-scale and systemic infringement of the EU GDPR. This means that as the Privacy International requests, the data protection authorities not only investigate these specific companies, but also, “take action in respect of other relevant actors in these industries and their practices.” Privacy International, *Submission to the Information Commissioner: Request for an Assessment Notice of Data Brokers Acxiom & Oracle* (2018), para 4; Privacy International, *Submission to the Information Commissioner: Request for an Assessment Notice of Data Brokers Experian & Equifax* (2018), para 4; Privacy International, *Submission to the Information Commissioner: Request for an Assessment Notice / Complaint of AdTech Data Brokers Criteo, Quantcast and Tapad* (2018), para 6.

⁶⁰ The third-party rule, also known as the principle of originator control, underpins foreign intelligence cooperation. It is the rule that information shared with foreign intelligence service or government should not be transmitted to third parties (domestic or foreign) without the prior permission of the service which originally shared the information. Aidan Wills & Hans Born, “International Intelligence Cooperation and Accountability: Formidable Challenges and Imperfect Solutions” in Hans Born, Ian Leigh & Aidan Wills, eds, *Intell Coop Account* (Routledge, 2011) 277 at 283.

information or are confidential according to the provisions of their contracts and hence, protected by trade secret laws.⁶¹ Such secrecy contributes to the opacity and complexity of the value chain of the data broker industry and also increases the degree of separation between sellers and buyers at different points along the value chain, making it impossible for anyone to draw a full picture about the institutional processes of data production and monetization in the data broker market.

The complexity of the value chain is also the result of the techno-fundamentalist approach to the problems of data explosion and quality discrepancies. As mentioned previously, the production of data and people's digital personas is very much a self-enclosed process where individuals are neither consulted nor informed. Data brokers often patent their in-house-developed analytical programs or use patented programs licensed by third parties, and claim intellectual property rights over the processed data products to disable any efforts of uncovering analytical processes.⁶² Apart from being covered by trade secret laws, data analytical tools create additional veils to the industry because advanced data processing broadens the distance between the data products and data's empirical sources. Processed information such as probabilistic predictions may be acquired through complicated algorithmic determinations which use multi-layer neural networks that can become unexplainable and incomprehensible even to their own designers,⁶³ not to mention consumers who do not have the technical expertise. Meanwhile, as these advanced analytical tools are used by data brokers precisely as a solution for missing or inconsistent data, these computationally inferred data do not have their empirical sources.⁶⁴ These inferred data are put in algorithms with other raw or processed data elements to generate more data segments and patterns. The technologically-enabled data production process circumvents actual interactions with individuals who are what the data are supposed to signify. People have no access to and cannot understand, let alone question, the technologically mediated process of data production, the purposes data products serve and the condition under which they will be used.

The opacity of the data broker industry – the structural complexity and the technological secrecy of the data value chain – causes great difficulties for people to encounter data brokers

⁶¹ Office of Oversight and Investigations Majority Staff, *supra* note 47 at 12–13.

⁶² E.g., note 51 at 23–24.

⁶³ Reuben Binns et al, “*It’s Reducing a Human Being to a Percentage*”: *Perceptions of Justice in Algorithmic Decisions* (ACM Press, 2018) at 2.

⁶⁴ Crain, *supra* note 49 at 94.

and to reverse-engineer the processes by which they have been datafied into products and their value is extracted by the market. To summarise the above discussion on the lack of the human rights encounter in the surveillance economy, then, we can just imagine the situation in which someone gets to peek into the maze-like data broker industry: I receive an ad that gets me seriously wrong (e.g. age, gender, occupation, etc.). Out of curiosity or anger, I send an inquiry to the sender of the ad, requiring them to delist me and asking how they have got my name. The sender may or may not reply to say where they purchased their mailing list. If lucky enough I will obtain the name of the entity that sold the sender the mailing list and I can go to ask this entity how it accessed my name to add to the list. The entity may not respond or may tell me they bought the list from yet another entity. So, I end up in either a cul-de-sac or a wild goose chase.

If I am told by a company that it collects my information because it assumes that I have consented to the data collection according to its privacy policy displayed in their website, I can withdraw my consent and demand to opt out. If I ask the company who else it has shared or sold my information to, it may or may not respond, and I end up in a similar wild goose chase. If I am finally told by a company that they have computationally generated the mailing list and the methodology is a trade secret, I tell them their sloppy algorithm has made mistakes about me. My complaint becomes a reason for the company to keep gathering more data, investing and using data analytics to improve the quality of products. Consequently, I remain stuck in the totalising loop of the digital surveillance economy; in the process of trying to reclaim my subjectivity, I have actually reinforced the surveillance that objectifies me.

3. From customized service to control by nudging

The example of the data broker industry illustrates the non-people-facing characteristics of surveillance capitalism. The means of production of surveillance capitalism include surveillance technologies, big data analytics and machine-learning programs, which convert people and the living environment into data products bearing commercial values. Individuals are largely excluded from the processes of generating data and data products and their monetization not least because lack of knowledge and consent, but also because the whole process of valuation is tremendously different from traditional capitalism and can dispense with peoples' active engagement (both as labour input or consumers).

This one-sided control over the means of production by a handful of tech giants, the market which trades in people's future behaviours and the easy technology transfer to the public sector has serious consequences for individual subjectivity, human rights and democracy. One way of connecting the new logic of the surveillance capitalism with the transformation of governance and regulation discussed in Chapter 1 is to highlight the unidirectional nature of the power relations. Whether it is targeted advertising or predictive policing, private and public institutions calculate and make decisions about people's future behaviours and act on those decisions, largely bypassing individualized encounters. Digital surveillance amplifies institutional capacities and enables new ways for institutions to make decisions and to insert control over people's lives.

There is another way of drawing a connection between surveillance capitalism and the transformation of regulation. The reason that the surveillance-based business model has been so powerful and become the default model of the current digital economy is partly the convenience it offers to consumers. The personalization of services, often for free, is widely celebrated because it gives people a sense of empowerment and control. The sense of empowerment and control, however, can be exactly a consequence of deliberate calculation, manipulation and concealment of actual power relations. Borrowing terms from nudge theory, the personalization of services works by giving someone a specific "choice architecture". The choice architecture is designed to make individuals behave "in a predictable way without forbidding any options or significantly changing their economic incentives".⁶⁵ Again, Google provides an example of the nudge in the highly surveilled, networked and computerized environment. The order of results presented from a Google web search is to direct, without forcing, people's clicks in a way that will increase the value of Google's sponsored advertising space.⁶⁶ Here, although it seems the individual who does a Google web search is exercising his or her decisional autonomy when deciding which link to click, the exercise of autonomy is in the context of a highly flexible and adaptable choice architecture which has already optimised the choices so that the person will make a decision as guided and preferred by Google. This is a very subtle way of control: unlike those cases when control is directly inserted by an authority informed by digital surveillance,

⁶⁵ Richard H Thaler, *Nudge: Improving Decisions about Health, Wealth and Happiness* (Yale University Press, 2008) at 6.

⁶⁶ Karen Yeung, "Hypernudge": Big Data as a mode of regulation by design" (2017) 20:1 Inf Commun Soc 118 at 121.

here digital surveillance is used to create a choice environment and to guide individuals to make decisions about themselves without coercion and prohibition.

Nudge as strategy is key to the surveillance capitalism which makes the market of future behaviour profitable. A company that predicts and nudges people's choices obtains competitive advantage in the market.⁶⁷ Nudging is also a highly powerful tool in governance and regulation because it is presented as non-coercive which lets people decide for themselves. It is also very much compatible with neoliberal ideologies concerning governance and individual autonomy. Then, of course, the critical question becomes what the choice architecture is and who gets to design and impose the choice architecture. This question is important not only for the general public but also for bureaucratic professionals who are themselves increasingly dependent on machines for their work in a context where bureaucratic logic increasingly mimics that of the market. As discussed in Chapter 1, the deployment of digital surveillance in the functioning of public authorities could signify a power shift from traditional bureaucratic professionals to data scientists. For bureaucratic professionals to maintain their discretionary power, to exercise their professional judgement and correct biases ingrained in the data collection and data analysis programs, it is necessary to know how the design of the programme conditions their choices. The tricky issue is that the choice architecture, just like other forms of surveillance, works when it is not revealed because the choice architecture is often about creating and utilising the subconscious factors that influence the decision.⁶⁸ Once it is subject to public deliberation and scrutiny, it is unlikely to be effective anymore. For the bureaucrats who reclaim their control within the institution, it would be less a problem that they game the system. However, in the larger scale of governance by nudging, of making people behave in a preferred direction, the nudge is meant to be unspeakable. Governance by nudging therefore has essentially the same element of secrecy at its core and shares with the imagery of hunting the same elements of deception, camouflage and manipulation of the environment to seduce the target. Unlike hunting, nudging does not end up in a violent confrontation. This is precisely the power of secrecy of both

⁶⁷ However, this could also raise the question about the sustainability of such competitive advantage. As more and more companies and industries adopt the new logic of surveillance capitalism, one could argue (in a way similar to Marx predicting the end of capitalism) that behavioral surplus would be depleted at some point and there would be no competitive advantage in one's prediction of people's future behaviour. This perhaps could become one internal contradiction of surveillance capitalism.

⁶⁸ Yeung, *supra* note 67 at 126.

the objectives and exercise of control in governance by nudging which eliminates the human rights encounter.

The logic and means of production in surveillance capitalism can be transposed to governance in at least two ways: first, by enhancing the capacity of institutions to predict or pre-empt individuals' behaviours and therefore enlarging the pre-existing power asymmetry between institutions and individuals when they encounter each other; second, creating the choice environment for individuals so that they behave in a predictable way and therefore avoiding the encounter which used to be necessary for enforcing regulatory decisions. Both ways of transposition raise challenges for human rights, democracy, bureaucratic accountability and the rule of law, but the challenges are manifested differently. In the first case of transposition, problems arise when technologies make wrong predictions about people, e.g. giving higher risk scores for fraud because the algorithm is biased and hence causes unjust and unfair treatment. In the second case, the problems are precisely the opposite; that is, the predictions are correct because people are conditioned to behave as predicted. The algorithm does not so much predict as it shapes – although that is also the source of its optimal prediction. It is hard to say which one is more damning, but at least it seems that the second situation is even more unnoticeable and its impact more profound.

4. Wrapping up

Following the double-inscription of the Frankenstein myth, Chapters 1 and 2 examined the first-inscription – the elimination of the human rights encounter by the deployment of digital surveillance by state authorities and private entities. The technologies of surveillance and big data analytics exhibit huge potential for control in advance and at-a-distance, which amplifies the capacity of the state intelligence and law enforcement services and also enables more streamlined administration of public resources including the judicial system, and the provision of public services. These technologies further enable the industrial revolution of the 21st century and help generate enormous economic values.

At the same time, the potential of these technologies for doing harm is significant. Digital surveillance technologies make possible (1) the bypassing of existing legal framework that regulates state intelligence and law enforcement activities, (2) the displacement of decisional

discretion and authority from bureaucratic professionals which makes decisions incomprehensible and unaccountable, (3) the reinforcement of existing biases and prejudices against particular individuals or groups of individuals which are rebranded as evidence-based and objective, and (4) the bypassing of existing privacy laws that are premised on individual autonomy and self-determination by manipulating the subconscious factors that influence one's choice.

Underlying these actual and potential social harms of surveillance technologies are more fundamental challenges to the conditions of the human rights encounter. Deployed by and co-evolving with the new logic of governance and surveillance capitalism, digital surveillance not only enlarges the power asymmetry between surveillance authority and the target of surveillance but also profoundly reconfigures the power structure by producing actionable⁶⁹ “knowledge” and transforming individual subjectivity, the character of ruling (i.e., the temporality and spatiality of control), compliance and resistance. In addition to these changes is the fact that the technologies of digital surveillance are largely monopolized by a few big brothers and a handful of digital service providers.

Although these profound challenges have been raised by an increasing body of critical scholarship, as will be seen in Part II, the current regulatory frameworks addressing the problems of surveillance still frame the problem in a very narrow way. Formal legality, transparency and bureaucratic accountability are the main focus of the mainstream approach. This is especially the case when it comes to policy and law making where different and even conflicting interests are reformulated as mutually compatible precisely by invoking formal legality, transparency and bureaucratic accountability. These are no doubt important questions, as demonstrated here in Part I, and policy and legal interventions following this way of problem-framing could potentially lead to incremental improvements. These questions, nevertheless, can also be dealt in a way that further contributes to the elimination of the human rights encounter, essentially re-inscribing the problem that it seeks to tackle.

⁶⁹ Sheila Jasanoff describes actionable information as that which both can be perceived by people and demands, “interrogation, explanation, or resolution.” Sheila Jasanoff, “Virtual, visible, and actionable: Data assemblages and the sightlines of justice” (2017) 4:2 Big Data Soc 1 at 1.

Part II

The Frankenstein Myth Part 2: Regulating Digital Surveillance

Part II proceeds to the re-inscription of the Frankenstein myth and turns to current major regulatory frameworks addressing the challenges raised by digital surveillance as discussed in Part I. As seen in Part I, the deployment of digital surveillance has gradually become a necessary component of a new logic of governance and the capitalist economy and has posed serious questions to the conventional understanding and practice of individual rights, democratic participation and the rule of law. I have also discussed these challenges as the transformation to the point of elimination of the human rights encounter. As mentioned already, these challenges are symptoms of the intrinsic covert nature and power asymmetry of digital surveillance. It seems natural, then, to address the issue of secrecy and abuse of power by requiring a clearer legal basis for digital surveillance and more procedural guarantees to ensure the legality and institutional accountability for surveillance activities. Currently, most solutions follow such an approach of opening the black box of secret digital surveillance for public and, above all, judicial scrutiny. As Justice Louis D. Brandeis said, “Sunlight is said to be the best of disinfectants.”¹

This approach of framing the problem as a matter of legality, transparency and accountability is underpinned by basic natural justice values and theories about the rule of law and liberal democracy. Its focus on institutional accountability-building is also supported by the fact that the realization of individual rights is conditioned by the systemic power asymmetry in digital surveillance. Chapter 3 will discuss many valuable legal interventions and initiatives following this general approach, some incremental and some quite ambitious, to tame digital surveillance. Many of them push for the provision of clearer and more detailed legal basis and procedural requirements for state and commercial digital surveillance. They also work to create organizational and social conditions and legal avenues to help individuals exercise their informational self-determination and due process rights.

As will be seen in Chapter 4 however, this approach, which is supposed to be deeply embedded in values for justice and human dignity, risks being considerably skimmed in practice, only paying lip service to those values. More fundamentally, the risk can be attributed to the positivist, reductive account of law, seeing law as merely an instrument to deal with the social effects of digital surveillance and to tame the monster of digital surveillance by (micro)managing its deployment. Such an instrumentalist understanding of law creates problems for law itself,

¹ Louis D Brandeis, *Other People's Money and How the Bankers Use It* (New York: Cosimo, Inc., 2009) at 62.

especially when the law-making process exhibits serious fault lines between different interest groups and the law is devised to satisfy fundamentally conflicting interests.

In Part II, Chapter 3 will first provide an overview of the mainstream regulatory approaches for state and commercial digital surveillance. I will look into both positive legal regimes and scholarly discussions on regulating state digital surveillance and commercial digital surveillance. In Chapter 4, I will proceed to a critical analysis, demonstrating some difficult ambivalences and contradictions in the current regulatory regimes and discourses. The analysis will especially problematize the flattening of the rule of law principle into formal legalism, the increasing bureaucratization in the major regulatory frameworks and will point out some potential ways of reinforcing the lack of the human rights encounter in digital surveillance.

Chapter 3. A Sketch of the Regulatory Regimes for Digital Surveillance

1. Regulatory mechanisms for state digital surveillance

This section will be divided into two parts, roughly following the discussion of different scenarios of state digital surveillance in Chapter 1. The first part specifically deals with bulk surveillance programs and corresponding human rights legal responses. The second part moves to the regulatory regimes for less high-profile but equally significant surveillance practices involved in state policing operations and judicial decision-making. In the first part, the problem identified in the mainstream regulatory responses is not quite the absence of law which has led to the violation of human rights and the abuse of power by state surveillance authorities, but how extant legal framework for state surveillance can be manipulated and even corrupt. The sense of lacking legal framework is more explicit in the second part, as the use of surveillance in law enforcement is presented as something indeed novel. Whether it is the lack of legal framework or the corruption of existing law, mainstream responses in both contexts exhibit a strong demand for legal intervention, with a strong tendency of proceduralization, to save law itself from the abuse of power as well as new logic of surveillance-based governing.

1.1 Bulk digital surveillance programs

1.1.1 Problem framing

As seen in Chapter 1, many of the state surveillance programs were put in place, expanded and reinforced in the era of global war on terror. The human rights problems caused by state surveillance activities were, hence, part of the larger problem of ensuring human rights in counterterrorism. Accordingly, they have been raised and considered years before the Snowden Revelations. In the international human rights regime, two reports by the special procedures of the UN Human Rights Council are particularly important. One was by Martin Scheinin, then Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, issued in 2009. Scheinin's report pointed out that the ever-expanding power of state surveillance in counterterrorism had a "profound, chilling effect" on fundamental

human rights and urged governments to articulate in detail how their surveillance policies uphold the principles of proportionality and necessity and what measures have been taken to prevent and punish abuse.¹ The other report was by Frank La Rue, then Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, issued in 2013, about two months before the Snowden leaks.² It also specifically addressed the implications of state surveillance of communications for the exercise of the right to privacy and the freedom of expression. The observations in La Rue's report of the different methods of communications surveillance, and its analysis of risks posed by the surveillance to individual rights to privacy and freedom of expression, and of the insufficient domestic legislations and judicial scrutiny have been repeatedly endorsed and relied on in many post-Snowden reports and judgments concerning state surveillance.

After the 2013 Snowden Revelations, Germany and Brazil, the two “victim” countries of the US global mass surveillance programs, pushed the adoption of a resolution by the UN General Assembly entitled “The Right to Privacy in the Digital Age”.³ The resolution emphasized that, “unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the rights to privacy and freedom of expression and may contradict the tenets of a democratic society”, and expressed the deep concern, at “the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights”.⁴ Upon the request of this resolution, the UN High Commissioner for Human Rights published a study on the right to privacy in the context of domestic and extraterritorial surveillance.⁵ Among other things, the study relied on Human Rights Committee's general comment no.27 and case law of the European Court of Human Rights regarding limitations on fundamental freedoms and stressed

¹ Martin Scheini, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, 13th Sess, UN Doc A/HRC/13/37 (2009).

² Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 23 Sess, UN Doc A/HRC/23/40 (2013).

³ *The Right to Privacy in the Digital Age*, GA Res 68/167, UNGAOR, 68 Sess, UN Doc A/RES/68/167 (2013).

⁴ *Ibid.*

⁵ Office of the High Commissioner for Human Rights, *The Right to Privacy in the Digital Age: Report of the OHCHR*, UNHRC, 27th Sess, UN Doc A/HRC/27/37 (2014).

that, “the relationship between right and restriction, between norm and exception, must not be reversed”, and that:

Mass or ‘bulk’ surveillance may ... be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate.⁶

In 2015, the Human Rights Council appointed a new Special Rapporteur on the right to privacy,⁷ Joseph Cannataci, who started his mandate by focusing on state surveillance legislation and practices. In his 2017 annual report, the Special Rapporteur specifically criticised so-called “gesture politics” by which politicians who wish to be seen to be doing something about security play the “fear card” and legalise intrusive surveillance measures without demonstrating that this is either a proportionate or an effective way to tackle terrorism.⁸

The regional human rights bodies in Europe have been even more active in addressing state mass surveillance. The Parliamentary Assembly of the Council of Europe, the European Commission for Democracy through Law (the Venice Commission) and the Commissioner for Human Rights have issued new or updated statements and resolutions strongly critical of state surveillance and intelligence liaisons.⁹ Similarly, the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) have decided a number of cases on state surveillance. In the recent case *Szabó and Vissy v. Hungary* at the ECtHR for instance, the concerns over the intrusiveness of state surveillance on a massive scale are vividly expressed by Judge Pinto de Albuquerque in *Szabó and Vissy v. Hungary* who insisted that “the vitrification of

⁶ *Ibid*, at 9, para 25

⁷ *The right to privacy in the digital age*, HRC Res 28/16, UNHRC, 28 Sess, UN Doc A/HRC/RES/28/16 (2015).

⁸ Joseph Cannataci, *Report of the Special Rapporteur on the right to privacy*, 34 Sess, UN Doc A/HRC/35/60 (2017), at 13-14, para. 42.

⁹ E.g. Council of Europe PA, Resolution No 2045, *Mass Surveillance*, 2nd part Sess, Texts Adopted (2015); Council of Europe, European Commission for Democracy Through Law (Venice Commission), *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*, 102nd Plen Sess, CDL-AD (2015) 006.

society brings with it the Orwellian nightmare of 1984”.¹⁰ The CJEU has been increasingly operating like a human rights court when dealing with data protection. In the *Tele 2 Sverige* case, which concerned the Swedish and British legislations that required telecommunication providers to retain traffic data in bulk in order to make that data available to national authorities, the CJEU held that the interference entailed by such legislations in the right to privacy and freedom of expression was “very far-reaching” and “particularly serious”.¹¹ The CJEU also held that the objective of finding organised crime and terrorism, however fundamental it may be, could not, “in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purpose of that fight”.¹²

In each of these responses to state digital surveillance, while human rights are often invoked as a baseline to constrain the activities of state surveillance,¹³ the responses soon move to focus on the state’s legislative framework and the accountability mechanisms for digital surveillance. Such an approach – focusing on the legality and accountability of state surveillance rather than arguing over the exact substance and scope of the rights itself – is hardly surprising given that these fundamental freedoms themselves, under international human rights law, allow for limitations, provided that the imposition of the limitations fulfils certain legal requirements. Ensuring the legality and accountability of the limitations on these rights is hence integrated into the protection and realization of these rights. Moreover, the exact nature and content of the right to privacy have always been subject to controversies¹⁴ and the uncertainty of the substance of the

¹⁰ Judge Pinto De Albuquerque, Concurring Opinion, *Szabó and Vissy v Hungary*, No 37138/14 (12 January 2016), at 60, para 22.

¹¹ *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*, Joined Cases C-203/15 and C-698/15, [2016] ECLI:EU:C:2016:970, para 100.

¹² *Ibid*, para. 103.

¹³ For example, La Rue’s 2011 report recognized that internet vastly expanded the capacity of individuals to enjoy their right to freedom of opinion and expression which is an “enabler” of other human rights. It is also endorsed in many UN documents that rights held by people offline must also be protected online. La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UNHRC, 17th Sess, UN Doc A/HRC/17/27 (2011), para 67; GA Res 68/167, *supra* note 4, para 3; *The Right to Privacy in the Digital Age*, *supra* note 6, para 5.

¹⁴ Oliver Diggelmann & Maria Nicole Cleis, “How the Right to Privacy Became a Human Right” (2014) 14:3 Human Rights Law Review 441; Toby Mendel et al, *Global survey on internet privacy and freedom of expression* (UNESCO, 2012) at 51; Joseph Cannataci, *Report of the Special Rapporteur on the right to privacy*, 31st sess, UN Doc A/HRC/31/64 (2016), at 8-9, paras 19-21.

right seems to be exacerbated by the rapid change of communication technologies.¹⁵ So, it seems indeed more practical to not indulge in a complex and culturally specific conception of the substance of rights but to instead emphasize the formal requirements limiting restrictions on these rights as a set of basic human rights obligations of states.

There is one rare case in which the substance of the right to privacy was reconsidered and amplified by the modern telecommunication technologies in the context of state surveillance. The capture of communications data is considered as also amounting to an interference with privacy. As the CJEU has observed, this data, “taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained.”¹⁶ In other words, a certain understanding of data informed a new conception of privacy – rather than the contours of privacy being taken more or less for granted and the issue then swiftly moving on to limitations analysis. Apart from this special case where the technical feature of digital surveillance has made a difference to the substance of the right to privacy, the main focus and primary task of the mainstream approach to regulating state surveillance remains to establish legal basis and accountability mechanisms for state surveillance and to ensure that the imposition of limitations on human rights is consistent with the legal requirements set out in human rights law.

However, this is not to say that state surveillance activities have always been in legal vacuum and therefore need to be legalized. While the lack of domestic legal regimes for state surveillance may be true for some states which do not have a developed legal system, the state surveillance apparatus is often legally constituted and entrusted with specific mandates as seen in Chapter 1. It may be especially the case that states with wide-ranging surveillance capacities have more detailed surveillance regulations to separate the power and coordinate the functions of different surveillance agencies. Human rights requirements and rule of law principles could have been incorporated in these legal regimes in the first place, rather than added as an afterthought. But as mentioned in Chapter 1, it is often that state surveillance activities happen regardless of the extant law, by taking advantage of certain aspects of the legal regime, or by bypassing the

¹⁵ La Rue, *supra* note 3, para 22 [“The rapid and monumental changes to communications and information technologies experienced in recent decades have also irreversibly affected our understandings of the boundaries between private and public spheres.”].

¹⁶ *Digital Rights Ireland Ltd v. Minister for Communications and Others*, Joined Cases C-293/12 and C-594/12, [2014] ECLI:EU:C:2014:238, paras 26-27. See also La Rue, *supra* note 3, para 15.

extant law with the help of new technologies. So, the problem of undermining democracy and corrupting the rule of law is not just due to the secrecy and arbitrariness of surveillance activities as such, but more importantly about how the secrecy and arbitrariness are made possible under the extant domestic and international legal frameworks themselves.

Accordingly, the common regulatory reactions to state surveillance consider the major legality and accountability deficits as arising from the legally-sanctioned secrecy of intelligence activities and intelligence cooperation. Legally-sanctioned secrecy is often expressed in several ways. First, surveillance collects intelligence for national security and foreign relations, which are traditionally within executive power based on the doctrine of separation of power. As a result, domestic courts, respecting the limitations on their jurisdictions, tend to be reluctant to question such activities when national security ground is invoked by the government.¹⁷ The legally-sanctioned secrecy over national security and foreign relations also hampers the access to information by domestic oversight bodies, especially regarding the sources of intelligence and methods of obtaining the information. As mentioned in Chapter 1, state surveillance agencies often share or obtain intelligence information from partner surveillance agencies, and the liaison often takes the form of the so-called, “arrangements below the waterline”¹⁸, and therefore have no basis in legal agreement. This means that the scrutiny over such arrangements between surveillance agencies of different states cannot go through the usual parliamentary procedures by which international treaties are deliberated and given effect domestically.

Specific domestic oversight procedures are also unlikely to succeed due to the so-called third-party rule. This rule prevents the sharing of information with third-parties without the permission of the information’s supplier agency. Oversight bodies, no matter international or domestic, judicial or non-judicial, are considered “third-parties”.¹⁹ Although the third-party rule applies to foreign intelligence cooperation and may not have legal effect outside the intelligence

¹⁷ Dider Bigo et al, *National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges*, Study for the LIBE Committee (Directorate-General for Internal Policies, Policy Department C: Citizens’ Rights and Constitutional Affairs, European Parliament, 2014).

¹⁸ As mentioned in Chapter 4, judicial oversight over such arrangements are unlikely. The UK Investigatory Powers Tribunal described such arrangements as “too confidential and sensitive for discussion in open court in the interests of preserving national security.” *Liberty and others v GCHQ and others* [2014] UKIPTrib 13_77-H, para 7.

¹⁹ Aidan Wills & Hans Born, “International Intelligence Cooperation and Accountability: Formidable Challenges and Imperfect Solutions” in Hans Born, Ian Leigh & Aidan Wills, eds, *International Intelligence Cooperation and Accountability* (Routledge, 2011) 277 at 283.

community, national legislations often effectively recognize it when defining the mandate of oversight bodies.²⁰

Besides the legally-sanctioned secrecy traditionally given to state surveillance, the circumvention of the existing legal frameworks governing state surveillance by the surveillance agencies exploiting both the law and new technologies is another major problem. Such encroachment and corruption of the legal system and the rule of law could be more alarming and damaging than the mere non-existence of law. As discussed in Chapter 1, the spatial diffusion of state digital surveillance makes meaningless the territorially-based distinction between internal and external communications, which may be subject to two different sets of legal regulations. The surveillance agencies can avail themselves of a much looser legal regime, as seen in the example of UK government's interpretation of external communications in Chapter 1.

The two situations – legally-sanctioned secrecy and circumvention of existing law – show that it is not enough to bring the state surveillance under the realm of law. It is, instead, necessary to figure out the conditions leading to corruption of the extant legal frameworks themselves in light of the technological and institutional development of state surveillance. In all these ways of problem framing (*i.e.*, seeing the problem of state surveillance as lack of legal regulation, or as enabled by a particular form of legal regulation, or as enabled by perverting the extant legal framework), the focus is on the state institutions. Such framing has also determined the approach of problem solving, *i.e.*, rescuing the legal frameworks for state surveillance from corruption and improving democratic accountability and legality to re-establish the state-individual equilibrium.

²⁰ E.g., In Hungary, the National Security Committee of the Parliament oversees the activities of the anti-terrorist organ with the limitation that the Committee, “may not learn of information which might endanger the prime importance of national security interests in protecting the methods and sources (participating persons) relied on in the case at issue”. The Ombudsman examines law enforcement organs including the anti-terrorist organ, also with the limitation that, “the report made on the examination of the secret intelligence activities of the authorities authorised for using secret intelligence devices and methods may not contain data from which the secret intelligence gathering activities carried out by the organ in the case at issue can be inferred.” *Szabó and Vissy v Hungary*, No 37138/14 (12 January 2016), paras 114-119, 121.

1.1.2 Problem solving

Naturally, mainstream solutions for these accountability deficits of state surveillance mostly coalesce around the establishment or re-clarification of the legal framework that sets out the conditions of surveillance activities and their supervision, the creation of special and independent oversight bodies and procedures to ensure that surveillance is not illegal or abusive, and the provision of effective remedies to victims of state surveillance. More detailed requirements about the establishment and the quality of the law as well as the oversight procedures and the domestic remedies are developed by human rights bodies, notably the ECtHR in recent surveillance case law drawing from substantial jurisprudence concerning the lawful limitations on fundamental freedoms.

As for the existence and the quality of the law, it is commonly described as the requirement of being “in accordance with the law”. Under the jurisprudence of the ECtHR, it is necessary not only that surveillance measures find some basis in domestic law, but also that the domestic legislations are compatible with the rule of law, which means the law must be adequately accessible and foreseeable to affected individuals. The requirement of accessibility and foreseeability means the legislation should be formulated with sufficient precision regarding the scope of discretion of the authorities and the manner of its exercise, so that the individual can regulate his or her conduct.²¹ In the context of secret surveillance, the ECtHR conceded that foreseeability cannot mean that an individual should be able to foresee when the authorities are likely to intercept his or her communications so as to adapt his or her conduct accordingly.²² Domestic legislations should nevertheless, be of sufficient clarity to give citizens an adequate indication as to the circumstances and the conditions in which public authorities are empowered to resort to surveillance measures.²³ In *Weber and Saravia v. Germany*, the ECtHR developed minimum safeguards that should be set out in statute law to avoid the abuse of power. The statute

²¹ *S and Marper v the United Kingdom*, No 30562/04 [2008] V ECHR 167, para 95. Similarly, the UN Human Rights Committee considered that the laws should be sufficiently clear with respect to the circumstances in which the right to privacy would be interfered and specify the body that is authorised to take surveillance measures. Human Rights Committee, *General Comment 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 32nd Sess, (1988), para 8. This is also endorsed by the Special Rapporteur Frank La Rue in his 2011 report. La Rue, *supra* note 14, paras 58, 83.

²² *Roman Zakharov v Russia*, No 47143/06 (4 December 2015), para 229; *Malone v the United Kingdom*, No 8691/79 [1984] ECHR10, 7 EHRR 14, para 67; *Rotaru v Romania*, No 28341/95 [2000] V ECHR109, para 55; *Weber and Saravia v Germany*, No 54934/00 [2006] XI ECHR 1173, para 93; *Kennedy v the United Kingdom*, No 26839/05 (18 May 2010) para 152.

²³ *Kennedy v the United Kingdom*, *ibid*.

law should (i) contain clear and detailed rules that identify the nature of the offences which may give rise to an interception;²⁴ (ii) provide a definition of the categories of people liable to have their communications intercepted; (iii) set out a limit on the duration of interception, (iv) the procedure to be followed for examining, using and storing the data obtained, (v) the precautions to be taken when communicating the data to other parties, and (vi) the circumstances in which recordings may or must be destroyed.²⁵

The quality of supervision of secret surveillance is closely connected to the effectiveness of the remedies. As for the nature of the oversight bodies, the ECtHR does not preclude the possibility of the oversight by non-judicial authority with sufficient independence from the executive.²⁶ Oversight procedures may take the form of *ex ante* independent judicial authorisations or *post factum* judicial oversight.²⁷ For the authorisation of secret surveillance, the ECtHR further requires that the authorisation authority must be capable of verifying the existence of, “a reasonable suspicion”,²⁸ against the person concerned. *Post factual* oversight bodies, judicial or non-judicial, should also be independent of the executive, have the competence to examine the complaints about surveillance activities, make binding decisions and grant appropriate relief.²⁹ These requirements need not be fulfilled by a single oversight body,

²⁴ *Kennedy v the United Kingdom*, *ibid* para159.

²⁵ *Weber and Saravia v Germany*, *supra* note 23 para 95.

²⁶ See *Zakharov v Russia*, *supra* note 23 paras 258, 233, *Szabó and Vissy v Hungary*, *supra* note 21 para77. [“The Court recognizes that authorization of secret surveillance by a non-judicial authority may be compatible with the Convention, provided that the authority is sufficiently independent from the executive. But it emphasizes that it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure.”]

²⁷ *Szabó and Vissy v Hungary*, *supra* note 21 paras77, 79. [“The *ex ante* authorisation of such a measure is not an absolute requirement *per se*, because where there is extensive *post factum* judicial oversight, this may counterbalance the shortcomings of the authorisation”; “the external, preferably judicial, *a posteriori* control of secret surveillance activities, both in individual cases and as general supervision, gains its true importance ... by reinforcing citizens’ trust that guarantees of the rule of law are at work even in this sensitive field and by providing redress for any abuse sustained.”]

²⁸ *Zakharov v Russia*, *supra* note 23, para 260 [“Whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures”.]; *Szabó and Vissy v Hungary*, *supra* note 21 para 71.

²⁹ For the requirement of making binding decisions for constituting an effective remedy, see *Silver and others v United Kingdom* (1983), 61 ECHR (Ser A) 161, 5EHRR347, para 115; *Kennedy*, *supra* note 23 para167. Similarly, Human Rights Committee considered in the light of the obligation to exhaust domestic remedies, that if the decisions handed by an oversight body would only have recommendatory, rather than binding, effect, it could not be recognized as effective remedy. See *Francesco Madafferi v Australia*, UN Human Rights Committee, Communication No 1011.2001, UN Doc CCPR/C/81/D/1011/2001 (2004), para 8.4

but can be satisfied by an aggregate of remedies provided for under domestic law.³⁰ For example, in the *Kennedy v. the UK* case, the ECtHR considered both the Interception of Communication Commissioner established under RIPA and the Investigatory Power Tribunal (IPT). Both were considered as having sufficient independence and having access to all relevant documents. Whereas the Commissioner reported to the Prime Minister about the application of the RIPA and the Interception of Communications Code of Practice in surveillance activities, did not address individual complaints, and had no competence of referring individuals to courts or granting redress, the IPT could examine any complaint of unlawful interception and had the power to quash interception order, require destruction of interception material and order compensation when it found the interception unlawful. Taking together the Commissioner and the IPT, the ECtHR considered they provided the effective domestic remedies.³¹

The effectiveness of remedy in the situation of secret surveillance also requires the notification of surveillance measures to the persons affected. When surveillance measures are taken without *ex ante* notification, or if the accompanying review of surveillance when surveillance is ordered or carried out is not communicated with the individuals affected, subsequent notification becomes crucial for individuals to challenge the secret surveillance retrospectively.³² The ECtHR, hence, holds that, “as soon as notification can be carried out without jeopardizing the purpose of the restriction after the termination of the surveillance measures, information should be provided to the persons concerned.”³³

The ECtHR’s approach will be critically analysed in more detail in Chapter 4. Here, I want to make one brief observation. For the ECtHR, its approach of addressing state surveillance seems consistent with its procedural turn when assessing state compliance with the ECHR.³⁴ The

³⁰ *Leander v Sweden* (1987), 116 ECHR 9Ser A), 9 EHRR 433, paras 81-84. See also *Chahal v. United Kingdom* (1996), Reports of Judgments and Decisions, 1996-V 1853, 23 EHRR 413, para 145.

³¹ *Kennedy*, *supra* note 23 paras 166-169.

³² *Zakharov v Russia*, *supra* note 23 paras 233-234.

³³ *Szabó and Vissy v Hungary*, *supra* note 20 para 86. Subsequent notification is also recommended in La Rue’s 2013 report. La Rue, *supra* note 3 para 82 [“Individual should have a legal right to be notified that they have been subjected to communication surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath.”]

³⁴ Oddný Mjöll Arnardóttir, “The ‘procedural turn’ under the European Convention on Human Rights and presumptions of Convention compliance” (2017) 15:1 Int J Const Law 9; Thomas Kleinlein, “The Procedural Approach of the European Court of Human Rights: Between Subsidiarity and Dynamic Evolution” (2019) 68:1

ECtHR's turn to procedural consideration has specific conditions. The specific conditions are the subsidiarity of the Court and the interest of democratic legitimacy of the Court's decisions, especially in national security issues where states are given a considerable margin of appreciation. The proceduralization of the Court's review has been subject to some criticisms for giving too much deference to states and reducing its own judicial task.³⁵ Though it is not to argue that procedural guarantee is unimportant, it is important to bear in mind the ECtHR's detailed requirements for safeguards against the abuse of power by state surveillance could also normalize and empower state surveillance if the procedural requirements are detached from substantive principles of the rule of law and human dignity. The procedural approach even made the Court itself depart from its own much more principled stand about state bulk surveillance, as seen in the recent case *Big Brothers Watch*, which will be discussed in Chapter 4.³⁶

A related issue is that because of the procedural turn of the ECtHR, the ECtHR's case law concerning mass surveillance ties the necessity and proportionality of surveillance measures closely to its procedural guarantees and to a certain degree, attenuates the substantive criteria of necessity and proportionality. In *Szabó and Vissy v Hungary*, the Court held that the requirement, "necessary in a domestic society", should be interpreted as, "strict necessity": a measure of secret surveillance must be strictly necessary both for the safeguarding of the democratic institutions and for the obtaining of vital intelligence in an individual operation.³⁷ Despite declaring the strict necessity criterion, the Court only addressed the lack of prior judicial authorisation to ensure the surveillance measures as failing this criterion. It reaffirmed the Court's subsidiarity to domestic procedural guarantees and domestic oversight bodies' assessment of necessity and proportionality. The Court's tendency to emphasize procedural guarantees, then, is also a tendency to defer to the judgment of national authorities, in ways that enhance sovereign discretion and make it the key component in ensuring human rights compliant surveillance.

International & Comparative Law Quarterly 91; Thomas Kleinlein, "Consensus and Contestability: The ECtHR and the Combined Potential of European Consensus and Procedural Rationality Control" (2017) 28:3 Eur J Int Law 871.

³⁵ Arnardóttir, *supra* note 35.

³⁶ In *Zakharov v. Russia*, the ECtHR held that "a system...which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorization to the communications service provider, or to anyone else, is particularly prone to abuse." *Zakharov v. Russia*, *supra* note 23, para 270. But in *Big Brothers Watch v. UK*, the ECtHR accepted bulk surveillance regime and held the reasonable suspicion and prior judicial authorisation of interception were not required. See Chapter 4.1.

³⁷ *Szabó and Vissy v Hungary*, *supra* note 21 para 73.

It is interesting to compare with the CJEU, which has been more assertive in this respect and directly conducted a proportionality assessment in the *Digital Rights Ireland* and the *Tele2 Sverige AB* cases. When transposing the ECtHR's assessment to a domestic context, national judicial or quasi-judicial oversight bodies cannot simply refer to the ECtHR (given that the Court has essentially given them significant discretion), but need to develop their own substantive criteria. The issue of the self-judging character of the limitations on fundamental freedoms, especially on national security ground, resurfaces. But putting aside this long-existing issue, the ECtHR's procedural review which defers to the discretion of the national authorities is sometimes used by national oversight authorities as establishing legal standards that can justify their own decisions. This is seen in the *Human Rights Watch case* before the UK IPT. As discussed in Chapter 1, whether someone can claim to be victim of state bulk surveillance and bring human rights claims before the ECtHR is partially dependent on the unavailability of effective national remedies. This approach is not transposable to the IPT given that the IPT is itself a domestic remedy mechanism and has its own applicable law, *i.e.* RIPA, which stipulates who can bring a claim. Nevertheless, the IPT relied on the ECtHR's approach to deny the applicant victim status by claiming itself to be an effective remedy acknowledged by the ECtHR in the *Kennedy case*.³⁸

The underlying problem of the procedural guarantee is essentially the same one as the second inscription of the Frankenstein myth into law where law is treated as an instrument for (micro)managing surveillance activities. In a technical and instrumentalist approach to law and procedural guarantees inheres the risk that formal law and accountability mechanisms can be manipulated for the opposite objective: they can be used to reinforce the self-referring and self-judging character of state surveillance and normalize its intrinsic secrecy and the unbridgeable power differential between the surveillance authorities and individuals.

1.2 Surveillance in predictive policing and judicial decision-making process

While the human rights legal responses to bulk digital surveillance discussed previously still bear importance for regulating predictive law-enforcement, there are very few cases where the

³⁸*Human Rights Watch Inc. et al. v Secretary of State for the Foreign & Commonwealth Office et al.* [2016] UKIPTrib15-165-CH, para 46.

deployment of surveillance and data analytics in policing operations and the administration of justice is directly challenged for human rights violations. This is perhaps because the new digital technologies were introduced to the law enforcement and justice systems in the last ten years and have largely been kept secret only until recently.³⁹ There is no case concerning actuarial justice yet in the ECtHR. In the US the police departments of a few jurisdictions have been sued by civil society groups for using surveillance technologies in the past two years. The requests, however, have so far been limited to making certain policing documents available to the public based on the Freedom of Information Act.⁴⁰ The *Loomis* case mentioned in Chapter 1 is currently the only one about court using software of digital surveillance and data analytics in decision-making. The reason why there are so few cases may also have to do with, paradoxically, the generalized nature of such surveillance and the fact that in violating the rights of all the weight of violations is not felt more significantly by any single party.

The current reactions to the deployment of digital surveillance technologies by law enforcement can be categorised in two ways. First, making the acquisition and adoption of new technologies by the law enforcement authorities subject to democratic deliberation and judicial scrutiny. Second, designing the legal regime to address directly the problem of the new logic of policing and justice administration.

1.2.1 Making the acquisition and deployment of new digital surveillance technologies come under judicial and democratic scrutiny

Aside from the European Union, the regulatory difficulties caused by predictive policing and actuarial justice have not been systematically dealt with. It seems that although the fundamental challenges to human rights and the rule of law are raised by activists and academics, public

³⁹ For example, Ali Winston, “Palantir has secretly been using New Orleans to test its predictive policing technology”, (27 February 2018), online: *The Verge* <<https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd>>.

⁴⁰ “ACLU of Massachusetts v. Boston Police Department”, (14 November 2018), online: *ACLU Massachusetts* <<https://www.aclum.org/en/cases/aclu-massachusetts-v-boston-police-department>>; Rachel Levinson-Waldman & Erica Posey, “Court Rejects NYPD Attempts to Shield Predictive Policing from Disclosure”, (26 January 2018), online: *Brennan Center for Justice* <<https://www.brennancenter.org/blog/court-rejects-nypd-attempts-shield-predictive-policing-disclosure>>; Jim Dallke, “Chicago Police Sued Over ‘Heat List’ Algorithm by Journalists”, (8 June 2017), online: *American Inno* <<https://www.americaninno.com/chicago/chicago-pd-sued-over-crime-prediction-algorithm/>>; Matt Sledge, “Convicted gang leader can challenge NOPD’s use of crime-fighting software, judge rules”, (14 March 2018), online: *The Advocate* <https://www.theadvocate.com/new_orleans/news/courts/article_3a68a838-27bb-11e8-8b07-178e270926d4.html>.

discussions are quickly framed as issues of transparency and accountability on the part of the state institution, all but giving up on a deeper engagement with the very nature of surveillance. As for transparency, this is particularly the case in the US where the police forces have been using commercially developed and provided programs for years with barely any public knowledge and input.⁴¹ The problem of the lack of transparency in the US is also exacerbated by the transfer of military equipment to local police forces.⁴² To expose the existence of such practices and to make records about existing predictive policing programs available to the public are the first steps toward transparency and accountability of law enforcement activities. In addition, the American Civil Liberties Union (ACLU) has proposed a regulatory framework for the acquisition and deployment of surveillance and military equipment by the municipal law enforcement authorities.⁴³ This includes the requirement of prior approval by the city council, publication of the impact assessment report and use policy of the surveillance and military equipment, as well as annual report by the law enforcement authorities on the use of surveillance and military equipment that has been approved by the city council. The use policy of surveillance and military equipment needs to specify the purpose, the legal procedures and oversight mechanism for the deployment of the equipment, the necessary information about the conditions for data collection, data protection, data retention and data sharing, and the procedures addressing complaints and requests from the public.⁴⁴ In short, at the current stage, the primary task is to bring such practices to public knowledge and democratic procedures.

The issues of transparency and accountability have an additional aspect when decision making relies on algorithms. It is generally accepted in practice that information on surveillance

⁴¹ E.g. Ali Winston, “Palantir has secretly been using New Orleans to test its predictive policing technology”, (27 February 2018), online: *The Verge* <<https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd>>; Michael Isaac Stein, “‘Holy cow’: the powerful software behind the city’s surveillance system | The Lens”, (20 December 2018), online: *The Lens* <<https://thelensnola.org/2018/12/20/holy-cow-the-powerful-software-behind-the-citys-surveillance-system/>>, as well as the PredPol and COMPAS as discussed in Chapter 1.

⁴² “Restrictions on Military Gear to Local Police Are Lifted”, online: *Equal Justice Initiative* <<https://eji.org/news/restrictions-military-gear-local-police-are-lifted>>.

⁴³ “Community Control Over Police Surveillance + Militarization (CCOPS+M) Model Bill”, (October 2018), online: *American Civil Liberties Union* <<https://www.aclu.org/other/community-control-over-police-surveillance-militarization-ccopsm-model-bill>>; “An Act To Promote Transparency and Protect Civil Rights and Civil Liberties With Respect to Surveillance Technology”, online: *ACLU* <<https://www.aclu.org/files/communitycontrol/ACLU-Local-Surveillance-Technology-Model-City-Council-Bill-January-2017.pdf>>.

⁴⁴ *Ibid.*

and analytical programs developed by commercial entities is not made available to the public, and hence an accepted concession in terms of transparency.⁴⁵ This inevitable lack of transparency is sought to be balanced by improving accountability which essentially is about keeping the “human in the loop” and reasserting human decisional agency. This is seen in the *Loomis* case where the Wisconsin Supreme Court held that courts could not determine cases on the sole basis of the results of the program and must instead explain other factors which support the decision.⁴⁶ As will be seen shortly, a similar solution is given by the EU data protection law which includes many detailed requirements.

When considering the approach of subjecting the acquisition and deployment of surveillance technologies to public scrutiny, it is important to bear in mind that it is just a preliminary step that should lead to more substantive examination of the use of surveillance by law enforcement in light of basic principles of the rule of law and human rights. While this approach can indeed be formulated as the individual’s right to be informed and to participate in public and political affairs, attention needs to be promptly paid to two issues. First, there is always a risk that the requirements of transparency and accountability, such as those proposed by the ACLU, could be diluted into merely clerical work if they are not anchored in the rule of law and human rights principles and equipped with strong enforcement bodies. Merely knowing how surveillance operates is evidently not sufficient. Second and more importantly, the approach of having democratic and public input (potentially by majority rule) in the acquisition and adoption of surveillance by law enforcement can become quite problematic if detached from the rule of law and human rights principles, which protect vulnerable and marginalized people. It is not inconceivable that a city council, following deliberative procedures, would approve the use of a predicative policing program which would unfairly impact certain groups of people but was deemed as necessary after a cost-benefit calculation. So, this preliminary step toward transparency and accountability of law enforcement activities, although incrementally important, already raises normative questions about the relationship between democracy, human rights and the rule of law.

⁴⁵ Even in Brennan Centre’s request, the request for information about software and input/output data was dropped out by the Brennan Centre, see Levinson-Waldman & Posey, *supra* note 41.

⁴⁶ *State v. Loomis*, 881 NW (2d) 749 (2016), para 99.

1.2.2 Legal framework addressing the new logic of policing and administration of justice

The previous discussion suggests the need to engage more with substantive and normative questions regarding human rights and the rule of law. The human rights legal framework has some fundamental difficulties in dealing with predicative policing and actuarial justice. Chapter 1 showed some of the problems: typically, mass digital surveillance is radically incompatible with the requirement of reasonable suspicion as it collects data from and about everyone and suspicion is formed afterwards. There is a paradigmatic contrast between the forward-looking surveillance-based policing and the fundamentals of criminal justice which offer individuals the presumption of innocence and non-discrimination and only reacts to reasonable, individuated suspicion.⁴⁷ Surveillance and intelligence-led law enforcement is not only developed in spite of the human rights framework that contains basic principles of criminal justice, but also gradually changes how the right to presumption of innocence and the right of non-discrimination are understood.⁴⁸ This is reflected in discourses like, “nothing to hide, nothing to fear”.

The European Union has sought to tackle this deep fault line with its newly adopted Law Enforcement Data Protection (LEDP) Directive. It was adopted together with the EU General Data Protection Regulation (GDPR) in April 2016, forming the new data protection framework of the EU. A full analysis of the LEDP is beyond the objective of this section⁴⁹ and I will focus instead on the question of how the LEDP is positioned in the contrast between surveillance and intelligence-led law enforcement and the framework of human rights.

First, subject to the EU Charter of Fundamental Rights, the LEDP exhibits a right-based approach when stipulating the principles of data protection and creating specific rights for data subjects and obligations for the data-handling law enforcement authorities. The basic principles are lawfulness, fairness, purpose limitation, data minimisation, accuracy, storage minimisation,

⁴⁷ E.g. Andrew Guthrie Ferguson, “Big Data and Predictive Reasonable Suspicion” (2015) 163:2 University of Pennsylvania Law Review 327; Antonella Galetta, “The changing nature of the presumption of innocence in today’s surveillance societies: rewrite human rights or regulate the use of surveillance technologies?” (2013) 4:2 European Journal of Law and Technology, online: <<http://ejlt.org/article/view/221>>.

⁴⁸ The shift from presumption of innocence to presumption of guilt and the fundamental change of the assumptions of law were discussed by a House of Lords report on surveillance society in 2009. House of Lords, Select Committee on the Constitution, *Surveillance: Citizens and the State* (London: House of Lords, 2009) at 26–28.

⁴⁹ The technological and organizational guarantees for the accountability and security of data collection and data processing are laid down in detail in the LEDP. There are many resonances with the proposal from the ACLU previously mentioned in Section 2.2.1 and with the GDPR discussed below in Section 3.2. See also, Catherine Jasserand, “Law enforcement access to personal data originally collected by private parties: Missing data subjects’ safeguards in directive 2016/680?” (2018) 34:1 Computer Law & Security Review 154.

security and integrity.⁵⁰ Especially important are the principles of purpose limitation,⁵¹ data minimisation⁵² and storage minimisation,⁵³ which could impose useful restraints on the surveillance-based data-driven law enforcement, which also often defines the purpose of data collection and processing in broad and general terms to allow for function creep of the big data.⁵⁴ There is no principle of transparency as such in the LEDP, unlike the GDPR mentioned below. But the principle of transparency, combined with the principle of accuracy, is reflected in the individual's right to be informed about the collection and processing of the data subject's personal data, the right of access to personal data, and the right to rectification or erasure of personal data. In addition, the lack of an explicit principle of transparency also reflects the baseline that unobstructed function of law enforcement needs to be ensured.⁵⁵ Accordingly, these individual rights are subject to restriction. The imposition of restriction follows the classic criteria in human rights law; the restriction needs to be provided by law and to be proportionate and necessary in a democratic society.⁵⁶

Second, one individual right that is particularly relevant to law enforcement using algorithmic programs is the right not to be subject to a decision based solely on automated processing.⁵⁷ This right speaks to several problems raised by the automated social sorting in the law enforcement context. One such problem is of profiling which reinforces extant social discrimination and stigmatization. The LEDP expressly prohibits profiling that results in discrimination on the basis of special categories of personal data such as data around one's racial

⁵⁰ EU, *Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, [2016] OJ, L 119/89, ("LEDP"), art 4.

⁵¹ Personal data should be collected for "specified, explicit and legitimate purposes" and processed in a manner compatible with those purpose. LEDP art 4(1)(a).

⁵² Personal data processed for the "specified, explicit and legitimate purposes" should be "adequate, relevant and not excessive" in relation to those purposes. LEDP art 4(1)(b).

⁵³ Personal data should be stored for no longer than is necessary for the purposes of the processing. LEDP art 4(1)(e).

⁵⁴ Rosamunde van Brakel & Paul De Hert, "Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies" (2011) 20:3 *Journal of Police Studies* 163 at 178–179.

⁵⁵ The LEDP includes these functions of law enforcement: the official or legal inquiries, investigations or procedures; the prevention, detection, investigation or prosecution of criminal offenses or the execution of criminal penalties; the protection of public security; the protection of national security; the protection of the rights and freedoms of others. LEDP, arts13(3), 15(1), 16(4).

⁵⁶ LEDP, arts13(3), 15(1), 16(4)

⁵⁷ LEDP, art 11.

or ethnic origin, health and sexual orientation.⁵⁸ Another problem is the accountability of decisions based solely on automated processing. Under the LEDP, when such a decision is legally authorised, individuals should be provided with appropriate safeguards including the rights to obtain human intervention, to obtain an explanation of the decision and the opportunity to challenge the decision.⁵⁹ In particular, these safeguards are preconditions for decisions made by automated processing of special categories of personal data.⁶⁰ This seems to suggest an integration of due process rights in the law enforcement activities that use big data analytics. In addition, although the right to obtain an explanation of the decision does not mean the logic and function of the program must be explained, the right to challenge the decision arguably presumes that the explanation of the decision should be meaningful and intelligible to the individual concerned.⁶¹

There have been some criticisms about the limitation of this “big data due process right”.⁶² Notably, this individual right only applies to decisions based solely on automated processing, which could mean that even minimal human involvement could make it inapplicable. The problem of quality concerning human involvement also exists for the safeguards. As will be seen shortly, the EU GDPR contains similar rules on automated decision-making and the same problem of human involvement. This problem is dealt with by the Art 29 Working Party (“WP”) which is an advisory body set up by the EU Data Protection Directive, the predecessor of the GDPR.⁶³ Its interpretation of the term “solely” is that the data controller cannot “fabricate”

⁵⁸ LEDP, art 11(3). “Special categories of personal data” is defined as personal data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person’s sex life or sexual orientation. See LEDP, art 10.

⁵⁹ LEDP, art 11(1), Recital 38.

⁶⁰ LEDP, art 11(2).

⁶¹ While unlike the GDPR, which specifically requires meaningful information about the logic of the automated-processing to be communicated to data subjects, the argument for the right to challenge can only be effective if data subjects fully understand how the decision is made and on what basis, which supports a right to explanation in the GDPR, and should in principle also apply to the LEDP. Andrew D Selbst & Julia Powles, “Meaningful information and the right to explanation” (2017) 7:4 International Data Privacy Law 233.

⁶² Sandra Wachter, Brent Mittelstadt & Luciano Floridi, “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation” (2017) 7:2 International Data Privacy Law 76 at 92; Lilian Edwards & Michael Veale, “Slave to the Algorithm? Why a ‘Right to Explanation’ Is Probably Not the Remedy You Are Looking For” (2017) 16:1 Duke Law and Technology Review 19 at 44–45; Isak Mendoza & Lee A Bygrave, “The Right Not to be Subject to Automated Decisions Based on Profiling” in Tatiana-Eleni Synodinou et al, eds, *EU Internet Law: Regulation and Enforcement* (Springer International Publishing, 2017) 77.

⁶³ It is now replaced by the European Data Protection Board under the GDPR and is composed of the head of the Supervisory Authority from each EU Member State and of the European Data Protection Supervisor. Its missions

human involvement and the human input of the decision must be meaningful and carried out by persons who have the authority and competence to change the decision.⁶⁴ So, “if someone routinely applies automatically generated profiles to individuals without any actual influence on the result,” the WP considers it as still a decision based solely on automated processing.⁶⁵ The WP’s interpretation is transposable to the LEDP since the implementation of the two regulations has been largely aligned.

Third, the LEDP requires law enforcement authorities that collect and process personal data to make clear distinctions between the personal data of different categories of data subjects, and between personal data based on facts and personal data based on individual assessments.⁶⁶ The former distinction is necessitated by the fact that activities of policing and criminal justice often involve personal data of different categories of people, such as suspects, convicted criminals, victims, witness and associates of suspects and convicted criminals. The processing of data in each category needs to respect the basic principles such as purpose limitation. The LEDP requires not only a clear distinction to be made but also that the distinction should not prevent the application of the presumption of innocence.⁶⁷ The latter distinction between fact and opinion entails the obligation to verify the authenticity and accuracy of personal data. It leaves the question open as to whether processed data concerning behavioural patterns produced by analytical programs, for example, is categorised as fact or assessment. Hence, it is not clear whether the obligation of verification applies to processed data.

Fourth, it should be immediately said that the rights-based approach of the LEDP does not just circumscribe the new data-driven, surveillance-led law enforcement. The enabling side of taming the deployment of these new technologies by the LEDP is reflected by the exclusion of anonymous data from its application. The category of personal data in the LEDP is indeed very broad, covering any information relating to an identified or identifiable natural person,⁶⁸ and the

are laid down in art 70 GDPR and art 51 of the LEDP, which include issuing guidelines, recommendations and best practices for the interpretation and implementation of the GDPR and LEDP.

⁶⁴ Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision Making and Profiling*, 3 October 2017, WP251rev.01, at 21

⁶⁵ *Ibid.*

⁶⁶ LEDP, arts 6 and 7.

⁶⁷ LEDP, Recital 31

⁶⁸ LEDP art 3(1). Personal data is defined as any information relating to an identified or identifiable natural person, which includes name, identification number, location data, online identifier, data revealing the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person.

criterion of identifiability is “reasonable likelihood” of identification.⁶⁹ Despite the flexibility of “personal data”, anonymous data which are by definition not personal data, are not covered by the LEDP.⁷⁰ Hence for example, anonymous data in respect to a person’s living environment and derived or processed data products from commercial sources which cannot be used to re-identify the data subject, can be used in predictive policing to form patterns of criminal hotspots and hot time periods. This is actually claimed by the US Company PredPol (mentioned in Chapter 1) as its program does not use personal identifiable information, demographic, ethnic or socio-economic information for the protection of privacy. It is not inconceivable that the LEDP could simultaneously empower law enforcement authorities to further develop technologies and strategies that can dispense with personal data. As will be seen shortly, legal regulations for commercial digital surveillance have similar issues, which will be revisited from the perspective of the elimination of the human rights encounter in Chapter 4.

In short, the embeddedness of the EU LEDP in human rights framework provides several valuable tools to drive the new model of law enforcement back on the track in support of human rights and fundamental principles of criminal justice. Yet, the tension between individual rights and backward-looking law on the one hand and forward-looking surveillance on the other remains.

2. Regulatory regimes for commercial digital surveillance

2.1 Problem framing

Google’s invasive and disturbing digital surveillance encountered several legal challenges from consumers and rights advocates in the early 2010s⁷¹ and the public resistance was significantly intensified due to Edward Snowden, who revealed the cooperation of major tech companies with the NSA. The scandal of state mass surveillance was revealed to be the tip of an iceberg that

⁶⁹ LEDP, Recital 21. The test of identifiability is “reasonable likelihood”, which means that if an individual can be identified using “all means reasonably likely to be used”, the information is personal data.

⁷⁰ LEDP, Recital 31. [“The principles of data protection should...not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is no longer identifiable.”]

⁷¹ E.g. Julia Angwin, “Google faces new privacy probes”, *The Wall Street Journal* (16 March 2012), online: <<https://www.wsj.com/articles/SB10001424052702304692804577283821586827892>>; Charles Arthur, “Google facing legal threat from six European countries over privacy”, *The Guardian* (2 April 2013), online: <<https://www.theguardian.com/technology/2013/apr/02/google-privacy-policy-legal-threat-europe>>.

included much less regulated commercial digital surveillance. This soon led to a series of legal interventions, notably by the European Union. I will mainly discuss the regulatory regimes on the protection of personal data in the context of commercial digital surveillance.

Just a quick note here. It is important to bear in mind that the market power of global platforms such as Google and Facebook is an important factor that causes the problems related to human rights, democracy and the rule of law. In addition to the problems of individual lack of control and the lack of transparency on the part of the commercial entities (which will be discussed shortly), the domination of these tech giants and their abuse of the dominant positions they hold in the market are also a crucial problem which brings in a powerful regulatory tool – competition law. There have been several antitrust complaints against Google in recent years at the European Commission. It has fined Google for requiring smartphone makers to preinstall its services⁷² and for favouring its own comparison shopping service in Google’s web search results.⁷³ The German Federal Cartel Office (Bundeskartellamt) prohibited Facebook from collecting and combining data from websites and applications owned by Facebook and from third-party websites and smartphones and then assigning the data to users’ Facebook accounts without the user consent.⁷⁴ However, while competition law is a powerful tool to regulate digital conglomerates, its impact on human rights and protection of personal data, whilst important, should be seen as secondary. Its primary objective is to create a level playing field so that other service providers (especially enterprises from the EU) can compete and develop their services and products fairly in the market, not to tackle the problem of surveillance per se. Having said that, I will return to the regulatory challenges specific to human rights and personal data protection in commercial digital surveillance in this discussion.

Legal and political interventions typically frame the problem of commercial data surveillance mainly in two interrelated aspects: the lack of control by individuals over the

⁷² “Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google’s search engine”, (18 July 2018), online: *European Commission - Press release* <http://europa.eu/rapid/press-release_IP-18-4581_en.htm>.

⁷³ “European Commission - PRESS RELEASES - Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service”, (27 June 2017), online: *European Commission - Press release* <http://europa.eu/rapid/press-release_IP-17-1784_en.htm>.

⁷⁴ “Bundeskartellamt prohibits Facebook from combining user data from different sources”, (7 February 2019), online: *Bundeskartellamt* <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html>.

collection and use of their data and the lack of transparency and accountability of how data is handled in the private sector.⁷⁵ To a certain degree, this framing resembles that of state digital surveillance in the sense that both state and commercial surveillances are characterised by their obscurity and the lack of knowledge about the surveillances on the part of the surveilled. Regardless of this resemblance, the relationships involved in the two contexts of surveillance are theoretically rather different (*i.e.*, one is about the state-subject relationship and the other about the company-consumer relationship) and the problem framing of each context bears distinct features.

For state surveillance, the mainstream responses focus more on the encroachment of democratic accountability and the rule of law than on the status and substance of human rights *per se*. What digital transformation of individual subjectivity means to conceiving and practising human rights and how to name new human rights specific to the digital age receive much less consideration. This is not the case for commercial digital surveillance where there is much more focus on individual right-holders and the positive exercise of their rights vis-à-vis companies. New regulatory interventions in commercial surveillance (such as the EU GDPR) also seem to be less constrained by concern over naming new data protection rights. As will be shown later, European legislators in particular appear very keen to establish new rights regarding personal data protection, so that individuals regain control over their information and its use, as well as to impose corresponding duties on companies to protect those new rights. The problem of the lack of transparency in commercial digital surveillance is also framed by common legal and political interventions so as to centre around individual rights. To advance the transparency of data collection and processing would help people form a meaningful understanding of the circumstances of data collection and processing, which is often considered a prerequisite for informational self-determination.

The notion of informational self-determination, which is theoretically embedded in liberal humanism, was initially developed by the German Constitutional Court in 1983 in a landmark case which declared unconstitutional certain provisions of the revised Census Act that

⁷⁵ European legal interventions will be discussed below. Also see the reactions in the US. White House Report, “Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy” (2012) 4:2 *Journal of Privacy and Confidentiality* 95. See also, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Federal Trade Commission, 2012).

provided for governmental collection of personal data for statistical purposes. As Rouvroy and Poullet have observed, the German Constitutional Court arrived at the right to informational self-determination and the data protection legal regime through the fundamental right to the “free development of one’s personality”.⁷⁶ The notion of informational self-determination has migrated from the activities of public authorities to those of the private and commercial sectors and has become the core notion of the European data protection framework.

One crucial problem of informational self-determination in the current state of the information society is user consent. Consent marks another important difference between the mainstream responses to state surveillance and those to commercial data surveillance. In state surveillance, individual consent is not a precondition for lawful state surveillance when surveillance is carried out as part of the state’s coercive power on grounds such as national security and public order⁷⁷ (except perhaps through the very fictitious notion of the social contract). Presumably, the lack of pre-given consent is compensated by other conditions of state surveillance that ensure the exercise of coercive power is legally regulated and democratically accountable. The lack of consent as such is not considered a flaw in state cyber surveillance. In commercial data surveillance, the presumption of the legitimacy of the coercive power does not sustain, and therefore individual consent to data collection and data processing becomes an important, although not the only, precondition to lawful data collection and data processing.⁷⁸

As many scholars and policy makers have pointed out, the traditional notice-and-consent approach in the surveillance-based business model fails because the user cannot freely consent when put in a “take it or leave it” situation, without the possibility to negotiate. Privacy policies

⁷⁶ Antoinette Rouvroy & Yves Poullet, “The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy” in Serge Gutwirth et al, eds, *Reinventing Data Protection?* (Dordrecht: Springer Netherlands, 2009) 45. The right was claimed by the Court as ‘the authority of individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others’.

⁷⁷ E.g., EU Directive 2002/58/EC on privacy and electronic communication provides for the confidentiality of communications, which prohibits surveillance of communications without the consent of the users concerned. Exception to this prohibition is provided in art 15(1), which allows states to adopt legislation to restrict the scope of confidentiality of communications when the restriction is necessary, appropriate and proportionate in a democratic society to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of authorised use of the electronic communication system. This limitation is also provided in EU Directive 95/46/EC, article 13(1) and the EU General Data Protection Regulation, art 23(1).

⁷⁸ User consent is not the only lawful basis for data collection and data processing. Many jurisdictions require companies to collect and give user information to authorities for law enforcement purposes and allow the collection and processing of data for the “legitimate interest” of the companies. It remains however, the most important lawful basis in terms of giving individuals control over their information.

are often long, legalistic, difficult to understand and can be changed at will by companies.⁷⁹ Just recalling Hal Varian's idea discussed in Chapter 2 that marketers should "bribe" and "induce" users to give their information,⁸⁰ it becomes obvious how surveillance capitalism exploits user frailty in order to obtain consent. Moreover, how data will be recycled and reused and the consequences of such processing are often unknown at the time of collection, especially in the big-data age when the value of data does not primarily reside in its primary purpose.⁸¹ It is not possible for users to give informed consent to unknown data usage.

The challenge to the traditional idea of informed, freely-given consent has led some scholars to propose alternative models for data protection. For example, Hildebrandt has argued that purpose limitation (meaning that personal data should be collected for specific, explicit and legitimate purposes and should not be processed in a manner incompatible with those purposes), should replace the consent-based model of data protection.⁸² Mayer-Schönberger has also argued that data protection in the big data age should focus less on individual consent and more on holding the data-handling entities accountable for what they do and increasing the power of data protection authorities.⁸³

In addition to the issue of consent, the other prong of the problem framing – the lack of transparency of the data processing – has also raised questions. It is argued that whereas transparency is the default rule for governmental administrative actions,⁸⁴ the opposite is often true for the private sector, due to trade secrecy law, intellectual property law, and the autonomy

⁷⁹ Helen Nissenbaum, "A Contextual Approach to Privacy Online" (2011) 140:4 *Daedalus* 32; Rikke Frank Joergensen, "The unbearable lightness of user consent" (2014) 3:4 *Internet Policy Review* 1.

⁸⁰ See Chapter 2, Section 2.1.

⁸¹ Viktor Mayer-Schönberger & Kenneth Cukier, *Big Data: A Revolution that Will Transform how We Live, Work, and Think* (Houghton Mifflin Harcourt, 2013) at 153. Hildebrandt also observed the complexity of the relationship between an individual's personal data and data derived from group profiles, for which informed consent is seriously inadequate as a basis for group profiling: "First, group profiles that are applied to me have been inferred from masses of (personal) data that are not mine...; second they are applied because my (personal) data match the profile which does not imply that the profile actually applies...; third, sophisticated profiling technologies like e.g., behavioral biometric profiling (BBP) do not require identification at all..." Mireille Hildebrandt, "Who is Profiling Who? Invisible Visibility" in Serge Gutwirth et al, eds, *Reinventing Data Protection?* (Springer, Dordrecht, 2009) 239 at 243.

⁸² Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing, 2015) at 156.

⁸³ Mayer-Schönberger & Cukier, *ibid* at 173; Joergensen, *supra* note 39 at 9.

⁸⁴ Martin H Redish & Lawrence C Marshall, "Adjudicatory Independence and the Values of Procedural Due Process" (1986) 95:3 *The Yale Law Journal* 455 at 485–486.

of business⁸⁵ as exemplified by the data broker industry discussed in the Chapter 2. Moreover, transparency may provoke responses from the companies that deliberately display complexity to defeat people's attempts to understand the transaction or data processing. This is especially the case for decision-making using big data analytics and machine-learning where the transparency of decision-making does not mean the individual can comprehend the decision-making process.⁸⁶ Hence, transparency can create an illusory feeling of control for the individual while maintaining the structural power asymmetry.⁸⁷ Moreover, as pointed out by Crain, to frame the problem of commercial data surveillance as being about transparency is not only unhelpful but can also be dangerous since companies can deal with transparency requirements as a matter of public relations management and deflect more interventionist regulations by the government.⁸⁸

Despite these cautions of “meaningless consent” and “transparency fallacy”, the two-pronged problem framing, *i.e.*, the lack of control on the part of individuals and lack of transparency and accountability on the part of the companies, remains the dominant approach to address commercial data surveillance. To a certain degree, European legal interventions also share these concerns for the limitations of traditional understandings of consent and transparency.⁸⁹ Instead of completely changing the frame, the European legislatures and judges are motivated to ensure consent is meaningful and transparency is real, thereby reflecting that the legal interventions are anchored in the liberal notion of informational self-determination.

⁸⁵ Edwards & Veale, *supra* note 63 at 39.

⁸⁶ Malgieri et al. describe the transparency fallacy: “while, on the one hand, readability is an active tool for individuals, yet it is not so detailed in terms of impact of automated data processing (*comprehensibility without full transparency*). On the other hand, receiving information/explanation can be a powerful tool but it is usually not tailored to individuals’ understanding and comprehensibility (*transparency without full comprehensibility*).” Gianclaudio Malgieri & Giovanni Comandé, “Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation” (2017) 7:4 International Data Privacy Law 243 at 245; Mike Ananny & Kate Crawford, “Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability” (2018) 20:3 New Media & Society 973.

⁸⁷ Edwards & Veale, *supra* note 63 at 67; Frank Pasquale, *The black box society: the secret algorithms that control money and information* (Cambridge: Harvard University Press, 2015) at 8; Matthew Crain, “The limits of transparency: Data brokers and commodification” (2018) 20:1 New Media & Society 88.

⁸⁸ Crain, *supra* note 87 at 89.

⁸⁹ E.g., The Article 29 Data Protection Working Party had recognized the problem of illusory consent and opined that, “complexity of data collection practices, business models, vendor relationships and technological applications in many cases outstrips the individual’s ability or willingness to make decisions to control the use and sharing of information through active choice.” See Article 29 Data Protection Working Party and Working Party on Police and Justice, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, 1 December 2009, WP 168, online: < <https://www.garanteprivacy.it/documents/10160/10704/WP168++The+Future+of+Privacy> >, para 67.

2.2 Problem solving

While the two-pronged problem framing is an approach shared in many jurisdictions, the solutions vary and correspond to different conceptions of rights and of the legal and political traditions regarding how to regulate the market. The European approach is so far the most interventionist and comprehensive. It is largely a tripartite approach: first, empowering individuals by acknowledging a wider range of rights related to data protection; second, imposing extensive legal obligations on companies dealing with personal data to respect and protect those digital rights; and third, setting up enforcement mechanisms to ensure companies fulfil their obligations. Not all other jurisdictions recognize data protection as a fundamental right like the EU and are generous in granting new and extensive actionable rights to individuals. As for the transparency of handling data, while it is generally seen as a relatively straightforward solution, the concrete duties imposed on companies vary due to the different scopes of regulation in specific jurisdictions. For example, in countries adopting a sectoral approach to data protection, different industries such as health care and banking may have their own data protection laws. In some jurisdictions, particularly in the US, public policy is dominated by neoliberal ideology and companies have been lobbying for voluntary industry self-regulation for decades, which made the imposition of formal, legal obligations on companies much more difficult.⁹⁰ It also means that enforcement authorities have less power to intervene in business practices when the industry has been traditionally allowed to self-regulate.⁹¹ The European approach is so far the most influential for at least these two reasons: the EU data protection laws have extensive extraterritorial application;⁹² the Council of Europe's Convention 108 is an

⁹⁰ E.g., In May 2010, US Congressmen Boucher and Stearns released a discussion draft of comprehensive federal privacy legislation which would require, among other things, websites and network advertisers to provide users with clear and conspicuous notice of how they collect, use, store and share users' personal information. The bill was fiercely opposed by the industry, claiming it would devastate the digital economy. Dennis D Hirsch, "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?" 34 *Seattle University Law Review* 439 at 452–454.

⁹¹ E.g., The US FTC had accused Facebook for deceiving consumers about the privacy of their information on Facebook. In 2011, the FTC settled with Facebook and entered into a consent decree. Among other things, the decree required Facebook to obtain periodic assessments of its privacy practices by independent, third-party auditors for the next 20 years. Studies have observed that these third-party audits are poorly conducted and extremely inadequate to protect consumer privacy, as suggested by the Cambridge Analytica scandal. See Megan Gray, "Understanding & Improving Privacy 'Audits' under FTC Orders", (18 April 2018), online: *The Center for Internet and Society of Stanford Law School* </blog/2018/04/understanding-improving-privacy-audits-under-ftc-orders>.

⁹² E.g., The extraterritoriality of EU data protection law was provided for in the Directive 95/46, art 4(1)(a) and art 4(1)(c), which laid out two bases for establishing jurisdiction: the localization of an "establishment" of a data controller, or the localization of "equipment" used for data processing purposes. The CJEU has interpreted the

international treaty also acceded to by several non-European countries.⁹³ Against the repeated privacy breach scandals of some large tech companies, there are increasing voices from data protection and human rights advocacy groups promoting the European rights-centred and interventionist approach to data protection.⁹⁴

The two instruments just mentioned, the EU data protection law and Convention 108, have been modernized in parallel recently⁹⁵ and have considerable similarities,⁹⁶ saving that the EU data protection law, most notably, the EU General Data Protection Regulation (GDPR), contains detailed provisions while Convention 108 relies more on principles, which indicates their different binding nature. Within the EU data protection framework, in addition to the GDPR, the ePrivacy Directive is currently being updated. The proposed ePrivacy Regulation is the *lex speicalis* to the GDPR, which deals specifically with personal data in the electronic communications sector and ensures the confidentiality of electronic communications.⁹⁷ For the

jurisdictional bases with considerable flexibility, as evidenced in the *Google Spain* case where the Court held that processing activities related to search engine service were “in the context of” and “inextricably linked” to the activities of the establishment, i.e., Google Spain. *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12, ECLI:EU:C:2014:317, paras 55-56. The extraterritorial scope is also extensive in the new EU General Data Protection Regulation. It applies to the processing of personal data which takes place in the context of the activities of the establishment of the controller or processor within the EU, or the processing of the data of individuals within the EU by a controller or processor not established in the EU. See GDPR, *infra* note 99, art 3. Still in the *Google Spain* case, the CJEU found that individuals have a right to obtain removal of certain search results, subject to certain conditions, but left open the mode of implementation. The Article 29 Data Protection Working Party issued a guideline for implementing the *Google Spain* ruling, considering that the domain-based approach of de-listing (i.e., to modify the search results according to the domain name, such as google.es) is inadequate, and opined that, “in practice...in any case de-listing should also be effective on all relevant domains, including .com.” This means the obligation of de-listing is to be implemented globally. Article 29 Data Protection Working Party, *Guidelines on the Implementation of the Court of justice of the European Union Judgment on “Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” C-131/12*, 26 November 2014, WP225, at 9.

⁹³ *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 Jan 1981, ETS No.108 (entered into force 1 Oct 1985). It is ratified by all member states of the Council of Europe and six non-member states including Mauritius, Mexico, Senegal, Tunisia, Uruguay, Cabo Verde.

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=cN6J4BCa.

⁹⁴ E.g. Access Now, *Creating a Data Protection Framework: a Do's and Don'ts Guide for Lawmakers* (Access Now, 2018); Nuala O'Connor, “Reforming the U.S. Approach to Data Protection and Privacy”, (30 January 2018), online: *Council on Foreign Relations* <<https://www.cfr.org/report/reforming-us-approach-data-protection>>.

⁹⁵ The EU General Data Protection Regulation (GDPR), which modernizes the Data Protection Directive, was adopted in 2016, entered into force in May 28, 2018. And the updated Convention 108 was adopted by the Council of Europe on May 18, 2018.

⁹⁶ Drafters of the two modernization processes have taken utmost care to ensure consistency and compatibility between the two instruments. EU Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, 2018 edition ed (Luxembourg: Publications Office of the EU, 2018) at 12.

⁹⁷ European Commission, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, COM (2017) 10, 2017/0003 (cod) (Brussels,

purpose of this section, I will focus on the GDPR which has the broadest application and very detailed regulations.

The GDPR lays down the basic principles of personal data protection⁹⁸ and grants individuals a wide range of rights vis-à-vis entities identified as data controllers and data processors.⁹⁹ This includes the rights to be informed about the collection and processing of personal data, to access their personal data, to rectification and erasure, to object to or restrict the data processing, data portability; and not without controversy, the right to explanation when a decision is based solely on automated processing and the right to contest the decision made solely on automated processing.¹⁰⁰ Many of the seemingly innovative rights actually find their origins in the predecessor of the GDPR, the EU Data Protection Directive (DPD) and relevant jurisprudence of the CJEU.¹⁰¹ The principle of transparency is closely linked to the rights of data subjects, which is reflected also by the obligations of data controllers to respond to information requests of data subjects and provide information relating to the data processing in a, “concise, transparent, intelligible and easily accessible form, using clear and plain language,” without undue delay and free of charge.¹⁰² In case of automated decision-making including profiling, the data subject’s right of access to information requires the data controller to provide meaningful

1 Oct 2017). Among other things, the proposed regulation ensures the confidentiality of both the content data and the metadata of electronic communications.

⁹⁸ Principles include lawfulness, fairness and transparency, purpose limitation, data minimisation and storage minimisation, accuracy, integrity and confidentiality, accountability. See EU, *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*, [2016] OJ, L119/1, (“GDPR”), art 5.

⁹⁹ Data controller is defined as “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data”. Data processor is defined as “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.” GDPR, arts 4(7) and (8).

¹⁰⁰ Regarding the controversies over the right to explanation, see previous discussion in Section 2.2.2. See also, Wachter, Mittelstadt & Floridi, *supra* note 63; Edwards & Veale, *supra* note 63; Selbst & Powles, *supra* note 62; Malgieri & Comandé, *supra* note 86.

¹⁰¹ E.g., The DPD already contains some very limited remedial rights for data subjects in case of profiling and automated decision-making. The 2014 *Google Spain* case gave rise to the highly controversial right to be forgotten, which is incorporated into the GDPR as the right to have one’s personal data erased. The 2015 *Schrems* case annulled the Safe Harbour arrangement between the EU and US, which had allowed companies under the Safe Harbour regime to move data from the EU to the US despite the latter’s lack of stringent data protection law. See *Maximillian Schrems v. Data Protection Commissioner*, C-362/14, [2015] ECLI:EU:C:2015:650. The annulment of the Safe Harbour arrangement by the CJEU led to the replacement by the Privacy Shield in August 2016. Under the Privacy Shield regime, US companies can be certified as safe-third country recipients of data transfer from the EU. It is also incorporated into the cross-border data transfer framework provided by the GDPR.

¹⁰² GDPR, art 12.

information about the logic involved in the automated decision-making, the significance and envisaged consequence of such processing for the data subject,¹⁰³ and to offer human intervention to ensure the data subject's rights when the decision is solely made by automated processing.¹⁰⁴

In addition, the principle of transparency is concretised into a series of technical and organisational measures for data controllers and data processors. In terms of technical measures, as user consent under the GDPR is, “freely given, specific, informed and unambiguous”,¹⁰⁵ entities are required to obtain consent given by a clear affirmative act rather than merely displaying the privacy policy on the company website or using pre-checked opt-in boxes.¹⁰⁶ This means that entities need to create new service-specific user interfaces that enable users to actively give and withdraw consent for each of the envisaged purposes of data collection and processing.¹⁰⁷ As for organizational measures, the GDPR requires entities to record their data processing activities including information such as the purpose of processing and recipients of data transfers.¹⁰⁸ The purpose of the record keeping is to help fulfil the information requests from data subjects and to provide to the supervisory authorities who monitor the data processing upon request. The implementation of this obligation typically requires entities to conduct a sweeping audit of all their departments dealing with personal data.¹⁰⁹ In addition, the GDPR has introduced the Data Protection Officer, a position to serve as a contact point for data subjects and supervisory authorities.¹¹⁰ The Data Protection Officer is required to maintain a neutral position within the entities, advise and monitor the compliance of the GDPR by entities, provide advice regarding the data protection impact assessment, and cooperate with the supervisory authority.¹¹¹

¹⁰³ *Ibid* arts 13(2)(f) and 14(2)(g).

¹⁰⁴ *Ibid* art 22(3).

¹⁰⁵ *Ibid* art 4(11).

¹⁰⁶ *Ibid* Recital 32.

¹⁰⁷ Article 29 Data Protection Working Party, *Article 29 Working Party Guidelines on consent under Regulation 2016/679*, 28 November 2017, WP259 rev.01, 17-20.

¹⁰⁸ GDPR, art 30. The contents of records required for data controllers are more extensive than those for data processors, because general responsibilities of data protection lie with data controllers under the GDPR.

¹⁰⁹ Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer, 2017) at 246.

¹¹⁰ GDPR, art 37. Entities of which the core activities consist of processing that require the regular and systematic monitoring of data subjects on a large scale and those of which the core activities consist of processing on a large scale special categories of data (listed in art 9(1) of GDPR) and personal data relating to criminal convictions and offences are required to designate Data Protection Officer.

¹¹¹ *Ibid* arts 38(3) and 39(1).

While acknowledging the crucial role of transparency for holding companies accountable and re-establishing people's trust and control, the GDPR imposes many other obligations on companies which are not straightforward about transparency vis-à-vis data subjects. Data controllers and data processors have the obligation to ensure the security of data, which requires, among other things, that they ensure the integrity and confidentiality of their processing systems.¹¹² This means that data controllers and data processors are asked to be both more transparent and more secret. Chapter 4 will discuss what this seeming paradox tells about the formalistic disciplining of commercial surveillance and its implication on the human rights encounter. In case of data breach, the data controller has the obligation to notify the supervisory authority about the nature of the data breach, its likely consequence and measures to address it.¹¹³ In addition, two important concepts are introduced: privacy by design and privacy by default. Privacy by design requires data controllers and data processors to develop and use technologies that are minimally invasive (for instance, IT systems directed towards data minimisation¹¹⁴), and timely and comprehensive pseudonymise personal data.¹¹⁵ Privacy by default means that by default, only personal data which are necessary for each specific purpose of data processing are obtained and processed.¹¹⁶ To implement it, the default settings of a service or product should be of maximum privacy protection. So, even if users do not have the technical knowledge or time to implement privacy settings or to monitor the handling of their data by companies (as the principle of transparency aims to enable), they are still protected by the default privacy settings. Another new obligation created by the GDPR for the data controller is to conduct a data protection impact assessment when a type of data processing is likely to result in a high risk to the rights and freedoms of individuals.¹¹⁷ This is an internal assessment which does not need to

¹¹² *Ibid* art 32.

¹¹³ *Ibid* art 33. But there is no absolute obligation to communicate the data breach to the data subject. The obligation of communication of data breach only occurs when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. Communication is not required if the controller has implemented appropriate technical and organisational protection measures to the personal data affected by the personal data breach, or the controller has taken subsequent measures to ensure the high risk is unlikely to materialise, or the communication would involve disproportionate effort. *Ibid* art 34 (1) and (3).

¹¹⁴ Data minimization is a principle of the processing of personal data, which requires the personal data be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. *Ibid* art 5(1)(c).

¹¹⁵ *Ibid* art 25(1).

¹¹⁶ *Ibid* art 25(2).

¹¹⁷ *Ibid* art 35.

engage data subjects. However, if the impact assessment indicates a high risk, the data controller should consult the supervisory authority prior to data processing.¹¹⁸

European legislators have addressed “meaningless consent” and “transparency fallacy” by putting in place the technical, organisational and societal environment to facilitate communication between data-handling companies and individuals. More importantly, they have established internal accountability mechanisms and complemented the limited transparency of a company vis-à-vis the individual with the transparency vis-à-vis enforcement and supervisory authorities. This is also seen by the extensive powers entrusted to the supervisory authorities of EU member states. Compared with their predecessors, under the Data Protection Directive they have much greater investigative powers, subject to the administrative procedural laws of the states where they are established, to monitor and enforce the application of the GDPR and the corrective powers to impose administrative sanctions and fines.¹¹⁹ They also have advisory and authorisation powers, such as to issue opinions to governmental institutions and bodies on any issue related to the protection of personal data.¹²⁰

3. Summary

This Chapter provided an overview of the current mainstream regulatory interventions for state and commercial digital surveillance. From the perspective of the traditional human rights legal framework, state digital surveillance must fulfil the requirements for lawful limitations on fundamental rights and the jurisprudence of the ECtHR on mass surveillance suggests an increasing focus on the provision of formal legal bases and procedural guarantees. However, the traditional human rights framework has significant difficulties in dealing with the paradigm shift brought on by surveillance and intelligence-led law enforcement. In the US, the design of specific legal frameworks for the new model of law enforcement is currently at a preliminary stage due to limited public knowledge, and major initiatives by human rights groups are pushing for the disclosure and democratic input of the use of surveillance technologies by the police and

¹¹⁸ *Ibid* art36, Recital 84.

¹¹⁹ *Ibid* art 58 (1)(2). Whereas the DPD uses opening wording and enumeration to describe the power of the supervisory authorities, the GDPR requires that the supervisory authorities should have all of the listed investigative, corrective and advisory and authorisation powers.

¹²⁰ *Ibid* art 58(3).

courts. In the EU, specific legislation on the protection of personal data, the LEDP and GDPR, were adopted together. The former deals with data protection in the context of law enforcement activities, while the latter addresses any other situations of data collection and data processing, which has brought a sea change in the surveillance-based data-driven business model. The European frameworks grant specific and comprehensive data protection rights to individuals and impose a long list of obligations on data-handling entities based on the general principles of lawfulness, fairness, purpose limitation, data minimisation and storage minimisation, accuracy, integrity and accountability. The European frameworks also establish layers of implementation mechanisms, from the technical design of programs, to the organization arrangement of data-handling entities, and to supervision at national and the EU levels. The burgeoning of new legal instruments and institutional mechanisms to regulate state and commercial digital surveillance reflects the urgent call for law, as a technology of governing, to save the society that is threatened by the negative effects of new technologies, as well as to save law which is accused of either lagging behind technologies or being threatened by the corruption of abusive power using new technologies. The next chapter will critique the regulatory interventions discussed here and examine the irony of this resort to law in an instrumentalist way to save society from the crises posed by digital surveillance.

Chapter 4. A Critical Analysis of the Regulatory Mechanisms: The Second Inscription of the Frankenstein Myth

As seen in Chapter 3, state and commercial digital surveillances are developed either in spite of law or in the absence of law or by circumventing existing law. Prompted by the imminent challenges raised by state and commercial digital surveillance, there is a natural call for law to tame technology and the way it is used, and to reassert basic principles of human rights and rule of law. The current mainstream legal and regulatory interventions offer important frames – individual informational self-determination, legality, transparency and accountability – and valuable tools to tackle the challenges. In the EU especially, new legal regimes are given the teeth to make individual rights actionable. The most important lesson, perhaps, is recognition of the systemic and structural character of the challenges to human rights, which is to say that an idealized liberal subject of human rights is largely handicapped in practice without corresponding institutional and industrial reform to rebalance the power relationship. Accordingly, technological, institutional and social environments all need to be restructured to facilitate the realization of individual human rights in the digital age.

Having said this, it is nevertheless necessary to reiterate the risk of invoking law as merely an instrument to deal with social harms caused by technology. In a linear, problem-solving way, law is easily equated to a set of positivist rules that steer new technology and its application for the public good. But such a positivist and instrumentalist account of law makes law fall prey to the Frankenstein myth, which has to be rescued by either creating more legal instruments or resorting to norms of a higher order than positive law. The unintended consequence of a law based on an instrumentalist conception is alarming since digital surveillance activities often do not emerge in isolation from legal frameworks and are embedded in extant legal regimes. Similarly, the notion of legal vacuum is often a legal construct.¹ Chapter 4 aims to demonstrate the intrinsic paradox of an instrumentalist conception of law in the mainstream approach, a conception which could make the lost human rights encounter in the

¹ Fleur Johns, *Non-Legality in International Law: Unruly Law* (Cambridge University Press, 2013).

context of ubiquitous digital surveillance even more unlikely to be recovered. I will focus on the most developed regulatory regimes – the conventional human rights regimes dealing with state digital surveillance and the EU data protection law addressing commercial digital surveillance, leaving out other preliminary initiatives.

1. Formal legalism and the management of multiple conflicting interests

Throughout the different scenarios of the deployment of digital surveillance, nowhere is the technology or its use straightforwardly outlawed. The instrumentalist account of law does not prohibit but disciplines and manages by laying out extensive and complex conditions for the use of digital surveillance. This managerialism also suggests the different and even mutually conflicting interests and objectives are simultaneously served and balanced, which is very much a reality of the modern social and political affairs. But even if one does not take a strong stand against managerialism, it is still necessary to ask to what extent such managerialism does not deflect principled discussions about normative choices underlying surveillance-based governing.

While the mainstream responses to state digital surveillance criticise that state secret services abusively rely on national security and public interest clauses, human rights legal discourses accept the claim that the secrecy of intelligence work is legitimated by and necessarily required for the protection of national security and the public interest. The mainstream responses therefore focus on detailing the legal conditions and procedures of state surveillance.² By way of such management, the secrecy of state surveillance is remarkably repackaged from something to be cracked to something to be diligently carried out, supervised and hence carefully detoxed from the abuse and corruption of the surveillance agencies. The judicial or quasi-judicial bodies that supervise state surveillance and hear individual complaints wear two hats – the guardians of individual human rights and the guardians of democratic society and, for example, its ample security needs. Arguably, these two roles need not conflict with each other. Yet, the power equilibrium between state and individual is dramatically changed by a ubiquitous digital

² E.g. in *Szabó and Vissy v Hungary*, the ECtHR accepted that “[t]he governments’ more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance – a practice, whose usefulness in combating international terrorism is, once again, not open to question...” see *Szabó and Vissy v Hungary*, No 37138/14 (12 January 2016), para 78.

surveillance that makes individuals increasingly transparent and shifts the presumption of innocence to a presumption of guilt. Accepting the legitimacy of secrecy at the core of the state's coercive power regardless of the radical lack of "secrecy" on the part of individuals makes it impossible for supervisory authorities to mitigate the power asymmetries despite their careful management.

One example is the closed proceedings of the UK Investigatory Powers Tribunal (IPT), the judicial body that was created by the RIPA to hear complaints about unlawful interceptions by intelligence services,³ and was considered as an effective remedy in the *Kennedy v UK* case by the ECtHR. Under IPT Rules 2000, the IPT has the obligation to ensure that the disclosure of information is not contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the state or the continued discharge of the functions of intelligence services.⁴ The IPT has the discretion to hold *inter partes* or separate oral hearings.⁵ In the *Liberty v. UK* proceedings, the IPT kept refusing the requests from the applicants to disclose the closed materials relating to the external arrangements and internal practices of the intelligence services and held a closed hearing to consider those closed materials for the interest of national security.⁶ The case is now being challenged by ten human rights organisations at the ECtHR.

The problem of closed materials and closed hearings has already arisen in the UK's Special Immigration Appeals Commission (SIAC) created after the 1996 *Chahal* judgment of the ECtHR.⁷ In brief, the SIAC works as a court of appeal for deportation cases and it can rely on closed evidence presented in closed-door sessions. There are both similarities and slight differences between the SIAC and IPT. Using SIAC as a point of reference, it is possible to see the immanent unfairness in the closed proceedings of the IPT.

³ *Regulation of Investigatory Powers Act 2000* (UK), c23 ("RIPA"), s 65.

⁴ *The Investigatory Powers Tribunal Rules 2000*, 2000 No 2665, s 6(1).

⁵ *Ibid* s 9. The original section 9(6) which stipulated that the IPT's proceedings shall be conducted in private was found ultra vires section 69 of the RIPA and does not bind the IPT, and the IPT have the discretion to hold public hearings. *Rulings of the Tribunal on Preliminary Issues of Law* [2003] UKIPTrib 01_62 & 01_77, para 173.

⁶ *10 Human Rights Organisations v the United Kingdom*, no.24960/15, "Additional Submission on the Facts and Complaints" (9 April 2015), paras 13-16, 19-21.

⁷ It is established after the European Court of Human Rights held in *Chahal v. UK* that detention pending deportation based on secret evidence that the applicant could not challenge violated the right to fair trial and the right to an effective remedy. See *Chahal v. United Kingdom* (1996), Reports of Judgments and Decisions, 1996-V 1853, 23 EHRR 413, paras 131, 144.

The position of Special Advocate of the SIAC was created to counterbalance the lack of a full, open adversarial proceeding at the SIAC when the detentions of certain detainees are based on closed materials. The Special Advocate attends closed hearings, represents the detainees who are excluded from closed hearings, and cannot communicate with the detainees after seeing the closed materials.⁸ So, the Special Advocate does not enable the full disclosure of evidence to the detainees and cannot mitigate the difficulties of lawyers in representing the detainees.⁹

The IPT invites “counsel to the Tribunal” to participate in the proceeding and make submissions on the closed materials. The role of counsel to the Tribunal is similar to that of *amicus curiae*, and therefore in principle different from the role of Special Advocate of the SIAC. Counsel to the Tribunal does not represent the interests of the party excluded from the closed hearing.¹⁰ When the IPT considers closed materials, the counsel to the Tribunal is expected to make submissions from the perspective of the applicant’s interests, as the applicant is not represented in the hearing.¹¹ So, in practice the roles performed by counsel to the Tribunal and Special Advocate are similar. Like the Special Advocate of the SIAC, counsel of the Tribunal cannot communicate directly with the applicant, take instructions from them and disclose information to them after seeing the closed materials.

Hence, the ITP suffers from a similar problem of procedural unfairness as the SIAC. This unfairness of the system itself results from the intrinsic secrecy and self-judging character of the state’s coercive power, regardless of the integrity of individual judges. The criticism has been levelled that individuals were prevented from encountering and challenging the secret intelligence services before an ordinary judicial body (which does not have the jurisdiction to consider secret surveillance when the national security clause is invoked).¹² However, the avenue of challenging state surveillance is similarly blocked by the IPT that holds closed hearings and claims that the disclosure of certain materials is detrimental to national security and the proper

⁸ *The Special Immigration Appeal Commission (Procedure) Rules 2003*, 2003 No1034, see <<https://www.judiciary.uk/wp-content/uploads/2014/08/siac-rules-2003-consolidated.pdf>>, sections 35, 36.

⁹ Amnesty International, *Left in the Dark: The Use of Secret Evidence in the United Kingdom* (Amnesty International, 2012).

¹⁰ *Liberty and others v GCHQ and others* [2014] UKIPTrib 13_77-H, para 8.

¹¹ *Ibid* para 10.

¹² Dider Bigo et al, *National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges*, Study for the LIBE Committee (Directorate-General for Internal Policies, Policy Department C: Citizens’ Rights and Constitutional Affairs, European Parliament, 2014).

performance of duties by intelligence services. The former eliminates the human rights encounter by carving out the function of domestic courts and creating a legally-sanctioned vacuum. The latter, special oversight procedures such as the IPT, in effect further normalizes the already legally-sanctioned secrecy. The normalization of secrecy through the special oversight procedures exemplifies an inherent paradox in disciplining and managing surveillance, namely that surveillance is required to be both more secret and more transparent. This paradox is made inevitable when national security is invoked to be the basis and purpose of state surveillance.

The problem in the IPT is not just about the deficiencies of procedural justice in the oversight bodies. It is important to bear in mind that the constitution of oversight bodies such as the IPT and the SIAC is also a consequence of the implementation of human rights standards by states, and hence the problem reflects a more fundamental dimension of reliance on formal legalism and the proceduralization of human rights protection. Under the human rights legal framework, the requirements of the accessibility and sufficient clarity of law are part of the requirement of being “in accordance with the law,” and are minimum criteria for a thin conception of the rule of law.¹³ An instrumentalist account of law, approaching law as morally neutral, allows for the separation of those formal requirements from normative values of justice and individual dignity, and empowers state surveillance agencies by way of disciplining. The framing of the problem as lack of formal legal basis and procedural guarantees should be treated with reasonable scepticism and considered together with law’s role of maintaining a self-referring and self-judging loop of state surveillance. In state digital surveillance, central secrecy is maintained and practiced by complicated layers of regulation that detail the procedures of surveillance, the mandates of surveillance agencies, the report and supervision procedures, and the establishment and mandates of supervisory authorities, etc., all in the name of being “in accordance with the law”.

A recent judgment at the ECtHR follows this managerial approach, one that flattens legality into legalism even further. As already discussed, the ECtHR has been focusing on procedural review rather than deciding on its own on substantive questions like the proportionality and necessity of the surveillance measures. The Court’s procedural turn has its

¹³ The instrumental purpose, argued by Joseph Raz, is the efficiency of the operation of law. Law, seen as instrument, has no intrinsic moral content but moral neutrality, which allows law to be used for various purposes. Joseph Raz, “Rule of Law and its Virtue” in *Auth Law Essays Law Moral* (Oxford: Clarendon Press, 1979) at 226.

specific reasons (*i.e.*, the question of the democratic legitimacy of the Court and the subsidiarity of the Court), but in effect it reinforces sovereign discretion of state in ensuring its surveillance is compliant with human rights standards. In *Big Brothers Watch v. the UK*, the Court recognized that “the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States’ margin of appreciation.”¹⁴ It hence recognized that states could have bulk surveillance in their arsenals subject to certain procedural conditions mentioned in Chapter 3.¹⁵ To recall how bulk surveillance transforms individual subjectivity (discussed in Chapter 1), such acceptance of bulk surveillance also led to the Court’s claim that there was no “necessary requirement” for objective evidence of reasonable suspicion, which significantly departed from its previous cases that dealt with Russian and Hungarian bulk surveillance programs.¹⁶ Furthermore, the Court acknowledged the oversight bodies (*i.e.*, the Interception of Communications Commission and the IPT) provided effective guarantees against the abuse of power. In its proportionality assessment, the Court also relied on the assessment of a domestic body, the Independent Reviewer of Terrorism Legislation, which claimed that no alternative or combination of alternatives could substitute for bulk surveillance.¹⁷ Having given states considerable deference with regard to the operation of bulk surveillance and oversight procedures, the Court nevertheless found the use of selectors and search criteria to filter the mass captured data a violation of Convention Art.8. The reason is that the search criteria and selector were not subject to independent oversight.¹⁸ Clearly, this is where the Court tried to discipline mass digital surveillance by way of formal legalism while simultaneously avoiding normative assessment of the human rights implications of bulk data collection the processing of collected data in the first place.

¹⁴ *Big Brothers Watch and Others v. the United Kingdom*, nos.58170/13, 62322/14/14, 24960/15, 13 September 2018, para.314.

¹⁵ See Chapter 3, section 1.1.1 on the six minimum safeguards established by the Court in *Weber and Saravia v. Germany*: the statute law should (i) contain clear and detailed rules that identify the nature of the offences which may give rise to an interception; (ii) provide a definition of the categories of people liable to have their communications intercepted; (iii) set out a limit on the duration of interception, (iv) the procedure to be followed for examining, using and storing the data obtained, (v) the precautions to be taken when communicating the data to other parties, and (vi) the circumstances in which recordings may or must be destroyed.

¹⁶ *Supra* note 14, paras 317-318.

¹⁷ *Ibid*, para 384.

¹⁸ *Ibid*, paras 346-347.

The regulatory regime for commercial digital surveillance also exhibits this managerial approach to addressing conflicting interests that maintains the extant power imbalance. It is crucial to notice that in the most rights-centred, interventionist European Union, the GDPR was adopted for another important reason than rights themselves, *i.e.* the development of a digital economy within the EU internal market.¹⁹ European legislators do not see this goal as conflicting with individual rights and claim that the enhancement of data protection can create the trust which is needed for the development of the digital economy.²⁰ This view that rights-protection and the development of the digital economy can go hand-in-hand is consistent with the strand of liberalism that sees the protection of individual rights as compatible with economic liberalization. This strand of liberalism sees broad parallels between freedom in the economic sphere (*e.g.*, free movement of trade, labour and property) and freedom in the political sphere (*e.g.*, freedom of expression and association), and between individuals as consumers in the free market and individuals as voters in an electoral democracy.²¹ These parallels seemed almost self-evident especially since the Cold War and the collapse of the command economy.

There are ample studies that suggest both that this ostensible connection between rights-protection and capitalist economic liberalisation is historically contingent and that the historical conditions for that connection have been fundamentally changed by financial capitalism.²² Without engaging too much with that literature, it suffices to say the difficulties in reconciling the two objectives are reflected in the law-making process itself. The negotiation of the GDPR and ePrivacy was marked by heavy lobbying and criticisms from different interest groups. The most typical criticism from the business sector was that regulation with too much teeth would curb innovation and would be especially damaging to small and mid-size enterprises;²³ by

¹⁹ GDPR, Recitals 7&9.

²⁰ *Ibid*, Recital 7.

²¹ *E.g.* David Beetham, “Market economy and democratic polity: Democratization” (1997) 4:1 Democratization 76.

²² Wolfgang Streeck, *Buying Time: The Delayed Crisis of Democratic Capitalism* (Verso, 2014) at 14–16; Daron Acemoglu & James A Robinson, *Why Nations Fail: The Origins of Power, Prosperity, and Poverty* (Crown Publishers, 2013) at 308–314; Roberto Mangabeira Unger, *Free Trade Reimagined: The World Division of Labor and the Method of Economics* (Princeton University Press, 2007) at 9 [“The concept of a market economy is institutionally indeterminate. That is to say, it is capable of being realized in different legal and institutional directions, each with dramatic consequences for every aspect of social life, including the class structure of society and the distribution of wealth and power.”].

²³ *E.g.* the Interactive Advertising Bureau Europe was “dismayed” by the European Commission’s e-Privacy regulation proposal. “While the Commission finally acknowledged the important role of advertising for funding free content online, it does so at the same time as presenting a law that as a practical matter would undeniably damage the advertising business model – without achieving any benefits for users from a privacy and data protection point of

contrast, for rights advocacy groups, the GDPR, which leaves room for co-regulation with industries, was still not comprehensive enough.²⁴ The fundamental question is what to do with the default business model, which alienates people and fabricates capital values detached from individuals.²⁵

The different lobbying and criticisms reflect difficult normative divides which will reappear in practice despite being glossed over by data protection law. Most remarkably, by creating a detailed legal regime to protect personal data and equipping it with strong authorities to supervise its implementation, the European data protection law could encourage surveillance technologies that can dispense with personal data. Technologies such as anonymization can render data non-personal and hence outside the scope of the law. It would seem such technologies protect the data subject from unwanted identification and associated consequences. However, from the perspective of a new logic of governing formed by surveillance and data analytics, such technologies which decontextualize data remove the human rights encounter by distancing the data subject even further from the process of data production and decision making. The value of anonymized data for analysing and training new analytical models is reduced. However, bearing in mind the “new oil” metaphor, companies do not throw away such anonymized data, but aim to make them useful again. The solution is again, technical. For example, through so-called “deep natural anonymization” technology, personal data, such as faces and license plates detected from a surveillance video, can be replaced. The replacement is said to match certain attributes of the source data for the purpose of analysis.²⁶ Such technical solutions raise many problems which are not new to surveillance-based governing – e.g., who gets to decide what attributes to maintain or not, the problem of unintended bias in the analytical model developed by replaced data. More important for the purpose of current discussion is that the rigorous protection of personal data under the European data protection law can unintendedly

view.” “IAB Europe Press release: Proposed ePrivacy Regulation Fails To Improve Cookie Rules | IAB Europe”, (10 January 2017), online: <<https://www.iabeurope.eu/policy/press-release-proposed-eprivacy-regulation-fails-to-improve-cookie-rules/>>.

²⁴ E.g. Access Now, *Creating a Data Protection Framework: a Do's and Don'ts Guide for Lawmakers* (Access Now, 2018).

²⁵ See discussions in Chapter 2, section 1.2.

²⁶ Brighter AI, “How to increase the value of your anonymized data? - Generate Vision”, (15 October 2018), online: *Medium* <<https://medium.com/generate-vision/how-to-increase-the-value-of-your-anonymized-data-c182ba4fc8db>>.

encourage new forms of surveillance and means of surveillance-based governing that are outside of its regulatory scope.

Moreover, the European data protection law can also encourage the kind of business activities that outsource the collection and processing of personal data to entities not subject to the GDPR and obtain from them processed data products. For example, an EU-based company working on artificial intelligence can arrange with a company based in China which collects personal data of Chinese users to train and test their AI program.²⁷ No human rights encounter would happen between the Chinese users and the EU-based company. The circumvention of the European data protection law is made possible by disparities across data protection of different jurisdictions, which is nothing new to global economic governance and the global value chain. Arguably, Chinese users would only have their own government to blame for not adopting a data protection law like the GDPR. The point I want to make is that the management of different and mutually-conflicting interests through a legalistic approach which strictly demarcates the regulatory field can simultaneously lead to new conditions of and possibilities for surveillance capitalism. The management of conflicting interests does not resolve the normative conflict. It only displaces it, creates different negative externalities and redistributes them elsewhere. Such unintended potential consequences resulting from a strong data protection law for the digital economy and other jurisdictions demonstrate the Frankenstein myth of the instrumentalist and technical discourse of law.²⁸

Turning back to the data protection law itself, the management of conflicting interests is expressed in the article of the GDPR that provides the “legitimate interest” of the companies as a

²⁷ This outsourcing of data collection has already existed and criticised. Oscar Van Heerden, “Africa remains a captive market – are we truly au fait with technology?”, (27 June 2018), online: *Dly Maverick* <<https://www.dailymaverick.co.za/opinionista/2018-06-27-africa-remains-a-captive-market-are-we-truly-au-fait-with-technology/>>.

²⁸ To consider the “unintended consequences” does not aim to blame the law for not being sufficiently inclusive. Any law-making exercise includes and simultaneously excludes certain spaces, subjects and relations. See Hans Lindahl, *Fault Lines of Globalization: Legal Order and the Politics of A-legality* (Oxford, United Kingdom: Oxford University Press, 2013). To regulate activities and relationships mediated by the global internet and imbricated with global capital flow, the authors of any law-making exercise have to be mindful of the implications on the larger geo-economic circumstances. Drawing from Levinas (as will be see in Chapter 6), I argue that this mindfulness is, in a sense, a responsibility of one legal collective toward its other and this responsibility does not lead to imposing the same law on the other but rather, encourages the communication and cooperation of different legal collectives to foster legal melange.

legal basis for the processing of personal data without clearly defining “legitimate interest”.²⁹ Such data processing does not require the consent of concerned data subjects. While such processing still needs to fulfil the data protection principles and procedural requirements (*e.g.*, the data protection impact assessment, as will be analysed below), and the legitimate interests should in principle not override individual rights,³⁰ it remains in fact a self-judging process where the company balances self-defined interests with individual data protection rights. An individual does have the right to object to such processing, but the company is not required to stop such processing if it can demonstrate compelling legitimate grounds for the processing which overrides individual rights.³¹ “Compelling legitimate grounds” seems stricter than simply “legitimate interests” and the burden of proof is on the company, but the balancing exercise is still within the company’s discretion.³² The maintenance of such a self-judging and self-referring process which exacerbates the power imbalance between individuals and companies is very similar to that discussed earlier in the context of state surveillance.

2. Increased bureaucratisation leading to more accountability loopholes

Closely related to the previous point is the increasing bureaucratization of digital surveillance. Accountability mechanism-building is a major task of the regulation of state and commercial digital surveillance to prevent the abuse of power, but depending on how accountability is understood, accountability mechanisms do not necessarily facilitate individual encounters with the institution. For state surveillance, accountability mechanisms are established to prevent abuse of power by the surveillance services and to protect democracy. Accountability mechanisms usually take the form of internal review, review by special administrative bodies or by authorities

²⁹ GDPR, art 6(1)(f).

³⁰ *Ibid*, art 6(1)(f) and Recital 47.

³¹ *Ibid*, art 21(1).

³² Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision Making and Profiling*, 3 October 2017, WP251rev.01, at 19.

external to the executive, or by a hybrid body.³³ The ECtHR also acknowledges that the effective remedy requirement can be met by the aggregate of remedies provided by domestic law.³⁴

The problem is that these review bodies are established by and entrenched in a huge bureaucratic state and subject to the internal politics of bureaucracy. The sheer scale of the surveillance operations of a state means that the supervision of surveillance services needs to be split up and shared by different supervisory bodies, which creates a problem of coordination between them. For example, a report has found that the US Department of Homeland Security (DHS) has been overseen by a hodgepodge of 92 congressional oversight bodies since 2014. The congressional oversight remained dysfunctional as most of the bodies could not develop expertise on the DHS as a whole, nor understand the DHS's overall mission. This fragmentation was criticised for being complicit in squandering DHS resources.³⁵

Other typical difficulties these mechanisms suffer from include the shortage of budget, human resources and expertise. They are also often politically weak compared with the government and the intelligence services that wage the “war on terror”, which makes it more difficult to gather the necessary resources for the task of supervision.³⁶ In addition, accountability mechanisms are often separate from complaint mechanisms, which means that the authorities supervise the operation of state surveillance and answer to their parent body such as the head of government or the parliament, but do not directly communicate with or answer to the individuals who are affected.³⁷ Even if supervisory authorities contain procedures for individual complaints,³⁸ they do not enable individuals to pierce the complex veil of bureaucracy to

³³ E.g., Council of Europe PA, Resolution No 2045, *Mass Surveillance*, 2nd part Sess, Texts Adopted (2015); Council of Europe, European Commission for Democracy Through Law (Venice Commission), *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*, 102nd Plen Sess, CDL-AD (2015) 006 (“the Venice Commission report”).

³⁴ *Leander v Sweden* (1987), 116 ECHR 9Ser A), 9 EHRR 433, paras 81-84. See also *Chahal v. United Kingdom* *supra* note 6, para 145.

³⁵ See Bipartisan Policy Center & the Annenberg Public Policy Center of the University of Pennsylvania, *Today's Rising Terrorist Threat and the Danger to the United States: Reflections on the Tenth Anniversary of the 9/11 Commission Report* (2014) at 21.

³⁶ Amy B Zegart, “The Domestic Politics of Irrational Intelligence Oversight” (2011) 126:1 Polit Sci Q 1.

³⁷ E.g., The Interception of Communication Commissioner annually reports to the Prime Minister on the exercise of his or her function and reports to the Prime Minister if he or she finds a violation of the RIPA or its safeguards are inadequate. While it claims that it is outward-facing and communicates with the public by speaking at conferences and publishing papers, it does not have the power to refer cases to the IPT or notify the victim of any excessive or unlawful interception. See, RIPA, *supra* note 2 sections 57 and 58.

³⁸ The Venice Commission updated report on signal intelligence mentioned the complaint mechanism provided by the Swedish Signals Intelligence Act, which allows any individual to request the controlling authority to check

encounter the state surveillance apparatus, as indicated by the early example of the IPT's closed proceedings. In short, accountability mechanisms do not always facilitate individual-institution encounters; they can function like a one-way mirror – reflective from one side and transparent from the other, also demanding trust from individuals in the rationality and self-cleansing capacity of the institution, a trust that has been compromised in the power relationship of surveillance.

For commercial digital surveillance, the GDPR has designed accountability mechanisms inside and outside data-handling companies. Outside private companies, the GDPR set up national supervisory authorities and EU-level cooperation and consistency mechanisms to help the implementation of the GDPR across the EU. I will not dispute their importance by speculating on their effectiveness at this stage. Suffice it to say that a repeated question for such national and regional bodies is how they can secure necessary resources from each Member State for their effective functioning.³⁹ I want to focus more on bureaucratization within the data-handling companies which does not really make them approachable for individuals.

To begin with, it is necessary to note that the paradox of requiring more secrecy and more transparency in the disciplining of surveillance also exists here. Data-handling companies have legal obligations to ensure the security of data from potential data breach. This accordingly requires a range of technological and organizational arrangements on the part of companies, especially in respect of the confidentiality of their processing systems. Arguably, confidentiality and transparency are not contradictory in the sense that the right to information of data subjects does not amount to the right to know about the technical specificities of the processing systems of the data controllers or processors. However, this way of demarcating transparency and confidentiality suggests that, to be responsible guardians of individual data, data-handling companies have a certain range of legally-sanctioned discretion which is not challengeable in individuals' encounters with the data-handling companies.

whether his or her messages have been collected under this Act and whether the collection and processing of the data are lawful. The controlling authority has the obligation to inform the individual that the check has been performed. The report also mentioned the internal complaints advisory committee of the Dutch oversight body, the CTIVD. The Venice Commission report, *supra* note 25 at 39.

³⁹ There were difficulties for the supervisory authorities in the DPD for the lack of necessary resources. David Wright, David Barnard-Wills & Inga Kroener, *Deliverable 4: Findings and recommendations* (PHAEDRA, 2015) at 20.

Accountability mechanisms within the company, more specifically, take the form of the company's self-regulation through the record keeping of data processing, the designation of a data protection officer and, data protection impact assessments. While the data protection officer answers to data subjects and supervisory authorities, record-keeping and data protection impact assessments are outward-facing in a very limited sense. The tool of record keeping is supposed to help answer the information requests of data subjects, but the GDPR limits the data subject's right to information if the provision of the information would involve "a disproportionate effort" by the data controller.⁴⁰ Meanwhile, the GDPR does not specify the level of detail of the processing records, which leaves the data controller the discretion to determine how detailed the records ought to be and whether an information request calls for disproportionate effort (unless supervisory authorities or courts determine the standard when actual cases arise). Here again is an example of managerialism that seems to address different interests by giving the discretion of balance to the powerful party.

With respect to data protection impact assessments, data-handling companies only have the obligation to consult the data protection officer and no obligation to seek the views of the data subjects on the intended processing and therefore, the assessment can be done entirely internally. Meanwhile, reasonable suspicion should be afforded when considering the rationale and function of the tool of impact assessment that ensures bureaucratic rationality. A similar tool of human rights impact assessment has already been advocated and used in the business sector with controversial effect. Such impact assessment tools translate normative human rights concepts to quantifiable business risks and also produce certain forms of knowledge on human rights compliance underpinned by business/market rationalism. From a critical studies perspective, such translation by the companies which demonstrate their human rights "performance" often does not lead to actual change of business practices or to improved compliance with human rights obligations.⁴¹

The translation of obligation through impact assessments is likely to be a serious issue in the context of data protection. As the GDPR defines "personal data" in a very broad way, it is

⁴⁰ GDPR, Recital 62 and art 14(5)(b). This limitation applies also to the obligations regarding rectification or erasure of personal data or restriction of processing (art 19), the obligation to communicate the data breach to the data subject (art (3)(c)).

⁴¹ Christian Scheper, "From naming and shaming to knowing and showing": human rights and the power of corporate practice" (2015) 19:6 Int J Hum Rights 737.

arguably possible to cover virtually all types of data and data processing (except anonymized data), and the GDPR would become, in effect, “the law of everything”.⁴² If that is the case, the broad application of the GDPR will create compliance problems for itself. Virtually, companies (fulfilling the requirement of territorial applicability) that have any business related to the digital economy could be imposed upon by the GDPR’s extensive positive data protection obligations and also the obligation to demonstrate on-going compliance. With this in mind, it is possible to conceive backsliding situations where those internal accountability mechanisms could only manage the performance of data protection obligations and are not really conducive to enhanced protection of individual personal data. It is also interesting to note that along with the adoption and implementation of the GDPR, the business of data protection risk mitigation has also emerged. This business provides compliance toolkits that are relatively easy to incorporate into a data-dealing company’s information system.⁴³ The option of outsourcing and even automating compliance with data protection obligations becomes increasingly available and cheaper. Whether these tools make any substantive changes to business activities, there is a real concern that the heavy obligation of ensuring institutional accountability under the GDPR could be responded to by introducing an additional element of bureaucratic obscurity.

Another factor of bureaucratic obscurity is co-regulation. Co-regulation expresses the idea that government and industry work together to define and enforce standards to regulate business. The GDPR allows and encourages the adoption of a code of conduct, the use of a certification mechanism, standard contractual clauses and binding corporate rules to facilitate and demonstrate a company’s compliance with the GDPR. While proponents of co-regulation argue that it eases and fast-tracks a company’s implementation, (especially for a small or medium-sized entity), and facilitates monitoring by the supervisory authorities, it also creates more bureaucratic complexities. For example, codes of conduct create their own monitoring mechanisms which need to be accredited by competent supervisory authorities.⁴⁴ It is claimed

⁴² Nadezhda Purtova, “The law of everything. Broad concept of personal data and future of EU data protection law” (2018) 10:1 Law Innov Technol 40.

⁴³ E.g. “PIA & DPIA Automation | Products”, online: *OneTrust* <<https://www.onetrust.com/products/assessment-automation/>>; “Nymity’s Software Solutions for the privacy office”, online: *Nymity* <<https://www.nymity.com/solutions/>>; “GDPR Compliance Solutions - Platform and Consulting”, online: *TrustArc* <<https://www.trustarc.com/products/gdpr-compliance/>>; “Evidon | Universal Consent Platform for Site, App, and Ad Compliance”, online: *Evidon* <<https://www.evidon.com/solutions/universal-consent/>>.

⁴⁴ GDPR, art 40(4).

that third-party monitoring bodies can reduce the workload of supervisory authorities, given that they actually have expertise in relation to the subject-matter of the code of conduct, the power to monitor committed companies, and can take measures when the code of conduct is infringed. Nevertheless, the big unknown is how this would be realized in practice. The failure of the third-party audit in the Facebook's Cambridge Analytica scandal is a timely warning of the limits of co-regulation.⁴⁵

Having laid out all these questions about the increasing bureaucratization of digital surveillance, it is interesting to note again that technologies like big data analytics, machine-learning and artificial intelligence have been advocated precisely for the purposes of making bureaucracy more transparent and accountable and less complicated, preventing human mistakes and making decisions more objective and evidence-based. It is the realization that machines also make mistakes, that machine-made decisions are not transparent, that human preferences are ingrained in machines and that machines can be the excuse to shake off responsibility, which leads to solutions that “keeping humans in the loop” as well as to other conventional tools of bureaucratic management to ensure accountability and transparency. Such a circular move – that solutions can cause the same old problems – evokes long-lasting anxieties about the monstrosity of modern bureaucracy. It is certainly reasonable to tame bureaucracy by having human and machine check each other. It is also conceivable that this mutual check can lead to a greater consolidation of bureaucratic impersonality and rationality, which removes what is unexpected as well as the contestability of decision. From this perspective, the innovative tools of privacy by design and privacy by default as introduced in the GDPR, by which data protection obligations are implemented by technological arrangements of the data controllers, can also be questioned as to how they could avoid contributing to the technological enclosure of digital surveillance. As will be discussed later in Chapter 6, unexpectedness is a key character of the human rights encounter, whereas the contestability of a decision is not a vice but a virtue from the perspective of the rule of law.

⁴⁵ See Chapter 3, note 91.

3. Conclusions: from futility to perversity

In Chapters 3 and 4, I have described the mainstream regulatory interventions addressing the deployment of digital surveillance by public authorities and the private sector. The common problem framing and solutions regarding the legality, transparency and accountability of the surveillance activities are underpinned by important rule of law principles and basic human rights notions. They benefit from rich judicial practices and theories that seek to establish just and fair relationships between individuals and powerful institutions and they provide valuable discursive and conceptual tools to reassert individual dignity and autonomy in a world of ubiquitous digital surveillance.

Nevertheless, the mainstream regulatory responses also fall prey to the double-inscription of the Frankenstein myth. While invoking law to tame technology and mitigate its negative social effects seems natural and necessary, I argued that there is an inherent risk in the positive and technical account of law. This account, essentially similar to the idea of technological neutrality, enables the detachment of law from its normative underpinnings, flattens legality to formal legalism, and makes bureaucratic accountability non-sensible to anyone outside the bureaucracy. The idea of technological neutrality suggests that a legal regime can serve multiple purposes through careful management and balance of different interests. Protecting individual human rights is balanced with ensuring the proper function of the state's coercive power or with the development of the digital economy. These objectives in the abstract are not necessarily incompatible with each other; the competition of multiple interests has always been a reality of liberal democracy. The rule of law and accountability mechanisms have been developed precisely to make different values and objectives go hand-in-hand.

However, they are made radically incompatible as ubiquitous digital surveillance, which has become an essential component of the new form of governance and economy fundamentally changes the power equilibrium between individuals and surveillance actors. Responding to the radical asymmetric relationship, an instrumentalist account of law that pretends to be value-neutral and to manage different objectives only glosses over their deep incompatibility. As Don Ihde has said about technical artefacts, technologies always encourage certain ways of perception and practice while inhibiting others.⁴⁶ An instrumentalist and technical account of law can be

⁴⁶ Don Ihde, *Technics and praxis*, Boston studies in the philosophy of science 24 (Dordrecht: Reidel, 1979) at 21.

understood in a very similar way. There are presumed value choices underlying the encouraging-inhibiting scheme. The question then is not just whether new regulatory regimes are effective in enabling individuals and cracking open the black boxes in practice; that is to say, the effectivity or futility of regulatory regimes is not the most important question. The more critical question is what kind of individual-institution relationship is encouraged and what kind is inhibited by regulatory regimes. This question will be explored next in Part III.

For both state and commercial digital surveillance, legalism, bureaucratic accountability and transparency are invoked increasingly as knee-jerk reactions with highly questionable effects. The discussion here in Chapter 4 has argued that current regulatory regimes have themselves contributed to additional difficulties for individuals to encounter institutions. Some impediments are due to the increased bureaucratization which only ensures internal bureaucratic rationality and is not concerned with how to redress the lost human rights encounter. This is seen in the example of the judicial oversight of state digital surveillance, which legitimizes the lack of human rights encounter and is also seen in the example of companies outsourcing and automating compliance with data protection obligations.

Some impediments are arguably unintended consequences of a rigid and enforceable law that seeks to rebalance the power relationship. This was shown in the example of the GDPR, which could conceivably contribute to a global value chain of the surveillance economy that disperses more widely the human rights encounter between individuals and surveillance companies in an already unfair global economic structure. What follows an instrumentalist account of law would be more legal instruments and bodies to deal with newly emerging accountability loopholes. Such problem solving is likely to be circular; what appears to be the solution ends up creating more problems. While it is surely not a new phenomenon in law and perfecting the law is always a long-term and collective commitment, it is necessary to pause and ask how and when the legal craftsmanship,⁴⁷ increasingly informed by managerialism, results in a monstrous consolidation of formal legalism, bureaucracy and technological-fundamentalist rationalism.

⁴⁷ See discussion on “crafting” the rule of law in Chapter 6, Section 3.2.

Interim conclusions

Parts I and II of this study have followed a scheme, the double-inscription of the Frankenstein Myth. Part I described several scenarios in which digital surveillance is deployed by public authorities and private actors and the challenges this development poses to human rights. The challenges to individual fundamental freedoms such as the right to be heard, non-discrimination, the presumption of innocence and self-determination, are inevitably related to and implicate the rule of law principles and values of liberal democracy. Without exaggerating, these challenges relate to our existential conditions which are being reconstructed by ubiquitous digital surveillance and the use of big data analytics. In less legalistic terms, Zuboff has spoken about the individual's right to the future tense as well as their the right to sanctuary to describe the existential challenges that the new surveillance-based logic of capitalism has brought about.¹ In Part I, I also discussed the elimination of the human rights encounter, the transformation of the most basic conditions which enable individuals to encounter institutions, and to invoke their human rights against the regulatory powers of institutions whether legally entrusted or self-conferred. State and commercial digital surveillance disperses the space and time of the human rights encounter through technological and organizational arrangements. It is not enough to label state and commercial surveillance activities black boxes; these activities exhibit highly complex, dynamic and inexplicable "global value chains" which are embedded in international cooperation and the global economy. Ubiquitous surveillance also transforms individual subjectivity by producing and acting on probabilistic knowledge concerning human beings and human behavioural patterns. These transformations of the basic conditions of human rights encounters when surveillance is used for law enforcement also profoundly implicate the operation of law. Moreover, a feedback loop is created in which surveillance-based governance and business practices create the conditions for human behaviour that reinforces the behavioural patterns they produce and rely on. This is also the case in governance-by-nudging and in that situation, more critically, people's behaviours and choices are conditioned by the choice architecture which has

¹ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019), chs 11, 17.

already optimised a certain course of action without forcing or compelling individuals. A human rights encounter with the institution is hence also dissolved by fundamentally changing how power is exercised and perceived to be exercised, from a confrontational relationship where individuals can say no to the coercive power of the institution into a seemingly friendly one where individuals enjoy an illusory sense of self-determination.

Part II moves to discuss current regulatory regimes and mainstream approaches of addressing the challenges posed by state and commercial digital surveillance. The common black box imagery of surveillance understandably leads to the common problem framing that focuses on the legality, transparency and accountability of surveillance actors. Individual rights are claimed to be essential, and in the field of data protection in particular, new rights of personal data protection are created and made actionable. The main focus remains on the disciplining of surveillance institutions. This is necessary because the realization of individual rights is always subject to social conditions and the power structure of the individual-institution relationship. Legality and accountability are the useful conceptual and discursive tools that are developed from rich human rights jurisprudences and scholarships to rectify the unbridgeable power asymmetry between the surveilled and the surveillant. However, as argued in Part II, I observed a problematic tendency in mainstream regulatory responses which routinely invoke legal basis and bureaucratic accountability to (micro)manage surveillance activities. The source of the problem is an instrumentalist, technical account of law that is increasingly detached from the theoretical underpinnings of the rule of law and human rights. The political and legal reactions to digital surveillance of the past few years have gradually moved from strong, principled criticisms to more detailed, fine-tuned and technical assessment of the purposes and procedures of digital surveillance, and the possibilities of more effective and efficient governance and stronger economy that the technologies promise are unlikely to be questioned by judicial authorities and legislators. The technical conception of law that claims to be value-neutral and claims that we can both have the cake and eat it inevitably puts the law itself at the risk of disempowering individuals, creating more obstacles for the human rights encounter, and reinforcing the existing power asymmetry.

As Tranter has observed, the problem of the double-inscription of the Frankenstein myth is caused by a very reductive view of both law and technology which sees them as just objects of a sovereign will, created from an unknown space and inserted into society *post facto*. These

objects have great potential for the public good but can also go terribly wrong and need other instruments to keep them in check. The double-inscription also gives the view that technology and law are ontologically separate fields. Legal regulation is the secondary or tertiary effect of technology, and hence the common perception of law lagging-behind technology appears inevitable.

At first glance, this view has some important descriptive values. It is very true that legal regimes are often created in response to sociopolitical crises. It is also true that many new social relations enabled by new technologies are caught in a legal grey zone, or are considered a-legal, and that people need law to help them orient in the new technologically mediated relationship. But the scheme of the double-inscription and its underlying positivist and technical view of law (and equally reductive view of technology) are limited in several senses.

First, the scheme of the double-inscription and the underlying conceptions of law and technology do not take into account the complex entanglement between technology and law. As Part I and Part II have demonstrated, digital surveillance activities often do not come out from complete legal lacunae. They are more often developed in spite of existing law or by manipulating existing law. This is actually also why the corruption of the existing legal system is considered so damning and more problematic than the mere lack of law. The absence of law of course entails the abuse of power, but corruption of the rule of law and treating legality only as formal legalism would legitimise the abuse of power with legal technicality which is supposed to tame the power. The permitting-inhibiting structure of legal regimes makes it inevitable that law itself implies the possibility of circumvention through ingenious legal techniques,² and such possibility of circumvention is not necessarily always triggered by new technologies. For example, the international intelligence liaison that bypasses the territorially-partitioned legal protection of human rights and other domestic constitutional and administrative legal constraints has existed before the invention of the internet. When new technologies seem to create a legal vacuum, it is often possible to configure the legal matrix where the vacuum is situated. For example, in the case of state law enforcement relying on surveillance technologies, the obscurity surrounding the technology transfer from the private sector to the public, from the military to the

² Again, referring to Johns' observation, "non-legality is, in its own right, a central structuring device of international legal thought and work". Fleur Johns, *Non-Legality in International Law: Unruly Law* (Cambridge University Press, 2013) at 11.

civilian and the black box of accountability for decisions involving automation are often the effects of pre-existing legal regimes that legalized the considerable discretion of policing authorities and gave commercial entities significant autonomy (e.g., with intellectual property law). This is not to say that technologies do not create new ways of distorting the law, but the problems are often new manifestation of old ones ingrained in extant legal regimes – e.g., the privilege of private business enterprises, the deference given to the military and the intelligence services of the state.

Second, the complex entanglement of technology and law is not just similar to the chicken or the egg question; in a more fundamental sense, both technology and law mediate and are constitutive of our perception and action.³ In this sense, I do not consider a technical discourse of law as mistaken as such, but a reductive view that disregards this formative role of technology that is often implied in the technical discourse of law is problematic. Pre-existing understandings and practices of law help us perceive the challenges created by digital surveillance. Law is not reactive, but actively frames our perception and language to make comprehensible certain relationships and phenomena caused by new technologies. This is perhaps the most enabling effect of law. The fact that mass surveillance and its black box character raise human rights challenges and that the right to privacy, for example, has undergone a significant conceptual crisis is due to the pre-existing conception and practice of human rights law that have constituted the frame of reference for understanding new social phenomena. In a radically different socio-legal culture where collective interests always take priority over individual rights and where “privacy” does not enter into common discourse, mass surveillance raises completely different questions. Conceivably, discussions can be directed toward how to make it efficient, how to reduce costs, or how to create a powerful organization in the face of competing political factions, rather than toward the consideration of the rule of law and human rights.⁴ It is indeed the case that ubiquitous surveillance points to some fundamental

³ For discussions on technology’s mediation of human perception and action, see Peter-Paul Verbeek, *Moralizing technology: understanding and designing the morality of things* (Chicago ; London: The University of Chicago Press, 2011); Don Ihde, *Technology and the Lifeworld: from Garden to Earth* (Indiana University Press, 1990); Don Ihde, *Technics and praxis*, Boston studies in the philosophy of science 24 (Dordrecht: Reidel, 1979); Bruno Latour, “On Technical Mediation: Philosophy, Sociology, Genealogy” (1994) 3 *Common Knowl* 29; Mithun Bantwal Rao et al, “Technological Mediation and Power: Postphenomenology, Critical Theory, and Autonomist Marxism” (2015) 28:3 *Philos Technol* 449.

⁴ Rana Mitter et al, *BBC World Service - The Real Story, China’s Big Social Experiment*.

vulnerabilities of liberal human rights and legal regimes, but the perceptibility of the problems framed in the language of the rule of law and human rights demonstrate the very active and constitutive role of law that mediates the human-human, human-technology and human-institutions relationships. Meanwhile, the conceptual and perceptive framework entailed by existing law inevitably exclude other ways of disclosing and interpreting the reality.⁵

These are just some ideas inspired by the literature on the philosophy of technology and on law and language. What follows from these ideas – the formative character of technology, the non-neutrality of the encouraging-inhibiting structure, and the inseparability of law and technology that renders reality comprehensible – are a series of questions that are not considered in the scheme of the double-inscription. For example, it is possible to ask how the elimination of human rights encounter in the context of ubiquitous digital surveillance is co-constituted by modern law and the power of surveillance, and specifically, what kinds of encounter between individual and institution are invited (or otherwise inhibited) by what legal discourses and practices about ruling, governing and compliance. It is also possible to ask what existing legal discourses and practices have entailed the combination of modern law and the power of surveillance which eliminate the human rights encounter. In asking these questions, I am trying to see law not as passive and innocent and only reacting to technology's social effects, but as more ambivalent, enabling and constraining, disclosing and concealing at the same time.

Moving to Part III of the study, I will explore this constitutive aspect of modern law, its specific understandings and practices that not only provide the tools and frames for individuals to exercise human rights and for constraining the regulatory power of public and private authorities, but that also enable the exercise of power without individual encounters which is then dramatically realized by ubiquitous digital surveillance. Uncovering modern law's potential for removing the human rights encounter, which is also considerably reliant on the available technologies, and examining its non-neutral structure and the according effects despite modern law's commitment to the realization of human rights will lead to new perspectives for revisiting the human rights challenges discussed in Part I and the problems of the regulatory interventions

⁵ Hans Lindahl, *Fault Lines of Globalization: Legal Order and the Politics of A-legality* (Oxford, United Kingdom: Oxford University Press, 2013) at 132 ["[B]y opening up a realm of legal possibilities, legal schemes go hand-in-hand with the closing down of other normative possibilities...The possibilities which are closed down are not merely forms of action which are declared illegal...*Qua* schemes, legal norms empower and disempower, enable and disable. accordingly, legal schemes of interpretation are conditions of possibility of legal acts."].

identified in Part II. If law is the solution and the rule of law needs to be firmly reasserted to protect individual dignity against the totalising force of digital surveillance, it will be necessary to anatomise modern law's encouraging-inhibiting structure before proposing any legal instruments.

Part III

Surpassing the Scheme of Double Inscription: The Human Rights Encounter and the Ambivalence of Modern Law

Chapter 5. The Transformation of the Human Rights Encounter and Modern Law

As mentioned in the interim conclusion, Chapter 5 aims to go beyond the scheme of double-inscription of the Frankenstein Myth and explore the constitutive role of modern law in transforming the human rights encounter and providing conditions for surveillance-based governance. The human rights encounter is considered to be a conflictual encounter between individuals and institutions where individuals can raise human rights claims against the coercive power of institutions. This idea, its theoretical underpinnings and normative implications of the loss of human rights encounter, will be explicated in greater detail in Chapter 6. The hypothesis of the discussion which follows in this chapter is that modern law and the policing power of the modern state co-constitute a prototypical form of human rights encounter informed by pastoral liberalism. This prototypical human rights encounter rationalizes individual encounters with powerful institutions, enabling individuals as legal subjects to make human rights claims, taming the power of the institution through modern human rights law. It also provides the two parties with a common legal discourse and legalized forums for the conflictual encounter to unfold and be resolved.

This prototypical form of human rights encounter now faces profound challenges and transformations in the context of ubiquitous digital surveillance, as discussed in Part I. By resisting technological determinism and the reductive account of both law and technology often implied in law and technology scholarship, Chapter 5 argues that the conditions of the current challenges are already implied in pastoral liberalism and in some modern legal thought and practices. Pastoral liberalism and modern law contain their totalising and illiberal aspects, which are significantly amplified in the digital surveillance context that could turn pastoral liberalism on its head.

By going beyond the double-inscription scheme, I also aim to go beyond the circular way of problem framing and problem solving, as discussed in Chapter 4, in which legal craftsmanship merely means technical solutions reacting to the perceived imminent challenges posed by the use of digital surveillance. The phenomenon of the elimination of the human rights encounter, which

has been taken as the social effect caused by the use of digital surveillance (see Part I), is itself in need of more understanding. The elimination of the human rights encounter is broader than the apparent black-box issue – the lack of institutional transparency and accountability of surveillance; it suggests a form of governing that extracts and acts on certain knowledge so that actual encounter with individuals becomes superfluous for the purpose of governing. Is this phenomenon unique to the context of ubiquitous digital surveillance or does it indicate something more than just a technological effect? Is there any continuity between the individual-institution encounter in the pre-digital age and that in the age of ubiquitous surveillance? If the human rights encounter is transformed to the point of elimination in contemporary ubiquitous surveillance, does it mean we could recover the lost human rights encounter by way of historical backtracking? In addition, the urgent call for law and the kneejerk reaction of resorting to formalist legal requirements to tame digital technology also beg questions about what the nature of legal ruling has become.

This chapter is motivated by these questions and tries to demonstrate the socio-legal conditions that give rise to surveillance-based governing and the elimination of the human rights encounter. I will provide a genealogical investigation to contextualize the surveillance-based governing enabled by digital technologies in the history of the transformation of the form of governance, power and subjectivity. In addition, by doing this genealogical investigation, I will highlight how the ruling of law has also developed to mediate the individual-institution encounter which effectively abandons certain non-legal forms of encounters. By contextualizing the elimination of the human right encounter and understanding its socio-legal conditions, my point is not to argue that the human rights encounter existed in a historical moment that needs to be retrieved. Instead, I will show that both the notion of the human rights encounter and the elimination of the human rights encounter are legal constructs, which paves the way to better understand the problem in the first two Parts of this thesis: the loss of the human rights encounter in the context of contemporary digital surveillance is a joint accomplishment of the technology of governance and modern law, rather than being first a side effect of technology and then a failure of legal regulation.

This Chapter is divided into three sections. Section 1 discusses the co-constitution of the prototypical human rights encounter under pastoral liberalism by modern law and policing. A

short historical and genealogical inquiry will be made to ask how the prototypical human rights encounter is different from the pre-modern encounter between individuals and political authorities and how modern law and policing rationalize the encounter under pastoral liberalism. In this inquiry, the interaction between modern law and policing power will constantly be emphasized. Inspired by Foucault and Foucauldian studies of law, this inquiry will examine how policing is considered generally as a disciplinary power which is supported by surveillance and calculating techniques to direct people's behaviour for public interests; law is not external to the disciplinary apparatus but can be considered as disciplinary *sui generis*. The two disciplinary forces of law and policing interrelate with each other: modern law rationalizes policing power by imposing legal restrictions on it; policing power also transforms some aspects of modern law, making certainty, order and utilitarian objectives part of the commitment of modern law.

Section 2 explains the idea of pastoral liberalism following Foucault's description of state policing as pastoral power. I will demonstrate the essential dilemma of pastoral liberalism – the simultaneous hiding and revealing of the pastorate and the simultaneous empowerment and disempowerment of the subjects. I will further show how this dilemma is reflected in some legal work on state and commercial surveillance.

Section 3 will pay attention to the historical connection between the precursor to the police state and the current deployment of digital surveillance as a logic of governance. I will argue that inherent to pastoral liberalism supported and mediated by modern law is a certain totalising and illiberal tendency of pacifying and disempowering individuals. This dark side of pastoral liberalism has been constrained by the substantive rule of law. Technology does make a difference, although not in deterministic way: compared with the pre-digital era, the totalising and illiberal tendency of pastoral liberalism is realized to different degrees and scales in the context of ubiquitous digital surveillance where the perception of and resistance to control become extremely difficult. I will conclude this chapter by making connections with the examples of digital surveillance discussed in Part I and Part II.

1. The prototypical human rights encounter under pastoral liberalism

This section investigates the co-constitution of the prototypical human rights encounter by modern law and police force, focusing on the following three aspects. First, confrontational encounters where individuals perceive and express grievances through naming, shaming, blaming and claiming¹ are transformed from personal, face-to-face encounters to impersonal encounters. This transformation can be traced within the process of modernization and political expropriation where formal institutions of political power are created. In particular, the modern state expropriates pre-modern, organic, and personal forms of political authorities. The modern state also exercises the sweeping power of policing to ensure security, wealth of the state, and the welfare of its subjects.

Second, the encounter between individuals and institutions is rationalized by modern law which subjectifies individuals as legal subjects, regulates the function and the exercise of power of institutions, and also becomes the medium by which disputes in the encounter are expressed and resolved. Especially with human rights legal discourses and practices, the encounter between individuals and institutions is further rationalized. The objective and purpose of powerful institutions, such as the policing power of the state, must be consistent with or justified by human rights legal language and individual grievances therefore find expression in human rights discourse.

Third, while modern law rationalizes, by imposing legal restraints on, the power and the exercise of power of political institutions, modern law is not external to the disciplinary power of policing of the modern state and operates as a disciplinary apparatus *sui generis*. It is disciplinary, in the sense that legislative acts have been increasingly similar to policy making, which means legal thoughts and practices place more emphasis on the utilitarian objectives of law. This is also intensified in human rights legal practices as a significant part of human rights law relates to economic, social, and cultural rights explicitly adopts a policy orientation and emphasizes the state's positive obligations. This is also true of civil and political rights where the standard of what is "necessary in a democratic society," under the guise of "limiting limitations" effectively drives much of the rights agenda. It is *sui generis*, in the sense that modern law is still

¹ William LF Felstiner, Richard L Abel & Austin Sarat, "The Emergence and Transformation of Disputes: Naming, Blaming, Claiming . . ." (1980) 15:3/4 Law Soc Rev 631.

different from policing and policy making by sticking to its own logic, which makes it possible to contest the power of policing by law. Nevertheless, this distinction of law does not remove its disciplinary character.

1.1 The transformation of encounter in the process of modernization and political expropriation

In broad strokes, modernization can be described as a process of rationalization and demystification, as famously discussed by Weber.² This rationalization is manifested by the replacement of personal, face-to-face encounters by the impersonal encounter between individuals and institutions. The most discussed instance of the rationalization of political authority is the formation of the modern state. The modern state expropriates the pre-modern, local and private forms of political power, “stands in top place,” and claims the monopoly of the legitimate use of physical force within its territory.³ Not only physical violence, but essentially the power of administering social affairs and resources is expropriated into this impersonal authority from the society.⁴ The impersonality and rationality of the modern state is also reflected in a body of professional state officials who run the state according to established rules without having actual ownership of political authority. A Weberian modern state, hence, is rationalized by centralizing pre-existing, organic, local and private forms of political power, subjecting the newly centralized political power to an order and directing political activities to realize that order.⁵

This is of course an extremely abstract and simplistic account of political expropriation. The following examples concerning the creation of state police will make this account more

² Admittedly, this understanding of modernization is specific to the European context. My discussion in this chapter is drawn upon the scholarship of police state in the European context to formulate an exemplar of the rationalized human rights encounter. I do not claim this understanding of modernization or the exemplar of human rights encounter to be universal.

³ Max Weber, *From Max Weber: Essays in Sociology*, translated by H.H. Gerth & Wright Mills (New York: Oxford University Press, 1946) at 82.

⁴ Karl Marx, *The Eighteenth Brumaire of Louis Bonaparte* (New York: International Publishers, 1969) at 122 [“Every common interest was immediately severed from the society, countered by a higher, general interest, snatched from the activities of society’s members themselves and made an object of government activity – from a bridge, a schoolhouse, and the communal property of a village community, to the railroads, the national wealth, and the national University of France.”].

⁵ Karl Dusza, “Max Weber’s Conception of the State” (1989) 3:1 *Int J Polit Cult Soc* 71 at 75–76.

concrete. Before the creation of the modern police force, policing was conducted locally, by and within the people and involved proximity and the face-to-face encounter. One example of local policing takes the form of popular operation. The function of policing was not entrusted to any specific individual (whether chosen locally or centrally appointed). Rather, everyone in the community was permitted to perform policing and enforce order. Witch-hunting is a typical example of how this was exercised. It is a quite ancient phenomenon, but remarkably, has also been revived as an ideal type several times in modern times. Because danger arises from the people themselves in this case, every member of the community had the right and duty to identify and eliminate or purge the danger, and so everyone was watching and being watched. Proximity and encounter were also necessary in such popular operations. Popular operations often lacked stable hierarchy and organization and tended to be extremely lawless and chaotic. Therefore, although the state sometimes deliberately delegated the power of policing to the mass of people, for a Weberian law maker, popular operations were not just irrational but also dangerous. Relying on the mass of people actually posed a great risk to the sovereign for losing the monopoly over legitimate violence. To consolidate the state's monopoly, such form of popular operation had to be gradually delegitimized and replaced by police of the state.

A slightly more organized form of local policing, which operates in proximity but does not give everyone in the community the right to police, can be seen in an example of the City of London in the late 18th century: The city's authority, composed of people elected from each district, regulated in a general way the city's patrol and watch (*e.g.*, in terms of the number of watchmen or constables and their payment).⁶ Leaders of each district would themselves appoint watchmen and constables from the residents of the district, make specific regulations regarding their working hours and activities, and deal with complaints from the district's residents about policing. The function of policing was specific to each local community and was performed as a civic duty by community members.⁷ Of course, not every community member would have been willing to do the job and sometimes would have good reasons, such as health issues or advanced age. Or sometimes, a "householder" did not live in the community anymore. It is possible for the

⁶ Andrew Todd Harris, *Policing the City: Crime and Legal Authority in London, 1780-1840* (Ohio State University Press, 2004) at 17.

⁷ *Ibid* at 13.

selected individual to hire someone else as a substitute watchman or constable, as permitted by the district's authority.⁸

In the late 18th and early 19th century, English utilitarian legal reformers often depicted this form of local policing as involving too much discretion and as being corrupt and inefficient. Why? One of the reasons is that the remuneration of such positions was too low to make a living. The low pay discouraged people from performing civic duties. It also meant that only those people already on the fringes of society (*i.e.*, the old, poor, uneducated, non-citizens, etc.) would work (as substitutes) in these positions and the low pay would motivate them to take bribes in exchange for looking away from a crime or releasing an offender. Unsurprisingly, legal reformers were very critical of having these people enforce public order and called for an independent, professional, hierarchically supervised and relatively well-paid police force. In short, in the eyes of an elitist, utilitarian legal reformer or policy maker, local policing was irrational, to use Weber's term.

These two reasons behind creation of modern police force, *i.e.*, monopoly over legitimate violence and rationality of policing, are obviously interrelated. The criteria for being rational (*e.g.*, efficiency of crime reduction, integrity of the police) can be understood very differently by the residents of a community and by the sovereign state. This is evidenced by the fact that police reform in the UK in early 19th century often faced local resistance for a few decades.⁹ People could prefer local policing precisely because of its flexibility, responsiveness, the proximity with local authorities, and the possibility of participation. If someone wanted his or her house or shop to be watched more often or someone complained about drunk people shouting around his or her house at night, they could go directly to the district authority to air their complaint or suggestions and get their problems resolved somewhat quickly. The fact that local policing did not reduce crimes does not necessarily mean it was inefficient. It could also suggest great tolerance or even sympathy of the locals with petty offenders, especially when the local residents and petty offenders were from a similar social class. Conversely, it could also suggest an unprincipled and unconstrained application of the idea of criminality by a mass of people, in which case mass policing does give rise to more crime. Both cases, leniency and cruelty, suggest the porous

⁸ *Ibid* at 20.

⁹ Harris, *supra* note 6.

legality enforced by local policing and different understandings of rationality or efficiency. The determination of the rationality of policing presupposes the determination of criminality and illegality of certain conduct. The monopoly of the power to decide what is criminal or illegal is a necessary part of the state's monopoly of legitimate violence. So, the centralization of policing expropriates not just the function and operation of policing from the local and private to the state, but also more generally expropriates the people's discretion and participation in criminal justice.

The expropriation of local police power and the creation of the modern state police exemplify the transformation of political authority exercised through personal encounter and proximity to that exercised through impersonal institutions. While the examples given – *i.e.*, mass operation and the modernization of police force in the 19th century England – concern criminal matters, it is important to note that the power of policing of the modern state and its rationalization has had much broader impacts on the encounter between individuals and modern states. As recent Foucault-inspired scholarship on police studies has revealed, a historical link can be drawn between policing and the welfare state.¹⁰ Those studies recover a rather different meaning of policing since its first appearance in the 15th century French-Burgundy until the 18th century: police generally referred to the state's governmental power and public administration, and starting only in the 19th century and throughout the 20th century did it become strictly about the constabulary power dealing with criminal matters.¹¹ The “police scientists” in the 17th and 18th centuries believed that the object and purpose of the modern state's governmental power (the *raison d'état*) was the production of social wealth and the increase of welfare of state subjects. Policing was the administrative tool for achieving this purpose.¹² So, policing was the term for political economy and public administration, and the power of policing of the modern state was extremely broad. For example, for Adam Smith, “police” includes cleanliness of roads and streets, security, cheapness or plenty.¹³ So, political expropriation that is seen in the example of the creation of modern police force in the 19th century England can be extrapolated to various

¹⁰ E.g. Markus Dirk Dubber & Mariana Valverde, eds, *The New Police Science: The Police Power in Domestic and International Governance* (Stanford University Press, 2006); Markus Dirk Dubber & Mariana Valverde, eds, *Police and the Liberal State* (Stanford University Press, 2008).

¹¹ Mark Neocleous, “Theoretical Foundations of the ‘New Police Science’” in Markus Dirk Dubber & Mariana Valverde, eds, *New Police Sci* (Stanford University Press, 2006) 17 at 22.

¹² *Ibid* at 26; Graham Burchell, Colin Gordon & Peter Miller, eds, *The Foucault Effect: Studies in Governmentality* (University of Chicago Press, 1991) at 16.

¹³ Adam Smith, *Lectures on Jurisprudence*, R. L. Meek, D. D. Raphael & P. G. Stein, eds. (Liberty Fund, 1982) at 331.

other matters of public administration where impersonal institutions of the state were created to replace face-to-face encounters and to dictate the purposes of public administration.

By actively asserting itself as the insurer of individual rights and the common good, the modern state made the population the object of its administration or policing. The modern state which exercises this sweeping power of policing resulting from political expropriation was described by Marx as a horrible and parasitic monster which de-politicised civil society.¹⁴ This does not mean that political expropriation and the power of policing are one-sidedly oppressive. As will be seen shortly, Foucault describes the policing power as “pastoral” to emphasize the productive side of its effect on individuals, the population, and civil society. One of such productive effect is the transformation of individuals into wage-labourers necessary for the development of early capitalism by police force.¹⁵ This transformation of individuals explains the close relationship between criminal law enforcement and economic affairs in the early modern period. For example, idleness was often criminalized and poor people were often the target of police interventions for crime prevention.¹⁶ Forced labour often existed in prisons where criminals (poor people) were given physical and moral training to become labourers.¹⁷ Without relying on the Marxian base-superstructure claim, it can be argued that the power of policing, against the background of early capitalism, helped to consolidate the transformation of individuals into wage-labourers. As the wage form makes each person’s value calculable, individuals are subjectified into rational homo economicus.

The point of recovering this historical meaning of police is to argue that the process of political expropriation transforms the pre-modern encounter between individuals and authorities by making the authority-holder, or the locus of political authority, a rational institution. Internally, following Weber, the institution has bureaucratic structures and rules regulating its

¹⁴ Karl Marx, *The Eighteenth Brumaire of Louis Bonaparte* (New York: International Publishers, 1969) at 62 [“through the most extraordinary centralization this parasitic body acquires a ubiquity, an omniscience, a capacity for accelerated mobility, and an elasticity which finds a counterpart only in the helpless dependence, the loose shapelessness of the actual body politic”].

¹⁵ Neocleous, *supra* note 10; Grégoire Chamayou, *Manhunts: A Philosophical History*, translated by Steven Rendall (Princeton University Press, 2012) at 84–85. See also Section 2.1 in Chapter 6 on the English Black Act, which included over 200 petty offences punished by the death penalty to protect the property rights of the new ruling class represented by the Whig Party.

¹⁶ E.g., *Vagrancy Act 1824* (UK), 5 Geo IV, c83. It prohibits behaviours such as sleeping in public or begging, and the punishment is forced labour for up to a month.

¹⁷ Chamayou, *supra* note 14 at 84.

functioning. Externally, the institution finds its rationality in welfare objectives, the *raison d'état*. The rationalization of the political institution creates new ways of perceiving and expressing social conflicts and individual grievances. For example, disputes in private or public relationships can be expressed in economic terms.

From this short story about the creation of modern state police and a mini-genealogy of policing, a few preliminary observations can be made. The encounter between individuals and state institutions is created by the modernization of policing, which has internal and external rationality as just mentioned. Centrally promulgated laws determine the object of criminalization and rules govern the exercise of police power by a professional body of police. Criminality is rationalized by being closely tied to social welfare. Individuals are subjectified and rationalized into the state's subjects and *homo economicus*. Perhaps an anachronistic assessment, the process of modernization and political expropriation, even though informed by liberal ideas of the Enlightenment, has its illiberal and totalising side in that it eradicates alternative forms of political power, forms of subjectivity, and forms of encounters. Even though the process is never perfected in reality, the illiberal and totalising aspect always exists in the idea and practices of political expropriation and modernization. This claim will be revisited in Section 2.

This mini-genealogy of policing reveals the historical connection between policing and the welfare state. It also provides new perspectives for considering the surveillance scenarios discussed in Chapter 1. The deployment of digital surveillance technologies in law enforcement, or by welfare agencies, or in business activities may seem to reflect very different situations regulated by different bodies of law with irreducible logics. Discussing these different scenarios together however is not just to show the broad application of digital surveillance technologies and some common challenges raised for human rights and the rule of law. The history of policing reminds us that surveillance has always been a necessary component, as a technology of power that produces knowledge, in varied fields where the state governs and exercises the reason of state. It also reminds us of the power structure which surveillance is implanted in and reinforces in the fields where power is less visible and contestable, for example surveillance used in commercial relationships and in cases of social benefits provision.

1.2 The rationalization of encounter by modern law

Underlying the transformation of political power and the subjectivation of individuals is modern law. To add briefly to the previous discussion about political expropriation, for a Weberian modern state, rationality is equated to legality which provides an authority legitimacy. Political expropriation has had a remarkable homogenizing and democratizing effect on the subjects of the state. The replacement of personal authority by the impersonal and the traditional by the rational-legal remove the old social and communal bonds among people and the privileges and duties corresponding to personal status. Individuals become formally equal subjects of the modern state and the formal equal status is established under modern law. Marx describes the correlation between the formation of the modern state and the rise of the rights of man: “The establishment of the political state and the dissolution of civil society into independent individuals – whose relation with one another depended on law, just as the relations of men in the system of estates and guilds depended on privilege – is accomplished by one and the same act.”¹⁸

So, modern law gives social conflicts specific expressions: modern law is the medium by which institutions, private entities and individuals organize their activities, exercise their power upon others and defend themselves. It rationalizes both the political power and the exercise of power. As will also be discussed in Chapter 6, the pre-modern, personal and face-to-face encounter has some dramatic effects of arousing affection, compassion, shame, shock, or even unleashing brutal violence. Yet, by political expropriation and especially through modern law, this dramatic effect of personal encounter is transformed into legally constructed claims about rights and obligations which are made and contested in legal forums. By legal forums, I do not mean only courts but also the non-adjudicatory and informal arenas which are either structured or recognized by law, such as parliament and local mediation councils.

Now, to move into some detail concerning modern law’s rationalization of political authority. As the earlier mini-genealogy of police suggests, the policing power of the modern state is extremely broad. Hence comes the persistent question about the relationship between the power of policing and law. As the modern state and its political expropriation gradually consolidated, the sphere of policing also expanded. A significant group of jurists and police

¹⁸ Robert Tucker, ed, *The Marx-Engels Reader* (New York: Norton & Company, 1978) at 46.

scientists had considered policing as outside the sphere of law and justice and the power of policing as unlimited, undefinable and unrestricted. For them, this was not just descriptive, but also a normative claim as the competence of policing was seen as necessitated by the *raison d'état* – to pursue the general interest and common good. For example, the German jurist, Stahl, believed that the administration of the state – *i.e.*, police in the general sense – should be unhindered by judicial review to serve the general interest.¹⁹ And more infamously, Schmitt defines sovereignty as the determination of the state of exception:

Therein resides the essence of the state's sovereignty, which must be juristically defined correctly, not as the monopoly to coerce or to rule, but as the monopoly to decide. The exception reveals most clearly the essence of the state's authority. The decision parts here from the legal norm, and (to formulate it paradoxically) authority proves that to produce law it need not be based on law.²⁰

This idea about the unlimited, undefinable and unrestricted power of policing, as many studies have pointed out, has recurred in the post 9/11 era in domestic and international arenas. Often adopting the contemporary restrictive understanding of policing, these studies pay close attention to the spaces of state police operation to demonstrate the unlimited-ness of policing power.²¹ The spatial expansion of policing which detects moving subjects is necessarily interrelated with the temporal and material dimensions of policing supported by surveillance technologies. For example, it is argued that counterterrorist policing practices cultivate a general climate of suspicion against migrants in society, which broadens the scope of policing interventions from crime prevention to migration control.²² So, even understood in the contemporary restrictive sense, policing has the inherent tendency of slippage because of its orientation towards prevention and security.

¹⁹ Mireille Hildebrandt, "Governance, Governmentality, Police, and Justice: A New Science of Police?" (2008) 56 *Buffalo Law Rev* 557 at 588.

²⁰ Carl Schmitt, *Political Theology: Four Chapters on the Concept of Sovereignty* (University of Chicago Press, 2010) at 13.

²¹ E.g. Mitchell Dean, "Military Intervention as 'Police' Action?" in Markus Dirk Dubber & Mariana Valverde, eds, *New Police Sci* (Stanford University Press, 2006) 185; Joseph Pugliese, *State Violence and the Execution of Law: Biopolitical Caesurae of Torture, Black Sites, Drones* (Routledge, 2013).

²² Nick Vaughan-Williams, "Borderwork beyond Inside/Outside? Frontex, the Citizen–Detective and the War on Terror" (2008) 12:1 *Space Polity* 63.

There are two possible ways in which modern law rationalizes the state's policing power, informed by two ideas related to the rule of law, one procedural and the other substantive. Following what Stahl and Schmitt conceived about the power of policing, it can be understood that law's rationalization gives policing a legal form and mode of exercise. Legalization regulates the exercise of policing power, but has nothing to say about the scope of policing, which is unlimited and undefined. The power of policing is given formal legal basis and rationality but is fundamentally extra-legal. The state's power of policing can suspend the law through legalised procedures when it considers a situation as emergency. The opposite move is to invoke the substantive notion of the rule of law, which brings both the exercise and the scope of policing power under judicial scrutiny. Rationalization by the substantive rule of law of the policing force makes the policing power contestable, not just as a matter of procedure and internal accountability, but also in its scope and external accountability. Decisions made on a state of exception itself are also bound by the rule of law.²³ Hence, the substantive notion of the rule of law rationalizes the power of policing by imposing limitations on the operation of sovereignty of the modern state.

The two ways of rationalization by the modern law of policing power are important for thinking about legal interventions and the rule of law in the context of ubiquitous digital surveillance and will be revisited in Section 2 and in Chapter 6. For now, whether the power of policing is brought within law or is ultimately beyond law, the minimum is that modern law gives policing a legal form of existence and provides some possibility of contestation in legal terms and within legal forums. Combining the legal rationalization of policing with the transformation of individuals into legal subjects, the encounter between individuals and state authority is given legal expression. One effect of the legal rationalization of encounter is that parties to the encounter become more prone to communicate by using the same language system to express their claims. For example, when a government decides to expropriate a piece of land for building a dam, individuals living on that land can contest the decision. They can do so by claiming the decision is procedurally unlawful because they were not given the chance to participate in the decision-making process and their voices were not heard, that the dam project is not for the public good, or that the expropriation fails the requirement of necessity and

²³ Mireille Hildebrandt, "Governance, Governmentality, Police, and Justice: A New Science of Police?" (2008) 56 Buffalo Law Rev 557 at 594.

proportionality. The government would then come up with the opposite claims using the same legal language. Resolution of the conflict will also focus on these legal issues. The legal rationalization of the encounter, meanwhile, also means it discourages those forms of exercise of power and the use of those language systems or forums of dispute resolution, which are deemed as being the underside of the legally rationalized encounter. For example, the resort to extra-legal violence by either party to the encounter is obviously delegitimized. Not only does the recourse to violence challenge state's monopoly over violence and hence is delegitimized, but extra-legal violence also breaks down the normal channel of individual-institution communication and the shared language system, which can lead to profound confusion and more chaos (the Yellow Vest movement comes to mind²⁴). Non-violent but extra-legal claims are also rendered unintelligible. In the example of the dam project, then, a legally rationalized encounter does not recognize claims made on behalf of mother earth against capitalism, for instance.

This enabling-discouraging effect of the legal transformation of encounter reminds us of the non-neutral structure of technological mediation mentioned in the previous interim conclusion. Technology mediates our experience by amplifying-reducing certain ways of perception and encouraging-inhibiting certain ways of action.²⁵ A law-as-technology discourse emphasizes this non-neutral structure of mediation in law's technicity. Lindahl's claim about law's intrinsic exclusion by inclusion is also reflected here.²⁶ Connected to the illiberal and totalising side of political expropriation discussed earlier, modern law's transformation of encounter legitimises the totalisation of political expropriation and provides an additional layer of totalisation by suppressing and making other a-legal ways of perceiving and expressing power and grievances unintelligible.²⁷ Of course, modern law's enabling effect, empowering individuals to express their rights through legal terms and restraining the power of political authority, cannot be lightly dismissed (as will be discussed in Chapter 6, legal historian E.P.

²⁴ The Yellow Vest movement was a mass political movement which began in France in October 2018. The movement started by protesting against rising fuel prices and the French government's tax reform and went to incorporate other demands for economic justice. The protest had significant impacts outside France and the symbol of yellow vest was adopted in a number of mass demonstrations in various countries, such as Croatia, Germany, Italy, Portugal and Spain.

²⁵ E.g. Don Ihde, *Technics and praxis*, Boston studies in the philosophy of science 24 (Dordrecht: Reidel, 1979).

²⁶ Hans Lindahl, *Fault Lines of Globalization: Legal Order and the Politics of A-legality* (Oxford, United Kingdom: Oxford University Press, 2013) at 132.

²⁷ The term "a-legal" is used by Lindahl to describe something so strange that cannot be characterised as either legal or illegal under extant legal framework but which transcends the extant legal intelligibility. *Ibid* at 37–38.

Thompson claims the rule of law as an “unqualified human good”). This enabling and empowering aspect of modern law faces serious challenges, however. One reason is that the instrumentalist account of law, criticised earlier in Parts I and II, legalises and manages intrinsically arbitrary powers. Another reason is that modern law itself becomes a disciplinary apparatus. In a sense, the evolution of modern law is also informed by an instrumentalist account of law, but unlike the former reason, modern law does not just give political power a legal form of existence *post facto*; it actively engages in the policing and disciplining of populations for utilitarian objectives.

1.3 Modern law as disciplinary apparatus

To complicate the relationship between modern law and policing, it is not a one-way relationship in which modern law rationalizes the power of policing, whether by formal legalism or the substantive notion of the rule of law; policing has also infiltrated modern legal thought and practices, and law has evolved from rules protecting individual rights (understood mostly as property rights) and regulating the public and private relationships to a policing apparatus (policing understood in the broad sense). For example, Adam Smith insisted that, “the end of justice is to secure from injury.”²⁸ This view of justice is now seen as extremely minimalist as compared to “justice as fairness”²⁹ or the notion of distributive justice. Modern law actively participates in the public administration of the welfare state. From a Foucauldian perspective, modern law is governmentalized and the, “constant and clamorous activity of the legislature” in fact suggests the, “regression of the juridical”.³⁰ To be more specific, Foucault’s own conception of law as equivalent to the imperatives of the sovereign and hence opposed to the disciplinary power of modern society has been repeatedly criticised. Law itself has changed and there are significant synergies between modern law and discipline. Apart from giving the different forms of disciplinary power legal modes of existence discussed above, whether by controlling or exempting disciplinary power from law’s control, synergies are also caused by law’s increasing

²⁸ Smith, *supra* note 12 at 399.

²⁹ John Rawls, *A Theory of Justice*, revised edition ed (Cambridge, Mass: Harvard University Press, 2009).

³⁰ Ben Golder & Peter Fitzpatrick, eds, *Foucault and law* (London: Routledge, 2016) at xvii.

proceduralization which is more concerned with standards and norms than positive rules.³¹ Law's proceduralization allows it to be deeply involved in the governance of social life.

The idea of law as disciplinary apparatus is perhaps most evident in the Chicago School of Law and Economics, where not only law's objectives are explicitly utilitarian – to simulate the market and maximize wealth – but economic principles are applied to legal analysis on assigning rights and responsibilities to allocate productive forces and reduce transactional costs.³² The reduction of the common good and general interest to economic interest and efficiency is disputed by other strands of legal thought. For instance, Dworkin has argued that wealth-maximization would lead to concentration of wealth from the poor to the rich and that it is wrong in principle.³³ Some problems picked out in Parts I and II of this study – *e.g.*, the inviolability of intellectual property rights and trade secrets of tech companies causes democratic deficits when tech conglomerates in fact control and make decisions about people's lives without judicial scrutiny – can arguably be justified by certain economic analysis, and the critical problem of economic analysis is of course who gets to decide what counts as a cost and what counts as a benefit. However, it is important to note that non-utilitarian criticisms of law and economics leave intact the implied idea of modern law as discipline for the *raison d'état*. So far as distributive justice or justice as fairness need law as a means to achieve welfare-based ends, there is also strong convergence between modern law and policing.³⁴

Human rights discourse joins in the convergence and becomes the dominant discourse for public administration and for structuring state-subject relationships.³⁵ Policing and human rights discourse converge because a significant part of human rights law – economic, social and cultural rights – is traditionally considered as welfarist. There has been heated debate about whether these rights are human rights or merely about social policy, and by the end of the Cold War, these rights had been given human rights status but remain welfarist and require the

³¹ Alan Hunt & Gary Wickham, *Foucault and Law: Towards a Sociology of Law as Governance* (Pluto Press, 1994) at 65–67.

³² Russell Hardin, "The Morality of Law and Economics" 11:4 *Law Philos* 331 at 344–345.

³³ Ronald Dworkin, *Law's Empire* (Harvard University Press, 1986) at 287.

³⁴ Critics of Dworkin's critique on law and economics have pointed out that distributive justice also implies an instrumentalist perspective on law and also accepts the morality of efficiency as crucial for distributive justice. Hardin, *supra* note 32 at 348; Matthew H Kramer, "Questions Raised and Questions Begged: Some Doubts about Ronald Dworkin's Approach to Law-and-Economics" (1993) 6:01 *Can J Law Jurisprud* 139 at 141.

³⁵ David Kennedy, "International Human Rights Movement: Part of the Problem? Boundaries in the Field of Human Rights" (2002) 15 *Harv Hum Rights J* 101 at 108, 113.

continued, positive actions of states. The International Covenant on Economic, Social and Cultural Rights, for example, obligates states to take steps, “to the maximum of its available resources, with a view to achieving progressively the full realization of the rights recognized in the present Covenant by all appropriate means, including particularly the adoption of legislative measures.”³⁶ Human rights law, while empowering individuals to secure and realize their human rights through legal means, gives the traditional administrative-welfare state a new discursive device and medium to express and exercise its power over individuals. Of course, state power that is expressed so as to realize human rights is constrained at the same time by human rights law’s own logic. For example, the principle of non-discrimination imposes limitations on positive measures which are to eliminate substantive discrimination; according to the Committee on Economic, Social and Cultural Rights, such measures, “are legitimate to the extent that they represent reasonable, objective and proportional means to redress *de facto* discrimination and are discontinued when substantive equality has been sustainably achieved”.³⁷ The point, however, is that these limitations only arise because a certain domain of intervention of the state has been secured and legitimated by human rights in the first place.

Now, a prototypical human rights encounter comes to fruition after three steps of transformation: first, the transformation from personal, face-to-face encounter to impersonal individual-institution encounter through political expropriation; second, modern law’s rationalization of the impersonal encounter by consolidating and taming the power of the modern state for welfare objectives, subjectivating individuals as equal rights holders, and becoming the dominant forum where conflicts are fought out; and third, the transformation of the legally constructed encounter extends a step further through a human rights discourse which expresses the state’s power in terms of positive and negative human rights obligations. The point of giving this very abstract account of a prototypical human rights encounter is not its facticity, but to provide a conceptual tool for thinking about the invitation-inhibition structure of modern law.

While the discussion in the section so far has focused on the state-subject relationship, it is necessary to mention that the process of legalizing and rationalizing encounters also

³⁶ *International Covenant on Economic, Social and Cultural Rights*, 19 December 1966, 993 UNTS 3, art 2(1) (entered into force 3 January 1976).

³⁷ *General Comment No.20: Non-discrimination in economic, social and cultural rights (art.2, para.2 of the International Covenant on Economic, Social and Cultural Rights)*, UNCESCR, 42nd Sess, Agenda Item 3, UN Doc E/C.12/GC/20 (2009), para.9.

transforms horizontal relationships between private actors and civil society in general. As just discussed, modern law closely interacts with disciplinary regimes such as hospitals and schools. Individual relationships within and with the private institutions are also rationalized by law because these relationships exist within the general contours of modern law and the power of private institutions needs to be legitimised by law.³⁸ Increasingly, as human rights practices move to emphasize the horizontal duties and human rights obligations of non-state actors,³⁹ disciplinary regimes are also transformed by human rights discourse.⁴⁰ For commercial entities – though their existence is structured by laws as regards private property, contracts, etc. and their activities are informed by economic principles – the discourse about corporate’s human rights responsibilities is superimposed on private companies and provides a new set of standards and norms to evaluate business activities. Transforming the power of private institutions by human rights discourse provides a special case of modern law as disciplinary apparatus. In the neoliberal era where private entities gradually become the main provider of many social services, human rights law, at least the practices of mainstreaming human rights in business normalizes private entities and their disciplinary power. For example, while prisons have already been a casebook example of the disciplinary regime in Foucauldian studies, the disciplinary regime is transformed in the context where prisons are run by private companies. The legal discourse of corporate human rights responsibilities disciplines the disciplinary power of the privately-run prison which in turn, finds new standards and a rationalized mode of existence, and mode of exercise in human rights discourse which may or may not be compatible with the economic interest of the business. This is also why short of an explicit rejection of privatization of the prison, human rights-based claims can be made both for and against privately-run prisons.⁴¹

Hence, modern law, augmented by human rights discourse, not only actively engages the power of policing of the modern state by way of converging the realization of human rights with welfare-based goals, but transforms the disciplinary power of private entities – which is

³⁸ Jacopo Martire, *A Foucauldian Interpretation of Modern Law: From Sovereignty to Normalisation and Beyond* (Edinburgh: Edinburgh University Press, 2017) at 114–115; Hunt & Wickham, *supra* note 31 at 65–67.

³⁹ E.g. John H Knox, “Horizontal Human Rights Law” (2008) 102:1 Am J Int Law 1.

⁴⁰ Ivan Manokha, “Foucault’s Concept of Power and the Global Discourse of Human Rights” (2009) 23:4 Glob Soc 429.

⁴¹ Frédéric Mégret, “An International Law Theory of Inherently Governmental Functions” (2019), unpublished manuscript; Philip Alston, *Report of the Special Rapporteur on extreme poverty and human rights*, 73 Sess, UN Doc A/73/396 (2018).

increasingly replacing the state's administration – by recognizing private entities as bearers of human rights obligations.

2. Pastoral hunting, surveillance and pastoral liberalism

I now move to discuss the underlying liberalism of the prototypical human rights encounter which modern law constitutes. As will be seen, the invitation-inhibition structure of modern law corresponds to the essential dilemma within liberalism.

Chapter 1 of this study examined the imagery of hunting in a discussion of state surveillance to demonstrate the high mobility, the tactics, and the intrinsic power imbalances of surveillance. To connect the imagery of hunting to what has been discussed regarding policing, the state's policing power, which protects its people from security threats, leads to a more specific type of hunting discussed by Grégoire Chamayou: pastoral hunting. "Every shepherd must have three sorts of power to defend his flock: a power over wolves, to prevent them from killing his ewes; a power over the rams, to prevent them from harming the ewes; and a power over the sheep in general, to give them the necessary pasturage."⁴² It is necessary for the shepherd to not just track down and kill wolves and rams, but also to find out and eliminate diseased sheep to protect the flock. The purpose is not predation as such but protection. To protect, the shepherd has to hunt and kill. Now, when applying the notion of pastoral hunting to the modern state, the state is the shepherd, which expropriates all forms of local policing and monopolizes the power of identifying and exterminating the vice within and outside the flock. All the actual and potential security threats – wolves, rams and diseased sheep – as well as the protected flock are, "bodies in movement", and so the shepherd has to pursue (using hunting dogs and shepherd dogs, *i.e.*, the police), to force stop the moving bodies and to catch escaped bodies.⁴³

Moving from the restrictive sense of policing to the broad, historical sense, policing viewed as hunting is a pastoral technique by which the pastorate raises, directs, and arranges the flock for the common good and ends of the flock. Foucault connects the modern state's

⁴² Chamayou quotes Cardinal Bellarmine. Chamayou, *supra* note 14 at 20.

⁴³ *Ibid* at 90.

governmentality with Christian pastorate's "art of governing men". Governmentality is described by Foucault as a set of techniques, institutions and tactics of government which, "has the population as its target, political economy as its major form of knowledge, and apparatuses of security as its essential technical instrument",⁴⁴ while the Christian pastorate is the "art of conducting, directing, leading, guiding, taking in hand, and manipulating men, an art of monitoring them and urging them on step by step, an art with the function of taking charge of men collectively and individually throughout their life and at every moment of their existence."⁴⁵ The governmentality of the modern state, according to Foucault, combines the "city-game" of the Greek polis and the Christian shepherd-game.⁴⁶

The imagery of hunting and the art of monitoring and manipulating the population can also conjure the image of an omniscient and omnipotent power squeezing out the subject's freedom and liberty by its unlimited pursuit and exhaustively detailed knowledge, which make people "docile bodies" in the name of security. Even if it is argued that government should have, "patience, wisdom, and diligence," to govern for the common good and the ends of the governed,⁴⁷ this conception of government is still extremely paternalistic, which would go against the humanist philosophical and juridical discourse of the state's policing power. A paradox exists between the police power, which identifies even the tiniest trace of threat to the population, and the sphere of personal liberty constructed as inviolable by the humanist legal and philosophical discourses. To resolve, or at least to moderate this paradox, the omniscient and omnipotent power itself and the asymmetric relationship it creates need to be somewhat hidden from the public, or at least kept in the background while individuals can still exercise personal liberty in daily events so that the omnipresent gaze of the sovereign becomes less overwhelming, frightening and invasive to subjects and a seeming equilibrium can be created out of the *de facto* power asymmetry. Basically, the transformation of encounter by hiding is both a consequence of and a condition for reconciling the conflict between security and liberty on liberalism's own terms.

⁴⁴ Michel Foucault, *Security, Territory, Population: Lectures at the Collège de France, 1977-1978*, translated by Graham Burchell, Michel Senellart, François Ewald & Alessandro Fontana, eds. (Basingstoke; New York: Palgrave Macmillan: République Française, 2007) at 108.

⁴⁵ *Ibid* at 165.

⁴⁶ Burchell, Gordon, & Miller, *supra* note 11 at 8.

⁴⁷ Foucault, *supra* note 44 at 99–100. [Foucault quotes La Perrière's definition for government: "Government is the right disposition of things that one arranges so as to lead them to a suitable end."]

I now related the construction of a prototypical human rights encounter to the transformation of the encounter between the omniscient and omnipotent shepherd and sheep in the pastoral relationship. Two tactics of the transformation can be observed, again dealing with the shepherd and the flock respectively. Firstly, the shepherd needs to be perceived as less threatening to the sheep and increasingly out of the sight of the sheep. The distance between the sheep and the shepherd could be physical or emotional. Secondly, for the shepherd to maintain a distance from the flock, the flock has to be made knowable and manageable at a distance. In view of the shepherd as the state and the sheep as the people then, both tactics involve complicated techno-legal mediation of the encounter and the relays of the surveillance gaze in society.

2.1 Making a loving and distant shepherd

For the first tactic of transformation of the encounter between the shepherd and the sheep, hiding the omnipresent gaze of the policing power is of course a technological issue. Surveillance methods manipulate the distance between the target and the surveillant and make the surveillant less visible. This action is not so much about respecting personal rights and liberties as it is about ensuring successful surveillance operations. The enlarged physical distance needs meanwhile to be technologically reproduced as extreme proximity and visibility of the target for the surveillance agents. The mixture of distance and proximity, invisibility and visibility both appeases the liberal sheep and meets the needs of the caring shepherd.

Hiding the surveillance gaze is also a matter for law. From the outset, the basic requirement of the principle of rule of law – the promulgation of surveillance legislations which meet the criteria of accessibility and predictability – would at first sight largely restrict technological explorations that aim to hide state surveillance from the public. Ideas about liberal democracy especially want the public to not only be informed but to also participate and deliberate over the creation and administration of the state apparatus. So, for example, if satellite signals could be intercepted for surveillance purposes, there would need to be a legal framework created by democratic procedures to govern such a practice, setting out its scope and operational processes.

However, revealing is always a form of concealing. This paradox suggests how efforts to make bureaucracy transparent can also be problematic. In a provocative way, Žižek claims that transparency is a special form of darkness because if something is transparent, it is not seen but seen through.⁴⁸ To a great extent, Parts I and II of this study have demonstrated that the more surveillance mechanism appears as exceptionally legalised and regulated, the more is concealed its flipside concerning illegality and legal gray zones which are constantly explored and experimented with by new surveillance technologies and strategies. Micro-management by way of formal legalism that reveals the heightened formal rationality of state surveillance while hiding the intrinsic secrecy and unbridgeable power gap could generate emotional distance. It could also perhaps create intellectual difficulties for the public to comprehend the full scale of state surveillance, while also demanding more public trust in bureaucrats to ensure the legal rationality of state surveillance.

In terms of the relays of surveillance that gradually make the gaze of policing power more invisible, Foucault discussed how small, everyday disciplinary mechanisms, such as the daily life in prison – also serve as relays in service of disciplinary networks. The point is that thanks to the various relays in society which help monitor and govern populations, the state is relieved from doing everything itself and benefits from the work of relay mechanisms. Cyber surveillance provides a remarkable case. Despite being born in the US Department of Defence, internet and telecommunications services are now commercialized and provided by private entities. At first glance, due to the strong libertarian ideology surrounding the internet, any form of governmental control and centralization of the internet is criticized. Yet, the collaboration of commercial and private entities in state surveillance (as discussed in Part I) exemplifies the complicated amalgamation of the public and the private and particularly the amalgamation of the commercial, the civil and the military in current society.

The concealment of the state's policing power in this case is not just by secret arrangements between government and tech companies about the sharing of user data or the access to people's devices. More importantly, it concerns the transformation of the state-subject relationship involved in the pastoral relationship of state policing into one between consumers

⁴⁸ Slavoj Žižek, *The Courage of Hopelessness: Chronicles of a Year of Acting Dangerously* (Penguin UK, 2017) at 77.

and internet service providers, as state surveillance is mediated by and heavily reliant on corporate-consumer encounters. The exercise of control is much more obscure in commercial relationships. Liberal ideas such as “the sovereign consumer” and free choice give the impression that consumers could dictate the market economy, but the problem is that consumers never really “dictate” the economy because options are made and given to consumers by providers.⁴⁹ This illusion of free choice that hides the actual exercise of control by the providers is especially problematic in the context of the contemporary surveillance economy, as already discussed in Chapter 2 regarding nudge theory and in Chapter 4 regarding the fallacy of user consent. In addition, in commercial digital surveillance, the collection and processing of personal data can be conducted on the legal basis of the “legitimate interest” of the service providers, such as marketing and improving their services.⁵⁰ This legal basis of legitimate interest effectively recognizes the right of internet service providers to define, shape and circumscribe users’ choices. As the exercise of power by corporations in corporate-consumer encounters is deliberately concealed, the policing power of the state which is relayed by commercial service providers becomes more invisible and inconceivable.

2.2 Producing a remotely knowable and manageable flock

With respect to the second tactic, making the flock knowable and manageable, Foucault famously discussed how the modern prison as an exemplary apparatus of discipline in the disciplinary society generates all sorts of knowledge about humans and particularly the human body. The design of the Panopticon already demonstrates the power relation and the elimination of encounter in the prison setting. Technologically, the architecture and optical system of the building ensure that every inmate’s behaviour in the cell is exposed to the gaze of the person in the watchtower and that what is in the watchtower is unknown to the outside.⁵¹ Meanwhile, inmates have daily encounters with those who check their physical and mental health, give them

⁴⁹ Niklas Olsen, *The Sovereign Consumer: A New Intellectual History of Neoliberalism* (Palgrave Macmillan, 2019).

⁵⁰ EU, *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*, [2016] OJ, L119/1, art 6.

⁵¹ Michel Foucault, *Discipline and Punish: The Birth of the Prison*, translated by Alan Sheridan (New York: Vintage Books, 1995) at 200.

moral re-education, and supervise their labour, exercise and other activities. These people are the intermediaries of the surveillance power. They use charts and tables to develop detailed “anatomy” and ethnography of the convicts, scientific knowledge about the criminal mind, the level of rehabilitation required and the possibility of recidivism.⁵²

It is not just individual inmates and their bodies who are made knowable, manipulable and hence subjectivated. Inmates in the prison also appear as a “population”, an artefact produced by the administration and discipline, as well as statistical knowledge as a result of discipline in the prison. Other disciplinary institutions, such as schools, factories and hospitals, use similar techniques of categorization and tabulation to classify, compare and measure human beings and human behaviour, determine where is the average and what is normal or abnormal. Human beings are both homogenized and individualized by such norm-based assessment.⁵³ This extremely detailed knowledge about human beings that makes the management of the population much deeper, finer and in greater precision arises from various small power relations and cannot realistically be obtained by a singular power of surveillance at the top.

What Foucault presents in *Discipline and Punish*, the everyday micro-mechanism of disciplinary power, appears very much opposed to a Weberian state or a Marxist parasitic monster that one-sidedly totalizes all private power relations. Nevertheless, Foucault’s concept of governmentality introduced in *Security, Territory, Population* complements the microphysics of disciplinary power to analyse the techniques of governing populations at the level of political sovereignty using the same methodology in analyzing the microphysics of disciplinary power.⁵⁴ The various forms of private, informal and material forms of disciplinary power have not displaced the power of the sovereign but are accompanied by the art of government in the modern state that takes the whole population as its essential object. Just as the Christian pastorate whose mission is the salvation, “of all and of each”, governmentality both individualizes and totalizes. It produces and relies on detailed knowledge of subjects of the state and controls them as both individuals and population and directs them towards happiness and prosperity.

In addition, Foucault talks about not a replacement or displacement of the sovereign by discipline but a triangular practice of power: sovereignty-discipline-governmental

⁵² *Ibid* at 249–254.

⁵³ Foucault, *supra* note 44 at 107; Foucault, *supra* note 51 at 189–192.

⁵⁴ Burchell, Gordon, & Miller, *supra* note 12 at 4.

management.⁵⁵ Foucault argues that this coexistence between power-as-sovereign and discipline is because, “the theory of sovereignty, and the organization of a legal code centred upon it, have allowed a system of right to be superimposed upon the mechanism of discipline in such a way as to conceal its actual procedures, the element of domination inherent in its techniques, and to guarantee to everyone, by virtue of the sovereignty of the State, the existence of his proper sovereign rights”.⁵⁶ This can be related to what has been discussed in previous subsections about transformation of the legal encounter by the discourse of human rights. Surveillance is therefore doubly concealed: first, the primary encounter of surveillance happens in various private and informal power relations, rather than a theatrical encounter with the sovereign state, while the sovereign state takes a back seat and plays an orchestrating role; second, the encounter in various small disciplinary mechanisms is mediated by a discourse of individual rights which conceals the actual power imbalance in the disciplinary regime. The commercial relationship mentioned earlier is an example where the discourse of the user’s rights premised on free will and contractualism can actually help to rephrase the power of companies to monitor and manipulate user preferences and courses of action as the provision of better services.

3. The dark side of pastoral liberalism and its amplification in the digital context

3.1 The totalising and illiberal tendency of pastoral liberalism

The takeaway from the previous discussion about pastoral liberalism is an intrinsic dilemma of the state-subject relationship. The *raison d’état* of the modern state is to govern and direct its subjects for happiness and prosperity, and for this reason, the modern state problematizes individual existence in various ways (*i.e.*, birth rate, health, education, etc.) and makes them the concern of state intervention. The enterprise of modern human rights law is the heir to the *raison d’état*. In the pastoral relationship, power is not just repressive and negative as manifested by injunction, prohibition and punishment, but becomes positive and productive. It produces individuals as subjects bearing rights and it helps subjects realize their rights and

⁵⁵ Foucault, *supra* note 44 at 107–108.

⁵⁶ Lecture on 14 January 1976, in Michel Foucault, *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977*, 1st American ed, Colin Gordon, ed. (New York: Pantheon Books, 1980) at 105.

increase their welfare. Indeed, it is especially emphasized in Foucault's later work that the pastoral power of the modern state produces possibilities of resistance, the so-called "counter-conduct". He argues that power, when understood as action upon the action of others, presupposes the agency of others.⁵⁷ If bringing this view to the context of contemporary digital surveillance, we can perhaps speculate that surveillance-based governing could produce possibilities of its own failure, and that the reason of the failure might not only be that digital surveillance also could drive some form of digital anarchist activism that undermines surveillance-based governing. More importantly, if power presupposes the agency of others, surveillance-based governing that operates a self-referring loop, nudges people's choices, and makes the future an ever-present cannot sustain itself as a technology of power because it fundamentally denies people's agency.

Such possibilities of resistance are so far just hypothetical and in need of more empirical studies to back up. For the purpose of this section, I want to argue that albeit the positive and productive side of pastoral power, the intrinsic dilemma is that pastoral liberalism requires a massive pacification of people which is the result of the *raison d'état* of the modern state and the concealment of the oppressive and violent side of policing power. This pacification is also realized through modern law's transformation and rationalization of encounters by which individuals, while being recognized formally as legal subjects also become the objects of various disciplinary apparatus which are legally authorised. The massive pacification of people through modern law's normalization of legal subjects and disciplinary power can be related to Habermas's discussion about the "colonisation of the lifeworld," where he points out the ambivalence of legally-institutionalised welfare policy that guaranteeing freedom and taking it away are both attached to welfare state. While individuals can secure welfare rights through legal means, their lives need to be restructured to fulfil the legal conditions for welfare benefits, which render the rights-holders into powerless recipients of a paternalist welfare state.⁵⁸

⁵⁷ Michel Foucault, "The Subject and Power" (1982) 8:4 Crit Inq 777 at 790 ["Power is exercised only over free subjects, and only insofar as they are free...faced with a field of possibilities in which several ways of behaving, several reactions and diverse comportments, may be realized."].

⁵⁸ Jürgen Habermas, *The Theory of Communicative Action: Volume 2: Lifeworld and System: A Critique of Functionalist Reason* (Boston: Beacon Press, 1987) at 361–362.

The rationalization of the power of policing and the concealment of coercion and violence also changes the possibilities and ways of perceiving social conflicts and individual grievances. One quotation from George Orwell perhaps best summarizes the intrinsic illiberal and totalising side of pastoral liberalism:

There are families in which the father will say to his child, ‘You’ll get a thick ear if you do that again’, while the mother, her eyes brimming over with tears, will take the child in her arms and murmur lovingly, ‘Now, darling, *is* it kind to Mummy to do that?’ And who would maintain that the second method is less tyrannous than the first? The distinction that really matters is not between violence and non-violence, but between having and not having the appetite for power.⁵⁹

Of course, the elimination of violence is undoubtedly a huge improvement. With this quotation, I nonetheless want to emphasize that the formally rationalized way of exercising power and the beneficent character of those who are powerful can be extremely deceptive. Pastoral power is presented here as a dilemma, not as one-sidedly oppressive, but as always having its illiberal and totalising underside. This section argues that how the dilemma is balanced, maintained or overturned by one side against the other depends on techno-legal conditions. In the context of ubiquitous digital surveillance, a serious question is what conditions remain which help actualize the positive side of the surveillance power and even enact the power of resistance in a context where a dark side seems to have been unleashed beyond limitation.

3.2 The rule of law, technology’s affordance and the techno-legal restraints on the dark side of pastoral liberalism

As hinted in Section 1.2, the substantive notion of the rule of law brings the power of policing (in the broad sense), both its scope and mode of exercise, under judicial control. The power of policing is no longer presumed to be necessarily pursuing the *raison d’état* but has to be checked by law. This heightened internal separation of sovereign powers allows the power of policing to be contested in a court of law, and it is the most important aspect of constitutional democracy. It

⁵⁹ George Orwell, *The Collected Essays, Journalism and Letters of George Orwell: In front of your nose, 1945-1950* (Secker & Warburg, 1968) at 301.

means that despite the inherent unbridgeable power imbalance between the surveillant and the surveilled, and despite that the power gap is further reinforced by the fact that it is the state which exercises both the power of policing and judicial control, to control the power of policing is not simply self-referring and self-judging. The substantive notion of the rule of law splits sovereignty internally: both the rule of law and the power of policing stem from the state's monopoly of violence, but the former controls the latter and controls the discretionary character of policing that exceeds formal legalism. Unlike the policing relationship where the surveillant has almost absolute advantage, the rule of law contains crucial opportunities for resistance by people, not only by way of claiming that the policing power does not “go by the book”, but more importantly by contesting what the law means and requires. The uncertainties surrounding law have been constantly explored by state agencies when expanding their surveillance power. Parts I and II of this study have discussed at length how the legal vacuums of surveillance operations are constructed by exploiting the existing legal framework. However, it is also important to highlight that legal uncertainty can be made to the advantage of individuals as well. The notions of proportionality and necessity, for example, are vague and allow for discretion, but precisely because of the underdetermined character of such notions, arguments can be made to problematize surveillance measures and to demonstrate their violation of the rule of law. For example, the *Tele2 Sverige* case⁶⁰ and the *Digital Rights Ireland* case⁶¹ before the CJEU involved the assessment of the proportionality of domestic legislation requiring the bulk retention of user communications data, (including all traffic and location data for all means of electronic communications), for the purpose of the prevention, investigation and prosecution of criminal offences. The domestic laws that were challenged in the two cases were implementing laws of EU Directive 2006/24.⁶² Before EU Directive 2006/24 was adopted, there was an impact assessment done by the European Commission which claimed that the bulk retention of communications data was proportionate because it excluded the content of the

⁶⁰ *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*, Joined Cases C-203/15 and C-698/15, [2016] ECLI:EU:C:2016:970 (“*Tele2 Sverige* case”).

⁶¹ *Digital Rights Ireland Ltd v. Minister for Communications and Others*, Joined Cases C-293/12 and C-594/12, [2014] ECLI:EU:C:2014:238 (“*Digital Rights Ireland* case”).

⁶² In *Tele2 Sverige* case, the UK 2014 Data Retention and Investigatory Powers Act that was challenged was not an implementing legislation of the Directive 2006/24, but established a general body of rules for the retention of communications data.

communications.⁶³ This assessment of proportionality was challenged in these two cases. As mentioned in Part II, the CJEU held that the communications data, taken as a whole, could allow very precise conclusions to be drawn about the private lives of the individuals whose data had been retained.⁶⁴ This then changed the proportionality assessment concerning the impact on fundamental rights and the EU Directive 2006/24 and domestic implementing legislations were quashed.

The scrutiny of the rule of law engages with these politically difficult and contested questions, and the indeterminacy of these questions can be turned into opportunities for individuals to advance their claims. Conceivably, such opportunities can also be created with the often poorly defined purpose of surveillance measures, such as the protection of national security, counterterrorism, economic interest, etc., which are accepted as legitimate purposes for imposing surveillance measures. Admittedly, courts have largely avoided such highly political determination, but the common strategy of argumentation by claimants is to connect the broadly defined purposes with procedural restrictions on surveillance agencies to argue that these purposes can(not) provide meaningful restrictions.⁶⁵ The question becomes whether the invoked purposes are meaningful under a surveillance regime. The power imbalance between the surveillant and the surveilled remains, especially since the two parties often do not have the same access to information, which is seen in the example of the UK's Investigatory Powers Tribunal. But at least, the rule of law provides this crucial avenue of resistance.

Ultimately, the indeterminacy surrounding these legal concepts inheres to human language, communication and reasoning. As will be seen in Chapter 6, communication is discussed by Levinas as not being about securing a common understanding, but about its infinity. We can never know if we and our interlocutor are talking and thinking about the same thing and we can never expect the interlocutor's reaction with absolute certainty, and hence we need to keep communicating and always remain attentive to each other. The rule of law can be related to

⁶³ European Commission, *Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC [SEC(2005) 1131]*, COM-2005-492 (Brussels, 21 September 2005), at 7.

⁶⁴ *Tele2 Sverige* case, *supra* note 47, para.99; *Digital Rights Ireland* case, *supra* note 48, para.27.

⁶⁵ E.g. *10 Human Rights Organisations v the United Kingdom*, no.24960/15, "Additional Submission on the Facts and Complaints" (9 April 2015) at 11, para.46. *Roman Zakharov v Russia*, No 47143/06 (4 December 2015), paras 191-218; *Szabó and Vissy v Hungary*, No 37138/14 (12 January 2016), paras 46-48; *Kennedy v the United Kingdom*, No 26839/05 (18 May 2010), paras 131-136.

this moral sense of the responsibility of communication. It is not only that individuals can take advantage of the inherent uncertainty of legal language to advance their claims, but that at a moral level, perhaps counterintuitively, there is an obligation to preserve legal uncertainty so that the rule of law always gets energy from the unexpected nature of human relations. Due process rules that guarantee the individual right to contest and the right to be heard are hence crucial for the rule of law. The uncertainty of legal language and legal argumentation is emphasized as a virtue by Waldron:

The institutionalized recognition of a distinctive set of norms may be an important feature. But at least as important is what we do in law with the norms that we identify. We don't just obey them or apply the sanctions that they ordain; we argue over them adversarially, we use our sense of what is at stake in their application to license a continual process of argument back and forth, and we engage in elaborate interpretive exercise about what it means to apply them faithfully as a system to the cases that come before us.⁶⁶

So, the illiberal and totalising underside of pastoral liberalism is kept in check by this avenue of legal argumentation under the rule of law. It is however important to also note that the inherent uncertainty of legal language is contingent on certain technology that mediates human communication. Hildebrandt discussed modern law and the modern state as the affordances of the printing press: the rule of law emerged from the need to interpret a written norm in light of the web of applicable norms and the case at hand and ultimately, the need to decide authoritatively on how to interpret the norm.⁶⁷ While written text always needs interpretation by its readers, the printing press and its proliferation meant that the opportunity to interpret and challenge a given interpretation of a written legal text proliferated as well.⁶⁸ A written legal text is open to interpretation by anyone who reads it. Of course, the job of legal argumentation and interpretation is largely taken over by lawyers and the state's courts decide how a dispute is

⁶⁶ Jeremy Waldron, "The Concept and the Rule of Law" (2008) 43:1 Ga Law Rev 1 at 56.

⁶⁷ Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing, 2015) at 180.

⁶⁸ *Ibid* at 177–178.

finally settled. However, the uncertainty in how a text will be interpreted in light of a particular situation is not and cannot be eradicated by any legal reasoning made *ex ante*.⁶⁹

Mentioning the technological condition of the rule of law is important for considering the implications of surveillance technologies and digital automation of the rule of law. Digital surveillance and the related technologies of simulation and automation change the mode of knowledge production and reasoning. They dovetail with formal legalism in the sense that both aim for perfect certainty, predictability and mechanical application of rules. It is hence deeply problematic that solutions for the legal and procedural deficits of surveillance programs, while invoking rule of law principles, increasingly bend toward formal legalism and bureaucratic micromanagement. Clearly articulated legal bases and procedural requirements are indeed necessary, but from the perspective of the substantive notion of the rule of law, these requirements should not be fetishized; their implementation should not amount to creating a formally challenge-proof surveillance regime which removes the unexpectedness of the human rights encounter.

I will revisit this idea in Chapter 6, but for now I will reiterate the example of proportionality assessment to illustrate the point. Proportionality assessment discussed in earlier examples is an exercise of human, legal reasoning which is open to questioning and needs justification. We can imagine a proportionality assessment which is done by relying on vast datasets of human behavioural patterns and uses machine learning to score human rights risks. An example is the collateral damage estimate in drone attacks as depicted in the movie *Eye in the Sky*. There, a 45 percent chance of fatal injury to the little girl selling bread in the immediate vicinity of the target area was finally accepted for the attack to proceed. The number was fudged by the targeteer in the movie. But say, if the algorithmic program had initially given a number below a 50 percent fatality assessment, the strike would proceed with a lot less back-and-forth using legal and moral arguments. The point is that to resort to algorithmic programs for objective assessment changes the nature and focus of deliberation: human assessment by soldiers on the ground becomes computerised calculation, which can only be countered by a different algorithmic program. The question about acceptable trade-off between the life of one's own

⁶⁹ *Ibid* at 148–149.

soldiers and the life of the enemy's civilians⁷⁰ comes down to fabricating a number about civilian casualties. A procedurally flawless strike – high precision, low civilian casualties, prior authorisation and *ex post* oversight, etc., could divert many complex legal and moral debates about just war, surveillance and datafication of the enemy population which pave the way for such a strike. Conceivably, surveillance programs can be introduced to many other areas of governance and business and can be made procedurally and legally challenge-proof to quieten public debate.

4. Conclusion

Chapter 5 has tried to demonstrate modern law's constitutive role in transforming the human rights encounter. I have argued that modern law rationalizes the way in which individuals encounter institutions, most notably the modern state and the way in which power struggles in such encounters are fought. The history of the political expropriation of the modern state and the power of policing shows that law tames the policing power of the state and shares the object and purpose of policing of the modern state – to increase common welfare. Modern law's rationalization of encounter is also accompanied by the evolution of law into a disciplinary apparatus that works closely with and orchestrates other disciplinary regimes in the modern state. Human rights law pushes modern law's rationalization of encounter further and makes more explicitly the individual's life the concern of state. Relating this account of modern law to Foucault's discussion of pastoral power suggests the difficult dilemma of pastoral liberalism, which empowers individuals as rights-holders, and disempowers individuals as passive recipients of social welfare; reveals the power of surveillance and policing through legalization, and conceals this power by the expansion of commercialisation and contractualism.

Hence, the illiberal side of pastoral liberalism is the massive pacification of people. This illiberal side is amplified when formal legalism is considered as equivalent to the rule of law because formal legalism sees legal uncertainty and the ambiguity of human language and human reasoning as pathologies that need to be eliminated. The impact of formal legalism is serious. As seen in Parts I and II, solutions for the challenges posed by digital surveillance often resort to

⁷⁰ Frédéric Mégret, "The Humanitarian Problem with Drones" (2013) 2013:5 Utah Law Rev 1283 at 1305–1308.

formalist legal requirements and procedural guarantees, which then tend to reproduce many of the problems they are meant to solve. But to see why resorting to formal legalism and bureaucratic rationality is like a knee-jerk reaction to a perceived regulatory challenge, it is important to note that in the evolution of modern law into a disciplinary apparatus, legal positivism is the dominant account of law. This is also reflected in Foucault and Foucault-inspired work on modern law and policing. So, perhaps one way to reflect on this body of Foucauldian literature is to argue that while it emphasizes counter-conduct and resistance, with its positivist view of law, it forgoes a vital chance of resistance through law. In Chapter 6, I will explore the opportunity of resistance through law by amplifying the rule of law with Levinas' and Arendt's writings. Before that, I will conclude Chapter 5 by connecting with some observations made about the deployment of surveillance in Parts I and II.

Having discussed the historical emergence of the power of policing and pastoral liberalism, we can reconsider the examples discussed in Chapter 1. First, despite the disparate situations and relationships involved in those examples – targeted or mass surveillance for intelligence and crime investigation, the administration of the justice system, the provision of social benefits, targeted advertising, etc. – they can all fit into a model of pastoral liberalism in which the power of the surveillant actor is claimed to be exercised for some sort of self-defined common good. In the state-subject relationship, even in cases like *Jawar Mohammed* where political dissidents were targeted and freedom of expression was violated, the government can still resort to the vague notion of national security or crime prevention to assert itself as the legitimate insurer of the common good. It might be a disingenuous claim to make in cases like *Jawar Mohammed*, but the basic premise that the state can use surveillance for the common good is not disputed. In commercial relationship, the common good that is claimed by tech companies such as Google and Facebook can arguably be conceived as helping individual users to exercise the right to self-determination. This perhaps sounds a bit strange as I have argued that informational self-determination is very much mythical in our relationship with digital service providers. But the emergence of the digital economy in the mid-1990s and early-2000s was celebrated as a “friction-free capitalism”⁷¹ that would break up the control of capitalist conglomerates. So, while tech companies like Google have become conglomerates now, they

⁷¹ Bill Gates, Nathan Myhrvold & Peter Rinearson, *The Road Ahead* (New York: Penguin Books, 1996) at 180.

keep emphasizing the importance of individualized products and services to make users feel some sense of ownership. In both relationships, the self-defined common good is often used to legitimise and enhance the power of the surveillant actors rather than impose restrictions. For example, the “common good” to protect the individual’s personal data and privacy is used to justify centralized control of the data by both governments and companies.⁷²

Second, it is remarkably difficult to perceive the control exerted on individuals that is enabled by digital surveillance. In Chapter 1, I discussed the temporal and spatial dissolution of a human rights encounter with surveillance agencies. In addition, I have also discussed the nudge theory, which argues that control can be made non-coercive by creating a certain choice architecture that directs an individual’s choice in a predictable way. All these technologies and strategies to hide the surveillant gaze and the actual power relationship can be connected to pastoral liberalism where the shepherd has to keep him or herself at a distance. These technologies and strategies can potentially unleash the illiberal and totalising side of pastoral liberalism by changing the confrontational nature of the power relationship and by removing opportunities for perceiving injustice, conflicts and grievances. A quote from Confucius can perhaps be the motto of such illiberal surveillance-based governance: “The people may be made to follow a path of action; they may not be made to understand it.”⁷³

Third, surveillance technologies and the related data analytical technologies provide unprecedented opportunities for the power of policing to realize its objectives. The police state and its modern version, the welfare state, engage in calculating processes to distribute social resources and risks. However, as observed by both Smith and Weber, the capacity of the state to obtain knowledge and exercise rational decisions is limited. For Smith, this is why the invisible hand of the market is needed to complement the state’s inabilities, while for Weber, a state should constrain itself by legal rationalism from arbitrarily intervening in the economy.⁷⁴

⁷² E.g. Matthew Panzarino, “Apple’s Tim Cook Delivers Blistering Speech On Encryption, Privacy”, (2 June 2015), online: *Tech Crunch* <<https://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/>> [Apple’s CEO Tim Cook spoke at the EPIC’s champions of Freedom event in 2015 that “some of the most prominent and successful companies have built their businesses by lulling their customers into complacency about their personal information... They’re gobbling up everything they can learn about you and trying to monetize it. We think that’s wrong. And it’s not the kind of company that Apple wants to be.”].

⁷³ *Confucian Analects, the Great Learning, and the Doctrine of the Mean*, translated by James Legge (Hong Kong: Lane, Crawford & Company, 1861) at 75.

⁷⁴ Colin Gordon, “The Soul of the Citizen: Max Weber and Michel Foucault on Rationality and Government” in Sam Whimster & Scott Lash, eds, *Max Weber Ration Mod* (293-316: Routledge, 2006) at 301.

Regardless of the implicit idea of the economic rationalism of the capitalist market in Smith and Weber, their observations essentially point to human knowledge as finite and the spontaneity of human activities which then require political and legal institutions to ensure the rationality and proper functioning of the government and the market. Arguably, this need for political and legal institutions as rationalizing and stabilizing mechanisms will be radically changed by surveillance and data analytical technologies as they promise full knowledge of human life and interactions from a “God’s eye” view. This critique about the promise of full knowledge is to question whether the knowledge obtained by big data analytics is true or false. What the nudge theory suggests is that it can be made true by providing particular choice architecture. So, it is possible that the shepherd becomes indeed omnipresent and omnipotent by surveillance and data analytical technologies. At that point, whether we need political and legal institutions at all for democratic deliberation and legal argumentation would become questionable. This is not just for political authorities but is also pertinent for considering the power of commercial entities.

Chapter 6. Reviving the human rights encounter

Following the previous discussions of pastoral liberalism, its hidden totalization and modern law's subjectivation and pacification of people, we may ask if the prototypical human rights encounter is actually a rationalized form of domination that reproduces power imbalances, why still hold on to human rights and law as a possible way of resistance and ultimately, of emancipation. To be more specific, if surveillance is a necessary element of ruling premised on pastoral liberalism and human rights law's role is to reveal-conceal it to make it more ideologically acceptable, what exactly can the idea of human rights encounter offer and why not get rid of human rights discourse?

Chapter 6 will examine those questions. As I argued in Chapter 5, modern law and pastoral liberalism operate according to a structure of empowerment-disempowerment, and this is understood as a dilemma – *i.e.*, the subjectivation of individuals by modern law and pastoral power both empowers and pacifies individuals – rather than as one-sided oppression. This chapter therefore explores possibilities of resistance by retrieving the normative foundations and aspirations of human rights and the rule of law. Those normative foundations and aspirations may have been marginalized by current legal practices and discourses that subscribe to the instrumentalist approach to law and become managerialist. Because they do not fit with current legal work, the institutionalization of those normative foundations and aspirations is difficult. But they should be intensified and should haunt current legal work and in particular the surveillance-based governing logic.

In Section 1 which follows, I trace the normative underpinnings of the human rights encounter to Emmanuel Levinas' and Hannah Arendt's writings about the human encounter. Although the prototypical human rights encounter, as discussed in Chapter 5, is a rationalized, legally constructed encounter, the very idea of encounter contains uncertainty, chaos, surprise and spontaneity. These aspects realized through human encounter are essential and constitutive of the self and the collective subjectivity in Levinas' and Arendt's work. Levinas' "infinity of the Other" and Arendt's "human plurality" are their attempts at "escaping from being" informed by

their experience of totalitarianism. I will draw upon their respective efforts to amplify the human rights encounter and the rule of law to escape from a totalizing, monotonous, self-referring loop of surveillance-based governing.

In Section 2 which is inspired by Levinas' and Arendt's work on the human encounter, I try to connect the normative significance of human spontaneity and uncertainty to the rule of law, arguing that human spontaneity and uncertainty are the reasons why we need law and more importantly, the sources of energy, as well as aspiration for law. So, despite what has been said about modern law's totalizing side in Chapter 5, the rule of law is not a "humbug"; only formal legalism is. The relationship between human encounter and law can be seen as this: because human encounters are full of surprises and unforeseen consequences, we need law to stabilize and structure human relationships; because law presupposes human spontaneity, it also has to preserve human spontaneity, or otherwise law will be unrooted.

This claim may seem unsurprisingly liberal, but arguably it is often not what policy-makers and legal practitioners think of when invoking the rule of law. As I have shown in Part II, the common instrumentalist discourse of law underlying current regulatory regimes for digital surveillance leads to rather mechanical applications of the formal requirements of legality. Motivated by Levinas' and Arendt's work, I argue that formal requirements of legality constitute constraints on the arbitrary power of powerful institutions because they preserve possibilities of, and even invite, unexpected human rights encounters. It is perhaps inevitable that the constraints offered by law on surveillance institutions can be turned into a form of discipline which also reinforces the power of surveillance institution. However, I would contend that a Levinasian-Arendtian account of the rule of law does not discipline, but in principle prohibits the very power of surveillance that eliminates human spontaneity. In addition, by preserving human spontaneity and inviting the human rights encounter, the rule of law makes it possible to constantly unsettle the power of surveillance institutions and its legal mode of existence.

Section 3 concludes Chapter 6 by articulating the normative implications of the loss of the human rights encounter. It weaves together the ideas of the previous two sections and reflects on the critiques of surveillance-based governance and the management of surveillance by formal legalism made throughout this study.

Going back to the questions at the beginning of this chapter: why still hold on to human rights and the rule of law? There is no guarantee that they promise emancipation, and the possibilities of emancipation need to be created by exploring new (or old) ideas about them and constantly tested by praxis. After criticizing the current regulatory regimes on digital surveillance and the dominant instrumentalist discourse of law, the last part of the study will convey some sense of hope and the need to keep engaging with human rights and the rule of law, which are essentially about preserving and exercising our own agency.

1. The theoretical underpinnings of the human rights encounter

1.1 Appreciating human uncertainty

As previously indicated, I draw on Levinas' and Arendt's work to argue that there is something deeply normative in the human encounter. Before surveying their specific thoughts, it is useful to explain why I choose these philosophers and what general threads relate them to the topic of my study. Briefly speaking, Levinas and Arendt belong to the same generation of philosophers, were trained in phenomenology, and their work dealt with essentially same problems about the alienation of modernity and the horror of totalitarianism. They both had experienced Nazi terror and the prospect of total war which profoundly influenced their thoughts. They were critical about abstract theories of human essence and progressive accounts of history that absorb and eliminate the contingencies of real-life experience. But their approaches are not the same. Levinas sought, "an escape from being", through a truly transcendental encounter with the Other which is absolutely different from *me, the self*. Arendt, in contrast, emphasized the "in between" that conjoins people and makes a common world. In their respective work, human encounter is a magical experience that constitutes the self and the collective identity. Human encounter reveals and actualizes the infinity of the Other and human plurality which exceed reduction and totalisation. This irreducible infinity of the Other and human plurality is a phenomenological observation, but also a prescriptive claim; that is to say, the infinity of the Other and human plurality should be preserved to defeat reduction and totalisation. This prescriptive claim reflects the influence of the prospect of annihilation of humanity by all-out nuclear war in their time.

Levinas' and Arendt's respective thoughts on totalitarianism and their attempts to revive humanity from totalitarianism, modern mass society and the prospect of total annihilation

provide many important insights for thinking about surveillance-based governing. As has been discussed throughout this study, surveillance-based governing is premised on the datafication of everything, the past, the present and the future. Though there are perceptible differences between surveillance-based governing and Nazi and Soviet totalitarianism, the all-encompassing character of surveillance-based governing needs to be interrogated with a view to unveiling the violence inherent to it. This is especially pressing because this form of governing positions authorities to become increasingly capable of concealing violence and dissolving confrontational encounters. Another thread that links Levinas' and Arendt's work with surveillance-based governing is the world alienation in modernity in which science and technology have played a major role and that has led to ungrounded notions of rights and the flattening of right-subjects. Their critiques of the lack of authentic intersubjective encounter in modernity contain many warnings for the current surveillance-based governing and surveillance capitalism.

1.1.1 Levinas

Levinas' attempt to escape from being is about reversing orders. As reformulated by Robert Gibbs, the central question Levinas asks is not, "is it rational to be ethical", but, "is it ethical to be rational".¹ Levinas laments the subject of traditional western philosophy, especially since the Enlightenment. The subject is independent and self-sufficient. It appropriates, objectivizes and thematizes the otherness of the world into concepts, doctrines and knowledge for its own use. The subject is a totalising subject: "Modern man persists in his being as a sovereign who is merely concerned to maintain the *powers of his sovereignty*". The activity of knowing is a totalising activity in which the subject constantly affirms sameness. Levinas expresses deep agony in *Otherwise than Being or Beyond Essence*,

To reduce men to self-consciousness and self-consciousness to the concept, that is, to history, to deduce from the concept and from history the subjectivity and the "I" in order to find meaning for the very singularity of "that one" in function of the concept, by neglecting, as contingent, what may be left irreducible after this reduction, what residue there may be after this deduction, is, under the pretext of not caring about the inefficacy of "good intentions" and "fine souls" and preferring "the effort of concepts" to the facilities of psychological naturalism,

¹ Robert Gibbs, *Correlations in Rosenzweig and Levinas* (Princeton, N.J: Princeton University Press, 1992) at 243.

humanist rhetoric and existentialist pathetics, to forget what is better than being, that is, the Good.²

Levinas says, “Not ‘[w]hy being rather than nothing?’, but how being justifies itself”.³ Such a self-sufficient subject suffers from, “ennui ... the enchainment to itself, where the ego suffocates in itself due to the tautological way of identity”⁴. It is possible to see how his own experience of being a prisoner of war in a German concentration camp had influenced his deep resentment about the self that is emptied of everything that can justify its being. The self cannot simply exist on its own and there must be something before ontology. Going beyond the self, Levinas says, “The social is beyond ontology”.⁵

The face-to-face encounter with the Other breaches the ego of the subject. Levinas describes the epiphany of the face as constituting a penetration of the crust of the self which is preserved in its being and preoccupied with itself.⁶ The face of the Other is the way in which the Other manifests itself to the self without going through any mediation. The face of the Other is present in its refusal to be contained: it cannot be comprehended, encompassed; it is not graspable.⁷ It resists my power. The face cannot be ascribed with a signification in relation to other things because the alterity of the Other is not relative. The epiphany of the face of the Other breaks up the world common to us. In a truly transcendental encounter in which the self can “escape from being”, the Other is infinitely foreign and non-recurrent. The face-to-face is not lateral; the approaching of the face is from a dimension of height,⁸ and so the relation with the Other is always unequal and un-reciprocal.

But the face of the Other resisting my power does not purely negate *I*. The face facing me speaks to me and invites me to a relation that is different from domination and identification in all the other sensible experience. The face should not be taken literally but suggest an immediacy

² Emmanuel Levinas, *Otherwise Than Being or Beyond Essence*, translated by Alphonso Lingis (Martinus Nijhoff, 1981) at 18–19.

³ Emmanuel Lévinas & Seán Hand, *The Levinas reader*, Blackwell readers (B. Blackwell, 1989) at 86.

⁴ Levinas, *supra* note 2 at 124.

⁵ Emmanuel Lévinas, *Ethics and infinity: Conversations with Philippe Nemo*, 1st ed, translated by Richard A. Cohen (Pittsburgh: Duquesne University Press, 1985) at 58.

⁶ Emmanuel Lévinas, *Alterity & transcendence* (Linton: Athlone, 1999) at 171.

⁷ Emmanuel Levinas, *Totality and Infinity: An Essay on Exteriority*, translated by Alphonso Lingis (Pittsburgh: Duquesne University Press, 2007) at 194.

⁸ *Ibid* at 214–215.

and an insolvable distance that makes the Other unreachable and ungraspable. In his later writing, Levinas elaborates the notion of the face as an ethical plane: the face is complete defencelessness and vulnerability, the extreme exposure and the extreme directness to inexorable death.⁹ This naked face facing me, in its mortality, “summons me, demands me, requires me”, as irreplaceable.¹⁰ The invisible death faced by the face of the Other puts me on the spot, calls me into question, as if the death faced by the face concerns me even before I was concerned by my own condemnation to death, as if I were guilty for my own surviving and I would become the accomplice of that death faced by the Other by my possible indifference.¹¹ So, facing the naked face of the Other calls myself into question about my being and the right to be. There is a fear for the violence generated from my pure being despite my conscious and intentional innocence. Such being called into question also means there is a primordial responsibility for the Other that is not assumed by the subject as an act of will. So, the encounter with the Other has the dramatic effect of constituting the self through affection, shock and even shame.¹²

The constitution of subjectivity is an intersubjective process in the encounter with the Other. The encounter constantly interrupts the established identity and transcends the egoist self; the self is responding to and takes responsibility for the Other, and the responsibility for the Other is preconscious. This preconscious vulnerability and absolute passivity of the self are seen by Levinas as the “original good”, rather than original sin.¹³ Moreover, we can also discern a temporal dimension to this ethical relationship with alterity. Interaction with the Other needs to be kept open and always ongoing. The self should never close itself by a settled and hence, a thematised relationship with the Other and should constantly open itself for interruption and challenge. Surely, the constant interruption by the Other and the openness of the self does not make the self comfortable. The self is always under the mercy of that which is uncertain and

⁹ Levinas talked about the Other “has no other place, is not autochthonous, is uprooted, without a country, not an inhabitant, exposed to the cold and the heat of the seasons.” Levinas, *supra* note 2 at 91. The Other is “the stranger, the widow, and the orphan”. Levinas, *supra* note 7 at 215.

¹⁰ Lévinas, *supra* note 6 at 24.

¹¹ *Ibid* at 24–25. The non-indifference to the Other (my neighbor) is the very meaning of the responsibility for the other, the primordial responsibility beyond any voluntary commitment.

¹² Levinas, *supra* note 7 at 252. [“My arbitrary freedom reads its shame in the eyes that look at me. It is apologetic, that is, refers already from itself to the judgment of the Other which it solicits, and which thus does not offend it as a limit.”]

¹³ Levinas, *supra* note 2 at 121.

uncontrollable. But it is only by experiencing and responding to these circumstances, that the self can overcome the nightmare of being alone.

In brief, Levinas' reversal of the subject-object relationship intensifies these two points: the impossibility of a self-contained sovereign; the absolute freedom and the infinity of the Other against totalization. A self-contained sovereign is stuck in solipsism, forgets "the Good" and cannot justify its being. It can only transcend solipsism by being absolutely vulnerable to the infinite Other, and the responsibility for the Other justifies its being.

1.1.2 Arendt

Arendt's attempt against totalitarianism is to bring human plurality to the center of political theory, letting the phenomena of plurality "shine forth". Plurality is about the uniqueness of each individual as actualized and disclosed in being together with other people. Plurality is not about certain perceivable properties of human beings; it is not what human beings are but what human beings do. It is expressed and experienced through one's action in, "sheer human togetherness".¹⁴ The action that reveals an individual's uniqueness always needs someone else's co-presence and participation.¹⁵ The emphasis on action and its presupposed human togetherness means that plurality is not something to be simply inserted from the outside into an already existing world. Whereas the key term for Levinas is "otherwise than being", for Arendt it is "being with", being with others in the world which is the realm of human affairs. While the emphasis is not on a vertical (as in Levinas), but a horizontal structure, this horizontal structure does not mean flattening, but the weaving of the web of human relationships while preserving the individual's freedom, uniqueness and dignity.¹⁶ This "in-between"¹⁷ both separates and connects people, making each individual irreducible to the same while also giving rise to a common world where the plural *we* inhabit and create reality and meaning.¹⁸

¹⁴ Hannah Arendt, *The Human Condition* (Chicago: University of Chicago Press, 1958) at 180.

¹⁵ Arendt distinguishes between labour, work and action, and sees action as the only activity that goes on directly between human beings and corresponds to the human condition of plurality and the political life. Labour and work are primarily apolitical, if not all private. *Ibid* at 7–9.

¹⁶ *Ibid* at 180.

¹⁷ Keith Breen, *Under Weber's Shadow: Modernity, Subjectivity and Politics in Habermas, Arendt and MacIntyre* (Farnham, Surrey, England; Burlington, VT: Ashgate, 2012) at 97.

¹⁸ Arendt, *supra* note 14 at 52, 182–183.

¹⁹ This is in stark contradistinction to Heidegger, who sees being together in public as completely absorbing the Dasein and hence, considers the public primarily negative. See, Sophie Loidolt, *Phenomenology of Plurality:*

While Arendt goes beyond the dyadic relationship, she shares with Levinas the phenomenological approach by which the “in-between” has to be experienced from the first person and the second person perspectives. Underlying the phenomenological approach is the key notion of intersubjectivity.¹⁹ Each manifestation of the uniqueness of the individual always relates to others and to the world and the individuality is revealed and unfolds in intersubjective encounters. But by moving beyond the dyadic relationship and being attentive to the common world, the “in-between”, Arendt highlights the fragility of the common world. Not only are there always new actions and newcomers that change the common world, but human actions and also their consequences carry “the enormous risk” of deadly and irreversible destruction.²⁰

In addition, Arendt observes two more threats to the common world in *The Human Condition*. One is modern mass society in which the space in-between that separates and relates people is lost and people are either radically isolated or homogenized.²¹ The pathology of mass society is a common theme among philosophers in the early 20th century. For example, Husserl discerned the “inauthentic” community which is, “an imperialist organization of will, a central will in which all single wills are focused and to which all must subordinate themselves.”²² The inauthentic community totalises the *plural we* into an overwhelming central will. By totalising, individual autonomy is taken away, which hence leads to mindlessness and laziness.²³ This echoes Arendt’s observation of Adolf Eichmann “not stupidity but thoughtlessness”.²⁴ Reflecting on the conditions of the Holocaust, Zygmunt Bauman connects Arendt and Levinas and holds that the creation of social distance through the apparatus of modern industry, transportation,

Hannah Arendt on Political Intersubjectivity, Routledge research in phenomenology 7 (New York: Routledge, Taylor & Francis Group, 2018) at 121.

¹⁹ Dan Zahavi, “Beyond Empathy: Phenomenological Approaches to Intersubjectivity” 8:5–7 *Journal of Consciousness Studies* 151 at 166 [“the subjectivity that is related to the world only gains its full relation to itself, and to the world, in relation to the other, *i.e.* in intersubjectivity; intersubjectivity only exists and develops in the mutual interrelationship between subjects that are related to the world; and the world is only brought to articulation in the relation between subjects.”].

²⁰ Arendt, *supra* note 14 at 268–269.

²¹ *Ibid* at 52–53, 58.

²² Philip Buckley, “Phenomenology as Soteriology: Husserl and the call for ‘Erneuerung’ in the 1920s” (2019) 35:1 *Mod Theol* 5 at 15–16.

²³ In the meantime, individual mindlessness also contributes to the making of an imperialistic community. *Ibid*.

²⁴ Hannah Arendt, *The Life of the Mind: The Groundbreaking Investigation on How We Think* (New York: Harcourt Brace Jovanovich, 1981) at 4.

bureaucracy and technology of the Nazi regime replaced the proximity of being with the Other and marginalized moral drive at the mundane interpersonal level.²⁵

Bauman's argument leads to the other threat to the common world discussed by Arendt. It is the capacity of human beings, dramatically augmented by modern science and technology, to rebel against our earthly existential conditions and replace them with man-made conditions. The earthly existential conditions are our own finitude and vulnerability, as well as the uncertainty of others, the world and the future; the man-made conditions are certainty and security. When the creation and imposition of the man-made conditions take the form of scientific truths, articulated by mathematical formulas and technologically proved, Arendt argues that the man-made conditions do not, "lend themselves to normal expression in speech and thought".²⁶ Their expression in science and technology impedes intersubjective communication and deliberation. The consequence, Arendt warns us, is that we are capable of doing things that we do not fully understand and that we risk becoming slaves to our know-how. More importantly, replacing the earthly existential conditions with man-made conditions eliminates not just our vulnerability, but also the conditions for human dignity to thrive. As will be discussed shortly, these insights on modern mass society, science and technology bear great importance for understanding the stakes of surveillance-based governing and help to think about consumer society and the so-called "attention economy" that digital surveillance is embedded in.²⁷

Whereas Levinas speaks about the responsibility for the Other and the preservation of the infinity of the Other, Arendt emphasizes the responsibility of caring for the common world and preserving the world of human plurality. As mentioned earlier, they resent totalitarianism and the idea of the sovereign self that is celebrated by western philosophy and political theory. They share the key insight that the vulnerability and insecurity of human beings and the chaos and uncertainty of human relations are not negative, but constitutive of the self and collective identity. The risk when one opens one's self to others is, for Levinas, "a fine risk to be run",²⁸

²⁵ Zygmunt Bauman, *Modernity and the Holocaust*, repr ed (Cambridge: Polity Press, 1989) at 185–197.

²⁶ Arendt, *supra* note 13 at 3.

²⁷ E.g., Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads* (Knopf Doubleday Publishing Group, 2017); Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (Knopf Doubleday Publishing Group, 2010).

²⁸ Levinas, *supra* note 2 at 120.

and for Arendt, a “joy of inhabiting together with others a world”.²⁹ Levinas’ preoccupation with the reserved asymmetry with the infinite Other may give the impression of unworldliness. Arendt’s political theory helpfully complements Levinas and makes transcendental relationships political. Moreover, while Levinas emphasizes the epiphany of the face and the disruption of the self in the encounter, an encounter with the Other is not to be seen as only an exceptional moment like an eruption of magma; the encounter is as dramatic as the eruption of magma, but not a rare phenomenon. Arendt’s human plurality provides an important clarification that dramatic disruption happens at every moment when someone appears, speaks or acts in front of other people, enacting his uniqueness and bringing something new to the already existing web of relations and the common world.

1.2 From human encounter to the human rights encounter

While both Levinas and Arendt adopt phenomenological approaches in their respective work, their conceptions of human encounter, the infinity of the Other, and human plurality are not only descriptive but are also prescriptive: the infinity of the Other and human plurality are not only to be celebrated, but also what we are responsible for – we have to make continuous effort to actualize human plurality and human infinity. Inspired by their work, I bring the normative conception of the human encounter to the theory of human rights. In doing so, I am aware of Levinas’ and Arendt’s critiques of universal human rights. For Levinas, the grammar of human rights needs to be completely shifted from the right of the self to the right of the Other.³⁰ Arendt’s critiques of universal human rights that half-heartedly denounce state sovereignty are

²⁹ Arendt, *supra* note 14 at 244.

³⁰ J A Indaimo, *The Self, Ethics and Human Rights: Lacan, Levinas & Alterity* (Abingdon, New York: Routledge, 2015) at 190.

well-known.³¹ My attempt here is not to bring about a Levinasian or Arendtian human rights conception, but to think about the individual-institution encounter *with* Levinas and Arendt.³²

In addition, before explicating the individual-institution encounter, I want to draw attention to an important counter-argument about the idea of human encounter. The counterargument is that from numerous atrocities in human history, we can also reach the opposite observation that the proximity of human encounter is conducive to causing one-on-one violence, for example torture, which destroys even language and the claims of consciousness.³³ This seems to have been the case in the former Yugoslavia and Rwanda, where mass atrocities were committed by using guns, knives, axes and kitchen tools. The crimes committed by ISIS in Iraq were shocking especially due to the extremity of physical violence and proximity between the perpetrator and the victim. These are counterexamples to Bauman's thesis of, "no proximity, no responsibility", in *Modernity and the Holocaust*, but I do not think they defeat Levinas' ethics. One reason, I argue, is that we do not consider the value of philosophical inquiry by judging its empirical correspondence. Levinas' ethics, sometimes described as, "mad goodness",³⁴ or, "saintly goodness",³⁵ is aspiration derived from daily encounters³⁶ and informs daily activities, which is also why his idea of the responsibility for the Other is prescriptive. A second reason is that Levinas's face-to-face encounter is an affective experience that is much more demanding than the mere co-presence of two persons. In Levinas' transcendental encounter with the Other, the self is radically vulnerable and hence drawn to the Other. The responsibility

³¹ In, "The Decline of the Nation State and the End of the Rights of Man", Arendt famously points to the gap between the human being as a natural entity and as an artificial entity as a subject of law and that the state-centric model of human rights can barely offer any protection to people who are excluded from the political community of the state. "[T]he loss of a community willing and able to guarantee any rights whatsoever, has been the calamity which has befallen ever-increasing numbers of people. Man, it turns out, can lose all so-called Rights of Man without losing his essential quality as man, his human dignity. Only the loss of a polity itself expels him from humanity." Hannah Arendt, *The Origins of Totalitarianism: New Edition with Added Prefaces* (New York: Harcourt Brace Jovanovich, 1973) at 297.

³² E.g. Klabbers comments, "Arendt is best used not as a fount of wisdom or as providing the right answer to any concrete political problem, but rather as a source for inspiration." Jan Klabbers, "Possible Islands of Predictability: The Legal Thought of Hannah Arendt" (2007) 20:01 *Leiden J Int Law* 1 at 23.

³³ Elaine Scarry, *The Body in Pain: The Making and Unmaking of the World* (Oxford University Press, 1987) at 54.

³⁴ Lévinas, *supra* note 6 at 106–109. [Levinas talks about Vasily Grossman's novel *Life and Fate* which is about life under Hitler and Stalin. Despite the complete dehumanization in the society, there remains the "little goodness" of everyday life without witnesses. This is goodness beyond all ideology, "goodness without thought", and a "mad goodness".]

³⁵ Gibbs, *supra* note 1 at 220.

³⁶ Richard A Cohen, *Face to face with Levinas* (Albany, N.Y.: State University of New York Press, 1986) at 32–33. ["even the smallest and most commonplace gestures, such as saying "after you" as we sit at the dinner table or walking through a door, bear witness to the ethical."]

for the Other is primordial, but it also takes hard work on the part of the self to be mindful of this primordial responsibility and act accordingly.³⁷ A key feature of Levinas' notion of responsibility is that acting according to this notion of responsibility would allow people to resist the influence of a corrupted society which effectively erodes personal responsibility.

Having responded to this counterargument, I will now consider how "aspiration"³⁸ could inform the way we think about human rights and the individual-institution encounter. A normative notion of the human rights encounter inspired by Levinas and Arendt starts from the claim that human rights ought not to be reduced to the natural properties of individuals, but have to be experienced and realized by individuals through practices and interactions with other people, and even such intersubjective experiences could mean the denial or violation of rights by powerful others. The emphasis is on the experiential and performative aspects of human rights for each specific encounter.

This is informed by Levinas' and Arendt's phenomenological methodology that emphasizes inter-subjectivity rather than a third-person perspective. Inter-subjectivity means that human rights, their violation and realization are to be experienced and expressed by people in the encounter and to be given encounter-specific content. By contrast, a third-person perspective detects human rights as an objective phenomenon or imposes a certain conception of human rights on people. Intersubjective encounter means uncertainty and unpredictability of human rights experiences; each intersubjective encounter is different and people in the encounter are addressed in unique ways. Such uncertainty of the intersubjective encounter is intrinsic to human freedom. To the contrary, adopting the third-person perspective would amount to reducing the infinite and chaotic intersubjective experiences to conceptions and themes. Influenced by Levinas' and Arendt's respective attempts toward "escaping from being", a normative idea of the human rights encounter seeks an escape from the rights-subject, which is abstracted into an "empty container" to be filled with rights recognized by states or the international community.³⁹

³⁷ The difficulty and challenge of the phenomenological task of "getting past oneself" are repeatedly emphasized in the writings of Husserl and other philosophers. Peter Willis, "The 'Things Themselves' in Phenomenology" (2001) 1:1 *Indo-Pac J Phenomenol* 1 at 7.

³⁸ See discussion on aspiration in Fuller's inner morality of law in Section 3.2.

³⁹ René Urueña, *No Citizens Here: Global Subjects and Participation in International Law* (Martinus Nijhoff, 2012) at 113; Joseph HH Weiler, "The geology of international law—governance, democracy and legitimacy" (2004) 64:3 *Z Für Ausländisches Öffentl Recht Völkerr* 547 at 558. [Weiler comments on the abstraction of human rights: "The surface language of international legal rights discourse may be neo-Kantian. Its deep structure is utterly pre-modern.

This is an escape that would allow the rights-subject her or himself to articulate and give meaning to her or his rights. This escape from being an empty container echoes the strand of feminist and postcolonial studies on human rights, which seeks to move away from liberal legalism and instead give affective, experiential and material accounts to human rights.⁴⁰

The emphasis on inter-subjectivity and the first-person and second-person perspectives is critical for individual-institution encounter. In individual-institution encounter, it is not because an institution is addressed by an individual that the institution necessarily adopts an inter-subjective perspective. There is always a tendency for an institution, because of its formal rationalism, to assume a third-person perspective, claiming some sort of objectivity and authority while holding onto certain presumptions about human rights. This then turns a conflictual human rights encounter into a sender-receiver mode of management that does not take seriously the anarchic experiences of intersubjective encounter. A normative notion of the human rights encounter inspired by Levinas and Arendt, requires the institution to open up and make itself vulnerable and disturbed by the encounter with the Other.

To be more specific, Levinas' and Arendt's respective emphases – Levinas' vertical self-other relationship, and Arendt's horizontal structure of human plurality – inform in different ways how we can think of the individual-institution encounter. Transposing the self-other relationship to the individual-institution encounter, an institution that objectifies and appropriates the otherness of someone whom it encounters into sameness can be considered as the self, which includes both sovereign state and non-state institutions that exercise totalising power. The infinite Other is the plural individuals who address the institution: they may display some sort of abnormal characteristics, or perhaps their practice of human rights cannot find expression in pre-existing legal language and be comprehended by conventional legal scholarship. This (perceived) abnormality of the Other is what the self wants to eliminate or normalize. In Levinas' reversed asymmetry of the self-other relationship, the Other can be physically extremely vulnerable and can be easily exterminated, but it carries the most powerful command to call the self into its

It is a rights notion that resembles that Roman Empire which regards individuals as an object on which to bestow or recognize rights, not as agents from whom emanates the power to do such bestowing.”]

⁴⁰ See Hilary Charlesworth & Christine Chinkin, *The Boundaries of International Law: A feminist analysis* (Manchester: Manchester University Press, 2000) at 218–244; Karen Engle, “International Human Rights and Feminism: When Discourses Meet” (1992) 13:3 *Mich J Int Law* 517; Ratna Kapur, “Precarious desires and ungrievable lives: human rights and postcolonial critiques of legal justice” (2015) 3:2 *Lond Rev Int Law* 267.

responsibility.⁴¹ The self, in the reversed asymmetric relationship with the Other, is “permeable”⁴² and vulnerable in the sense that it is infinitely drawn to the Other, questions its own being and has to respond to the Other, and this respons(a)bility is preconscious. Following Levinas and reversing the asymmetry of the individual-institution encounter, the paradox of the extreme vulnerability of the Other makes it possible for the individual, however weak and desperate, to resist the totalising power of the institution. The epiphany of the face of the Other makes the institution vulnerable; the self (*i.e.*, the totalising institution) that is addressed by the Other in the encounter is disturbed by the Other and comes to realize the violence of its totalization.

Arendt’s emphasis on worldly togetherness and the fragility of the common world provides another way for thinking about the individual-institution encounter. So far as modern society needs certain institutions to organize human activities and relationships, institutions can be considered as the agent that maintains the common world. But institutions themselves are not the common world; the common world emerges from below and is woven by the spaces in-between of plural intersubjective encounters, rather than imposed from above. The common world can easily be destroyed when the agent institution becomes a self-righteous sovereign self that seeks to impose a single “horizon”⁴³ and eliminate plural encounters. The individual-institution encounter, by virtue of its chaotic and unpredictable character, reminds the institution of its own grounded-ness: the common world needs institutions to withstand human plurality; but institutions have to be mindful of their own totalising violence that could kill human plurality and also destroy the common world. Once again, for both Levinas and Arendt, vulnerability is, just like uncertainty and insecurity, not negative but constitutive of the self and collective community. Hence, there is a normative argument against the removal of vulnerability of the totalising self, which may sound counterintuitive. This will be discussed in connection with the surveillance-based form of governing in Section 3.

⁴¹ The face of the Other, which is extremely vulnerable, is the primordial expression of an obligation “you shall not commit murder”, and it defies my ability for power. I can only wish to kill, but the absolute Other exceeds my power infinitely and “paralyzes the very power of power.” Levinas, *supra* note 7 at 198.

⁴² Levinas, *supra* note 2 at 125 [“The other in me and in the midst of my identification of itself. The ipseity fractured in its return to self.”].

⁴³ Horizon is very difficult phenomenological concept. I take it as a metaphor for the background that gives an object its mode of appearance. For example, whether white vinegar is an ingredient for some dishes or disinfectant which can clean the toilet depends on the horizon in which the object – white vinegar – is situated.

Moreover, following Levinas' and Arendt's resentment of totalitarianism and alienation of modernity, a phenomenologically inspired account of human rights is always alerted to institutionalised forms of human rights realization because institutionalisation has the tendency to thematize the infinity of intersubjective encounters. Returning to Husserl, the institutionalization of politics is criticised for being increasingly unrooted from and oblivious to the lifeworld where it is founded, and the phenomenological methodologies are to reactivate the forgotten lifeworld.⁴⁴ This then helps to think about what this normative account of human encounter has to do with the human rights encounter discussed as a form of encounter rationalized by modern law and human rights discourse in Chapter 5. I will turn to this issue in the next section.

1.3 Comparing the normative notion of the human rights encounter and the legally-rationalized human rights encounter

This normative notion of the human rights encounter is distinguished from what has been discussed in Chapter 5. There, the human rights encounter is a prototypical encounter between individual and institution, which is rationalized by modern law and human rights discourse. Human rights law is the medium by which conflicts and grievances are expressed in a legally-intelligible manner within this rationalized encounter. As discussed, the legally-rationalized human rights encounter empowers individuals to resist the regulatory power of the institution by enabling the conception and perception of human rights violations that can be attributed to a specific actor, as well as by providing human rights law as the forum for struggle. In short, human rights law facilitates the naming, shaming and claiming of conflicts and grievances.⁴⁵ The problem, however, is the inherent structure of empowerment-disempowerment (including-excluding) of human rights law. From a phenomenological perspective, human rights law remains one "horizon", despite its acclaimed universality.⁴⁶ The phenomenological conception of horizon suggests the reaffirmation of sameness and the inability of transcendence, because the

⁴⁴ Buckley, *supra* note 22.

⁴⁵ William LF Felstiner, Richard L Abel & Austin Sarat, "The Emergence and Transformation of Disputes: Naming, Blaming, Claiming . . ." (1980) 15:3/4 Law Soc Rev 631.

⁴⁶ Lindahl discusses the intentionality of legal ordering as horizontal. This means that law as "scheme of interpretation" anticipates in a general way who ought to do what, where and when and disclose something *as* something*. Hans Lindahl, *Fault Lines of Globalization: Legal Order and the Politics of A-legality* (Oxford, United Kingdom: Oxford University Press, 2013) at 129–130.

horizon is opened up by the subject's sensing and enables the signification of the objects sensed.⁴⁷ From this perspective, the disempowering aspect of human rights law is expressed by streamlining the chaotic experiences of the intersubjective encounter into those which can be made intelligible by human rights law.

This empowerment-disempowerment (including-excluding) structure, as Lindahl argues, is intrinsic to the exercise of legal ordering which is understood as a form of disclosure, or to use Kelsen's term, schemes of interpretation.⁴⁸ Naturally, one way of disclosing something *as* something* closes down other ways of disclosing reality. A more serious and repeated critique of human rights law is that its way of disclosure reinforces the pre-existing power imbalance.⁴⁹ This is seen in the pacification of individuals by making individuals rights-subject dependent on the welfare state as discussed in Chapter 5. The internationalisation of human rights protection only displaces individuals' reliance upon states to reliance upon international institutions, but the passivity of individuals remains.⁵⁰ This critique is linked to the previous point: streamlining the chaotic experience of intersubjective encounter includes the flattening of plural subjectivities to passive and dependent rights-subjects. So, a legally-rationalized human rights encounter has its totalising and extirpating consequences.

There are hence direct contradictions between the normative notion of the human rights encounter and the legally-rationalized human rights encounter. The normative notion of the human rights encounter is so because it emphasizes not only that intersubjective encounters and human experiences are chaotic and beyond attempts at totalisation and reduction, but also more importantly, that they should be so and there is a responsibility for preserving the irreducibility of human rights encounters. The normative notion of the human rights encounter, inspired by Levinas and Arendt, serves as a reminder and the source for inspiration for the legally-rationalized human rights encounter. The normative notion of human rights encounter reminds

⁴⁷ This is also why Levinas considers the approaching face of the Other as different from our sensible experience. By opening up a horizon, our sensible experience totalises the object. Levinas, *supra* note 7 at 191; Emmanuel Levinas, *Existence and existents* (The Hague: Nijhoff, 1978) at 47–49.

⁴⁸ Lindahl, *supra* note 46 at 122.

⁴⁹ E.g. Makau Mutua, "Savages, Victims, and Saviors: The Metaphor of Human Rights" (2001) 42 Harv Int Law J 201; Ratna Kapur, *Gender, alterity and human rights: freedom in a fishbowl* (Edward Elgar Publishing, 2018); Jan Klabbers, "Hannah Arendt and the Languages of Global Governance" in Marco Goldoni & Christopher McCorkindale, eds, *Hannah Arendt Law* (Hart Publishing, 2012) 229 at 244.

⁵⁰ Klabbers, *supra* note 49 at 244; Uruña, *supra* note 39 at 113–115.

the latter that the exercise of rationalization has its intrinsic limits and that legal rationalization should be mindful of the material consequences of its exclusion and disempowerment. Because the infinity of the Other and human plurality always surpass thematization, the normative notion inspires the legally-rationalized human rights encounter to renew the concepts and language used in the legal rationalization. The renewal does not change the fact that legal ordering operates the inclusion-exclusion structure but destabilizes it.

Again, as emphasized in Chapter 5, the structure of legal rationalization is a dilemma: it is not because the legally-rationalized human rights encounter reinforces and legitimizes existing power imbalances that it should be discarded; rather, the question is how to enact its empowering side. The answer seems to be a constant effort of questioning and renewing the boundaries⁵¹ laid out by legal rationalization, for example, the boundaries of the victim status laid out by human rights law (recall the discussion in Chapter 1). Each time when an individual addresses an institution and makes strange and idiosyncratic claims that do not fit into extant legal conceptions of human rights, the extant human rights law should not avoid encountering these claims, but engage with them and, in the process, question its own boundaries, practicing the phenomenological way of, “seeing things in themselves”.⁵² The engagement is motivated by this premise as Lindahl puts it, that it is not that nothing human is alien, but that the alien is human.⁵³

An example in the context of surveillance would be a claim by an individual for the absolute transparency of the state. In making such a claim, an individual would deny that a national security clause can be a justifiable ground for not disclosing certain intelligence materials. This claim would be alien to human rights law because it defies basic ideas about the legitimacy of the state’s monopoly on violence to preserve its own existence, which human rights law largely accepts. But, if taken seriously, the claim could disturb existing human rights law in several fundamental and productive ways. As a foundational question, the claim pushes us (those who make the claim, those who are confronted by the claim and those who decide the claim) to reflect on human rights law’s embeddedness in and reinforcement of the state-system rather than other forms of political authority. For human rights practices, the claim raises

⁵¹ I adopt Lindahl’s definition of “boundaries” which establish certain persons ought to behave in a certain way in a certain place and at a certain time. Boundaries establish legal orders by way of including and excluding. Lindahl, *supra* note 46 at 1.

⁵² Willis, *supra* note 37.

⁵³ Lindahl, *supra* note 46 at 246–247.

questions regarding the state's margin of appreciation in the context where the radical transparency of individuals is opposed to the radical secrecy of state's surveillance. So far as state surveillance also significantly relies on private entities, the claim also pushes against the protection of IP and trade secret laws, which human rights law normally is silent on.

2. The rule of law inspired by human rights encounter

The previous discussion is closely linked to how to think of the distinction between formal legalism and the thick concept of the rule of law. Formal legalism was discussed in Chapter 5 as one of the main constitutive force of the "pastoral liberalism" that reveals and conceals the policing or surveillance power of the modern state. Whereas Chapter 5 demonstrates the dilemmatic character of pastoral liberalism and the role played by law, in Part II, I criticised formal legalism for impeding rather than facilitating encounters between individuals subjected to digital surveillance and surveillance power. By maintaining secrecy at the core of digital surveillance and its structural exclusion of individual agency and introducing increased bureaucratization to the surveillance apparatus, the dilemma is turned into an opposition by which governing is more tilted to mean the absence of individual empowerment. However, just as I have argued about the idea of human rights encounter, criticising formal legalism for foreclosing the human rights encounter does not mean dismissing the idea of the rule of law. I want to intensify the empowering side of law, and I am motivated by Hildebrandt's argument that "The rule of law is not a necessary truth but a vulnerable historical artefact that needs to be sustained in the face of recurring threats to collapse into either chaos or undivided sovereignty."⁵⁴ The way I understand "sustaining" by reading Levinas' and Arendt's work is that "sustaining" means not building and defending a fortress, but cultivating the vigour that is needed for actualizing human plurality. In this section, I will first pay attention to the historical background of the rule of law and then amplify the rule of law by drawing on Levinas' and Arendt's work.

⁵⁴ Mireille Hildebrandt, "Governance, Governmentality, Police, and Justice: A New Science of Police?" (2008) 56 Buffalo Law Rev 557 at 590.

2.1 Rule of law as a frail historical achievement

E. P. Thompson in *Whigs and Hunters* makes an important distinction between the rule of law and instrumentalised rules. In this book, he examines the adoption of the English Black Act in 1723 and its historical, political and economic conditions. The Black Act, in brief, was one of the cruellest and bloodiest criminal laws in England in the 18th century: under this Act, over 200 petty offences were capital crimes, including killing cattle and cutting down young trees. It was adopted under some overwhelming emergency, and then renewed several times with additional crimes added to it.⁵⁵ It was described that, “[b]oth in its severity and in the loose and wholesale manner of its drafting, the Act was unprecedented. It provided a versatile armoury of death apt to the repression of many forms of social disturbances.”⁵⁶ The political background of the Black Act is extremely murky, but the political ascendancy of Robert Walpole and the Whig Party seems to be key. The economic background includes the land enclosure movement, which rendered many previously publicly or commonly held lands and resources into private properties. The abhorrently disproportionate punishment under the Black Act of the crimes committed against private properties, often mercilessly endorsed and executed by judges, seems to provide a classical example of a law that was an instrument for the ruling class – the owners of the newly propertied lands and resources – to violently protect their class interests.

This remarkable instrumentalisation of law would seem to support the argument that law reinforces and reproduces power imbalance. What is interesting for my purpose is that after detailing the adoption and execution of the law and demonstrating various aspects of the social transformation and power struggle of early capitalist England, Thompson did not land on a simplistic Marxian critique of law being the superstructure of the economic base, merely an instrument of the ruling class. To the contrary, he claimed that despite all the deficits of the Black Act and its implementation, the rule of law itself is, “an unqualified human good”.⁵⁷

The unqualified human good, to be more specific, is that the rule of law, as both formal rules and procedures and as an ideology by its principles of equity and universality, binds the ruling class, despite that law is indeed very often an instrument of the ruling class. The law, in order to be a useful instrument for the rulers, has to be applied to the rulers as well; otherwise,

⁵⁵ E P Thompson, *Whigs and Hunters: Origin of the Black Act* (Penguin Books, 1977) at 206.

⁵⁶ *Ibid* at 191–192.

⁵⁷ *Ibid* at 266.

says Thompson, if the law can simply be “twisted this way and that” by the rulers, there would be no need for law at all. Here, Thompson’s analysis reminds me of Fuller: in Fuller’s story, Rex’s hands were tied by the internal morality of law, and as his law was so badly drafted and implemented, after his death, Rex II abandoned the whole enterprise of law and turned the governmental power to psychiatrists and experts in public relations.⁵⁸ For Fuller too, if the law is simply too bad, it is of no use for the rulers. But Thompson’s interest lies not so much in the internal morality of law as in a class analysis of law’s function. He argues that law not only mediates and reinforces existent class relations, but also legitimizes class power. It is this legitimation of law that is needed by the ruling class and makes the ruling class abide by the law as well, because, “[i]f the law is evidently partial and unjust, then it will mask nothing, legitimize nothing, contribute nothing to any class’s hegemony.” The class hegemony of the 18th century in England is both expressed and legitimized by law, as opposed to military force or theological authority in previous centuries.

Moreover, the unqualified human good of the rule of law is that it makes possible for those ruled to fight for their rights in legal terms and in legal fora. In the case of a law protecting property rights (which is essentially what the Black Act was), the ruled were enabled to express their interests by making property rights claims different from those of the ruling class and to fight for their property rights with the legal weapons from customs or precedents. The odds of winning a case for those who were ruled was not great, but they still had the chance to fight under law, which was impossible under the monarchical absolutism of the 16th century. Here, it seems that Thompson alludes to an understanding of law as constitutive and empowering, but at the same time, he is not starry eyed about the violence of law. That class and social conflicts are fought out under law rather than with arbitrary extra-legal power of both the ruler and the ruled is seen as enormous historical progress. Thompson recognizes that the rule of law would indeed consolidate the ruling power and inhibit revolutionary movements.⁵⁹ He nevertheless, stresses that the paradox in the rule of law makes a big difference and that, “the notion of the regulation and reconciliation of conflicts through the rule of law – and the elaboration of rules and procedures which, on occasion, made some approximate approach towards the ideal – seems to

⁵⁸ Lon L Fuller, *The Morality of Law* (Yale University Press, 1969) at 38.

⁵⁹ Thompson, *supra* note 55 at 265.

me a cultural achievement of universal significance.”⁶⁰ Even in front of the “most sanguinary law”⁶¹ – the Black Act, Thompson is not dismissive of the rule of law. While it is not Thompson’s job as a historian, to proscribe what the rule of law should consist of, it can be argued that the rule of law, at the very least, facilitates the expression of social conflicts rather than forcing such conflicts into uniform obedience.

2.2 Amplifying the rule of law by the Levinasian and Arendtian human rights encounter

Thompson’s remarks on the rule of law can be extrapolated beyond the historical context of the Black Act to form a prescriptive argument about what the rule of law should entail. As I will explain, this argument can find significant support from Levinas’ and Arendt’s work on the human encounter. But just as I have acknowledged at the beginning of Section 1.2 that transposing Levinas’ and Arendt’s works to human rights raises some difficulties, there are similar problems in drawing on Levinas for legal theory. Levinas intensifies the reversal of the self-Other relationship, but he is well aware of the problem of the third party who interrupts a face-to-face encounter. The entry of the third party means that the self cannot be infinitely responsible for one neighbour while being indifferent to another. Levinas calls for justice which, for him, brings back thematization, objectification and calculation, “compare the incomparable”,⁶² for the co-existence of the responsibilities for plural others. The realms of ethics and of law or justice appear to be separate, and, “the entry of law into Levinas’ world seems a lot like the demise of ethics.”⁶³

Unlike in Levinas, law received much more discussion in Arendt’s political theory. One of the main characteristics of the Arendtian view of law is expressed in this quote, “The common dilemma – either the law is absolutely valid and therefore needs for its legitimacy an immortal, divine legislator, or the law is simply a command with nothing behind it but the state’s monopoly of violence – is a delusion.”⁶⁴ This quote reveals a view which fiercely opposes not only the more classic understanding of law as a set of commands only, but also law as objective truth

⁶⁰ *Ibid.*

⁶¹ *Ibid* at 23.

⁶² Cohen, *supra* note 36 at 21.

⁶³ Desmond Manderson, *Proximity, Levinas, and the Soul of Law* (McGill-Queen’s Press - MQUP, 2006) at 181.

⁶⁴ Hannah Arendt, *Crises of the Republic: Lying in Politics, Civil Disobedience on Violence, Thoughts on Politics, and Revolution* (Houghton Mifflin Harcourt, 1972) at 193.

revealed. She then discusses two concepts – *nomos* and *lex*. *Nomos*, as referring to the “wall” of the polis in ancient Greece, suggests law is the stabilizer that makes the political community enduring despite the constant changes of the web of relations by human actions.⁶⁵ But she also recognizes that no boundaries and limitations can reliably withstand the unexpected consequences of human actions and the “onslaught” of new generations.⁶⁶ *Lex* is not about “walls” but “bridges” by which the web of relations is not just established between members of the political community, but extended to strangers and brings strangers together.⁶⁷ It is mutual agreements of multiple strangers, established by the political activities of speech and action, rather than an imperative from a central lawmaker. It seems clear that for Arendt, law is both a result of human action and the condition for humans, in the plural, acting in concert. It is because of the freedom of human beings and the unexpectedness and irreversibility of human action that political and legal mechanisms such as contracts and treaties gain their meaning. These are the mechanisms for promising and forgiving. For Arendt, these mechanisms, as opposed to sovereign domination, take human freedom and the uncertainty of human affairs as they are and create “certain islands of predictability” and “certain guideposts of reliability”.⁶⁸ Hence, law is primarily constitutive rather than imperative, increasing rather than suppressing possibilities and choices for human action and the actualization of human plurality.⁶⁹

While it seems Levinas’ understanding of law is significantly narrower than that of Arendt, there are generative ways to think about law with Levinas. For example, Manderson asks “not, how does law operationalize ethics? but, how does ethics inspire law”.⁷⁰ Levinas’ ethics of alterity informs and unsettles the law and legal reasoning and justice is caught in the paradox of generality, stability and comparability on one hand, and a singular response to a particular situation or person on the other.⁷¹ This ethics of alterity is also discussed by Derrida, namely that in every legal reasoning and judgment, the law is continually suspended and reconstituted and

⁶⁵ Keith Breen, “Law beyond Command? An Evaluation of Arendt’s Understanding of Law” in Marco Goldoni & Christopher McCorkindale, eds, *Hannah Arendt Law* (Oxford; Portland: Hart Publishing, 2012) 15 at 33.

⁶⁶ Arendt, *supra* note 14 at 190–191.

⁶⁷ Arendt relates the Roman *lex* to Montesquieu’s idea of law as rapport subsisting between different entities. Hannah Arendt, *On Revolution* (Penguin Books, 1990) at 188.

⁶⁸ Arendt, *supra* note 14 at 244.

⁶⁹ Massimo La Torre, “Hannah Arendt and the Concept of Law. Against the Tradition” (2013) 99:3 ARSP: Archiv für Rechts- und Sozialphilosophie / Archives for Philosophy of Law and Social Philosophy 400 at 413.

⁷⁰ Manderson, *supra* note 63 at 182.

⁷¹ Sarah E Roberts-Cady, “Rethinking Justice with Levinas” in Desmond Manderson, ed, *Essays Levinas Law Mosaic* (Palgrave Macmillan, 2009) 240 at 253–254.

hence, uncertainties, something incalculable and irreducible to formal rules and established categories are already innate in the mundane operation of law.⁷² Similarly, Simon Critchley connects legal reasoning and judgment to the concept of reduction in Levinas' work. For Levinas, the reduction of "the saying" to "the said" can never be complete and the, "*the reduced Said retains a residue of the unsaid Said within the Saying*". Seeing legal reasoning as related to this concept of reduction, Critchley argues that law oscillates between the saying and the said and is informed and deformed by the experience of anarchic proximity.⁷³ A concept of law inspired by Levinas not only has the ethical register of alterity in its substance, but always contains the ethical element of alterity in the everyday operation and application of law. It seems to me that a Levinasian law that endlessly oscillates between competing responsibilities and an Arendtian law that augments the web of human relations are moving in a very similar direction. A kernel to both is still human spontaneity and hence the infinity of human affairs, which needs law not only to always attend to and be moved by, but also to preserve and nurture.

A prescriptive argument about the rule of law can be strengthened by these discussions in several ways. Thompson's claim of the unqualified human good is actually the paradox of the rule of law, not one-sided empowerment of the ruled nor one-sided legitimisation of the power of the ruling class. The difference that the paradox of the rule of law makes is that, compared with the domination by violence where all individuals are means to an end and, "everything and everybody must fall silent",⁷⁴ the rule of law provides a scheme and initiates the unfolding of conflictual intersubjective encounters within various spatiotemporal conditions. This can be related to Arendt's idea that law is more constitutive than imperative, and that law helps to actualize human plurality. While emphasizing law's constitutive aspect does not mean that law is cleansed of violence,⁷⁵ a Levinasian law is always mindful of law's "mythical" and groundless foundation and hence, its responsibility in deconstructing its determined boundaries.⁷⁶ This call for mindfulness goes to the same point as the discussions in Section 1.3 about the constant renewal of human rights concepts used in the legal rationalization of human rights.

⁷² Jacques Derrida, "The Force of Law: 'The Mystical Foundation of Authority'" (1989) 11 Cardozo Rev 920.

⁷³ Critchley, Simon, "Anarchic Law" in Desmond Manderson, ed, *Essays Levinas Law Mosaic* (Palgrave Macmillan, 2009) 203 at 209–211.

⁷⁴ Arendt, *supra* note 67 at 18.

⁷⁵ Breen, *supra* note 65 at 26–27.

⁷⁶ Derrida, *supra* note 72 at 944–945.

In addition, Levinasian and Arendtian accounts of law help to rethink the formal, “thin conception of the rule of law”. While the formal requirements of law can reinforce the power of the state by creating a legal fortress and fending off annoying encounters (which is the argument made in Chapter 4), both Levinasian and Arendtian accounts of law prescribe that the formal requirements of law do not give law absolute certainty, but should invite the unexpected and disturbances: *e.g.*, the clearer and the more accessible to the public the law is, the more open and more vulnerable it becomes when unexpected situations arise, and the more vulnerable an institution that abides by the rule of law becomes. To re-emphasize, vulnerability is not negative, but a condition that is necessary for the constitution of the self. Hence, we can perhaps rethink Fuller’s internal morality of law as referring to the openness that makes possible the encounter of alterity and makes the law moved by and response-able to such encounter. I will revisit this idea about Fuller’s internal morality of law in Section 3.2. The operation of law that is never settled can be related to Levinas’ discussion about communication. For Levinas, communication is radically different from monologue in the sense that communication does not seek certainty or coincidence with the self. Communication requires the opening of the ego for the Other and this openness is even more important than truthfulness in communication.⁷⁷ From a Levinasian-Arendtian perspective, even the thin conception of the rule of law maintains this dialogical character of law.

3. Normative implications of the loss of the human rights encounter

Having grounded the notion of the human rights encounter in Levinas’ and Arendt’s respective work and rethought the rule of law with Levinas and Arendt, I now move to articulate the normative consequences of the elimination of the human rights encounter in the context of ubiquitous digital surveillance. To recap briefly, throughout this study, I have highlighted two distinct and interrelated aspects of the elimination of the human rights encounter. One is the loss of the human rights encounter in surveillance-based governance. The second aspect is the role of law which not only reacts to but closely intertwines and interacts with the power of policing or surveillance in perpetuating the loss of the human rights encounter. Accordingly, I will go back

⁷⁷ Levinas, *supra* note 2 at 119–120.

to these two aspects and discuss the normative consequences of the loss of the human rights encounter as informed by the previous discussions in Chapter 6.

3.1 Surveillance-based governing

Throughout this study, I have discussed digital surveillance not as the aggregation of certain technical artefacts, but as a central component of decision making and hence of ruling. It involves the installation of surveillance devices and services, the application of data science to datify human behaviour and the living environment, the detection of probabilistic correlations and patterns, and the extraction of actionable knowledge from the collected and processed data to inform decision making in various fields. In Part I, I highlighted the amorphous and covert characteristics of the surveillance apparatus. I also identified the transformation of the form and logic of control that make the experience of a confrontational human rights encounter with the surveillance authorities increasingly difficult. The insights drawn from Levinas and Arendt discussed above seem to form strong and principled arguments against surveillance-based governing as removing the human rights encounter.

In a nutshell, the normative implications of the loss of the human rights encounter would be that it leads to the deprivation of the power and agency of the individual rights-subject to realize and practice his or her rights, as well as the loss of the possibility for the dominant power to come to realize its violence done to others and hence, the avoidance of its human rights responsibilities to others. This is vividly demonstrated in transnational migration management where digital surveillance is widely used by states to expand the scope of their bordering activities. For example, under the Frontex framework, EU member states collect and share among themselves the intelligence obtained by surveillance planes and satellites, and the intelligence is analysed to identify risks and trends in migration flows in the EU's external borders.⁷⁸ With Frontex reports that predict the risks and pressures of irregular migration and with the cooperation of the countries of origin of the migrants under bilateral agreements,⁷⁹ EU

⁷⁸ E.g. Itamar Mann, *Humanity at Sea: Maritime Migration and the Foundations of International Law* (Cambridge: Cambridge University Press, 2016) at 172–174; Nick Vaughan-Williams, “Borderwork beyond Inside/Outside? Frontex, the Citizen–Detective and the War on Terror” (2008) 12:1 *Space Polity* 63.

⁷⁹ E.g. “Friendship Pact” between Italy and Libya on 30 August 2008, see Natalino Ronzitti, “The Treaty on Friendship, Partnership and Cooperation between Italy and Libya: New Prospects for Cooperation in the Mediterranean?” (2009) 1:1 *Bull Ital Polit* 125.

states are able to prevent migrants from reaching their territories or even leaving their countries of origin. Such management effectively avoids human rights encounters where asylum seekers fall in the *de jure* or *de facto* jurisdiction of the EU states.⁸⁰

The loss of the human rights encounter in migration management is facilitated by surveillance technologies. This loss is deeply problematic and has systemically and structurally disempowered the rights-subjects. Of course, this claim about the systematic disempowerment by surveillance is not to deny that people in reality can still remain highly mobile and that the spontaneity in human mobility can exceed the state's far-reaching management such as Frontex. In fact, there is a growing body of literature that develops the "Autonomy of Migration" (AoM) approach to affirm the agency of migrants, arguing that the irregularity of people's escapes disrupts and reshapes the border control of states.⁸¹ In a sense, the AoM approach is not only Foucauldian, emphasizing migrants as a creative force in making new forms of political resistance and reconfiguring the space of borders, but also Levinasian, by underscoring the excesses and irregularities of mobility that always defeat migration control by states.⁸² However, what I want to pay attention to is a kind of trade-off that individuals are forced to make. I therefore ask: what kind of individual agency is exercised by migrants that gives rise to the phenomenon of human spontaneity and irregularity celebrated by the AoM approach? It is the agency to be unregistered, to disappear from the surveillance system, and to escape the migration management.

The observation about the trade-off goes back to the counter-surveillance strategy I mentioned in Chapter 1 by which people provide false information or make themselves anonymous and avoid encounter with the surveillance power. The consequences of avoidance on the part of the rights-subject, however, is that avoidance means foregoing the possibility of demanding protection from the state. It also means the loss of the agency to directly address and

⁸⁰ See *Hirsi Jamaa et al v. Italy*, the first case before the ECtHR dealing with interception on the high seas. The Court found that the migrants were under the, "continuous and exclusive de jure and de facto control of the Italian authorities," and hence Italy bore the human rights obligations vis-à-vis the intercepted migrants. *Hirsi Jamaa and Others v Italy [GC]*, No 27765/09 (23 February 2012) para81.

⁸¹ E.g. Maribel Casas-Cortes, Sebastian Cobarrubias & John Pickles, "Riding Routes and Itinerant Borders: Autonomy of Migration and Border Externalization: Riding Routes and Itinerant Borders" (2015) 47:4 *Antipode* 894; Nick Vaughan-Williams, *Europe's Border Crisis: Biopolitical Security and Beyond* (New York: Oxford University Press, 2015) at 122–123; Nicholas De Genova, ed, *The Borders of "Europe": Autonomy of Migration, Tactics of Bordering* (Duke University Press, 2017).

⁸² Casas-Cortes, Cobarrubias & Pickles, *supra* note 81 at 899.

resist the managerial and totalizing power of the surveillance authority and to demand that this authority acknowledge its violence and fulfil its human rights responsibilities. On the one hand, of course, the agency to escape by going underground is retained and no doubt needs to be duly recognized so that right-subjects are at no point completely passive; but on the other hand, the agency to directly face the managerial power, call it into question, and compel it to take responsibility is lost. This is the most tragic and problematic consequence of the loss of human rights encounter.⁸³

This tragic loss of agency of course goes both ways, as we speak about the inter-subjectivity of encounters. Think of the Levinasian encounter when the face of the Other penetrates the crust of the egoist self, then what if the Other turns away and disappears? Does it mean there is no otherness? The avoidance of the Other could mean that the self is left stuck in its solipsist and totalising loop. The totalising power of the surveillance authority will never encounter its alterity and hence never come to realize its boundaries and limitations and hence, the intrinsic violence in their creation and maintenance. This relates to Husserl's critique of the inauthentic community mentioned earlier and an imperialist form of unity that dictates its will while forgetting about its ground in human plurality and infinity.⁸⁴

The elimination of the human rights encounter is not just about the tactics of hiding and avoiding on the parts of both surveillance authority and the individual. As discussed in Part I, surveillance transforms the logic of ruling by flattening human plurality and infinity. The surveillance-based governance has the all-encompassing power which, rather than exclude, has the potential to account for and absorb all abnormal human behaviour and phenomena for social-sorting, which would feed back into the surveillance apparatus. This all-encompassing power for surveillance-based governance normalizes the alterity and the unexpectedness of human action. Hence, it removes the participatory and conflictual meaning-making and subject-forming processes in the human rights encounter by unilaterally imposing an order of things. Individuals displaying unusual behaviours do not force open the totalizing loop of digital surveillance, but

⁸³ This can be contrasted with an example of a human rights encounter. De Genova documented a self-mobilisation event by encamped migrants at Budapest's Keleti railway station on September 4, 2015 against the denial of access to trains to Austria and Germany by the Hungarian police. The protest was responded to with prompt action by Hungarian authorities to reopen the trains and with confirmation from Austria and Germany that their borders were open. Genova, *supra* note 81 at 11–12.

⁸⁴ Buckley, *supra* note 22 at 15–16.

rather, help to make surveillance-based governing more sophisticated and adaptable, because individual abnormality can be quantified and classified and help algorithms learn.

Hence, surveillance-based governing eliminates the human rights encounter by imposing one single perspective (*i.e.*, technological fundamentalism) on the world by which it creates its own reality. This means that problems such as false positives or false negatives do not negate the utility of surveillance-based governing because these problems can be solved by further perfecting data science and digital technologies. It also means that even when digital surveillance can sometimes reveal unexpected correlations, these unexpected correlations are epistemologically different from Arendt's plurality. To recall, plurality for Arendt is not about "what", *i.e.*, a plurality of properties of objects which are observed from a third-person perspective. Instead, plurality only emerges from the interactions of a plural "who", *i.e.*, when people interact and actualize their uniqueness in being together with others. So, the unexpected correlations detected by digital surveillance are the plurality of "what" rather than the Arendtian, actualized plurality. Arendt's remark on behavioural science can be applied to surveillance-based governing, "[t]he trouble with modern theories of behaviourism is not that they are wrong but that they could become true, that they actually are the best possible conceptualization of certain obvious trends in modern society."⁸⁵ Preserving the human rights encounter, hence, is also about the daunting task of preserving the possibility of escaping the endless, monotonous, self-feeding loop of digital surveillance, escaping, "the deadliest, most sterile passivity".⁸⁶

Furthermore, as I discussed in Part I, the process of producing and making value from data is structurally reserved for a few who control or have access to surveillance technologies. This technologically enclosed process of sense-making and knowledge production can be divorced from human comprehension and deliberation, and hence forms an additional factor of eliminating the human rights encounter in surveillance-based governance.⁸⁷ The technological enclosure has impacts both on regulatory interventions and on individuals. For regulation, when surveillance-based governing results in social harm (for example, a self-driving car kills a pedestrian), political and legal interventions need to rely heavily on expert knowledge, which

⁸⁵ Arendt, *supra* note 14 at 322.

⁸⁶ *Ibid.*

⁸⁷ The unilateral imposition of the reality created by digital surveillance is also closely related to the anti-democratic nature of the big data paradigm, which relies on post-explanatory pragmatics at the expense of human comprehension. Mark Andrejevic, "The Big Data Divide" (2014) 8 Int J Commun 1673.

could enhance the perception of legitimacy of the decision but could also increase the opacity of law and policy-making.⁸⁸ For individual users, technological enclosure undermines individual agency to make informed decisions, which is demonstrated by the problem of “meaningless consent” in commercial surveillance as discussed in Chapters 2 and 3. Once again, Arendt’s warning hits home: “it would be as though our brain, which constitutes the physical, material condition of our thoughts, were unable to follow what we do, so that from now on we would indeed need artificial machines to do our thinking and speaking.”⁸⁹

3.2 Formal legalism

In Chapter 4, I critiqued the current regulatory regimes and initiatives which tend to micromanage surveillance activities and perpetuate the elimination of human rights encounter. I made a larger critique of the role of law in transforming and eliminating the human rights encounter based on an instrumentalist conception of law in Chapter 5. There, I identified the close intertwinement and interaction between the state’s power of policing or surveillance and modern law and their respective transformation of the individual-institutional encounter. I would like to end the inquiry of this study by connecting some open-ended thoughts from Parts I through III and reflecting specifically on this question: how to reconcile the need for certainty of ruling and the ethical demand of human plurality and infinity of law inspired by Levinas and Arendt.

I discussed in Parts I and II that the deployment of surveillance technologies in bureaucratic decision making has been motivated by the perceived objectivity of technology, the need to remove human mistakes and improve decisional transparency. The belief that surveillance technologies help to achieve not only better rulings but also more legitimacy and accountability of rulings because of the alleged objectivity of technology is key. I argue hence that the reintroduction of the human element, reflected for example by creating independent oversight bodies and procedures to tame the surveillance technology and to make the surveillance-based governing accountable seems a circular move. The circularity of the effort does not mean that it is not worth making. But by paying attention to the circularity, I want to

⁸⁸ E.g. Sheila Jasanoff, *Science and Public Reason* (Routledge, 2012).

⁸⁹ Arendt, *supra* note 14 at 3.

stress the potential reinforcement of bureaucratic rationality by the co-consolidation of formal legalism and technological rationalism. To unpack this idea, it is often the case that legal and political decisions resort to scientific-technological proofs for legitimation, although the truthfulness of expert knowledge is a social construct.⁹⁰ Vice versa, decisions relying on surveillance technologies or even automated decisions can claim legitimacy by showing that the process respects all legal requirements. Just recall the discussion in Chapter 4 for thinking about the co-consolidation of formal legalism and technological rationalism. I mentioned there that one of the market responses to the EU GDPR which has laid down comprehensive obligations on data controllers and processors with the real possibility of sanction, is a growing industry for streamlining and automating the GDPR compliance of companies. Instead of asking to what extent the data protection law, as an external control, transforms commercial surveillance activities, perhaps we can also ask to what extent the data protection law is transformed by commercial surveillance. In addition, I discussed privacy by design and privacy by default in the GDPR which are technological measures that data controllers should adopt to ensure data protection. This seems an explicit case where law does not only impose obligations but also delegates its regulatory power to technology. Such delegation does not guarantee better protection of individual rights, and a possible side-effect is an enhanced technological enclosure of commercial data surveillance because privacy by design and privacy by default assume and reinforce the passivity of data subjects.⁹¹ Connecting to the idea of law's constitutive role discussed in Chapter 5, as I speak about the deployment of surveillance as constituting a form of governing, the legal instruments that regulate the design and use of surveillance technologies in public and private administration are an integral part of this new form of governing. The more micromanagement the law does, the more legitimacy the law is likely to give to surveillance-based governing.

The mechanical approach to law's ruling, hence, contributes to reinforcing the decisional legitimacy of the institution. What does this tell us about the values of transparency and accountability of governmental authority and the realization of these values through law? I

⁹⁰ E.g. Jasanoff, *supra* note 88 at 186; Sheila Jasanoff, ed, *States of knowledge: the co-production of science and social order*, International library of sociology (London ; New York: Routledge, 2004).

⁹¹ See discussion in Part II, Chapter 3.3.2 and Chapter 4.2.

would like to propose to rethink Fuller's inner morality of law from a Levinasian-Arendtian perspective.

In Part II, I discussed the requirements under human rights law for the imposition of restrictions on fundamental freedoms. One of the critical requirements is "in accordance of law". This means not simply that domestic legislation should set out legitimate grounds for restricting rights, the measures of restriction (which should fulfil the test of proportionality), the procedures and oversight of the restrictive measure, and provide legal remedies. More importantly, the requirement of "in accordance of law" concerns the quality of the law, that is, the law has to be written in such a fashion that it is accessible, foreseeable and sufficiently clear to the public. While I have argued these requirements should be treated with reasonable scepticism as they tend to be skimmed towards a "management technique" that perpetuates the loss of human rights encounter, they do have significant normative bases. According to Fuller, these formal requirements of having a legal basis and the accessibility and foreseeability of law carry moral values for their own sake.⁹² They constitute the inner morality of law which respects individual agency and justifies the duty of the state's subjects to obey the law.

The contrast between Fuller's and the Levinasian-Arendtian accounts of law is obvious. Fuller's law is based on a reciprocal relationship between the ruler and the ruled: the government operates within and is held accountable by law, and the subjects of the government have the moral obligation of obedience to law. For the latter, especially for a Levinasian account, law is grounded in asymmetrical responsibility for the Other, and for Arendt, although reciprocity seems more pronounced in *lex*, it is not the case for *nomos*,⁹³ and the opening and transcendence of the established boundaries and limitations by human plurality are inevitable and unintentional. A related point is that despite the possibility of having an adversarial relationship between the ruler and the ruled, Fuller's main issue is the conditions and moral basis of the subject's obedience to the state's authority. To flip Fuller's argument, the state can demand the subject's obedience by demonstrating its law fulfils the inner morality criteria. A best possible legal system would remain totalising. The totalisation starts by imposing the state law's interpretation of reality (e.g., deciding what conducts are legal and what are illegal, or, to use Lindahl's words,

⁹² Fuller, *supra* note 58 at 39–40.

⁹³ Lindahl, *supra* note 46 at 238.

opening up “the realm of legal possibilities”⁹⁴), and excluding other interpretive schemes. Relating to the earlier discussions on the human rights encounter, the imposition of the state’s interpretation of reality means that human rights-related conflicts can only be expressed and understood through the extant human rights discourse of the legal community.

However, I think Fuller’s inner morality of law does not have to be based on his reciprocity thesis and it is possible to understand the inner morality of law from a Levinasian-Arendtian perspective. As I discussed in Section 3.2, Fuller’s eight criteria do not just allow for public scrutiny and resistance to the oppressive measures adopted by the state. Inspired by Levinas, the eight criteria already contain the oscillation between determinacy and infinity, between the saying and the said. The requirements of law being general, public and prospective force the law to always respond to unexpected situations and this responsibility is un-reciprocal and unpremeditated. Fuller himself is well-aware of this inevitable indeterminacy and messiness of law and hence distinguishes between a morality of aspiration and a morality of duty. The morality of aspiration means the full realization of human capacity, while the morality of duty is the basic rules without which the enterprise of law is destined to fail.⁹⁵ The inner morality of law includes both the morality of duty and the morality of aspiration. Fuller argues that, save for the requirement of promulgation, the more we try to realize the requirements of inner morality through duties, the more we are likely to fail,

It is easy to assert that the legislator has a moral duty to make his laws clear and understandable. But this remains at best an exhortation unless we are prepared to define the degree of clarity he must attain in order to discharge his duty. The notion of subjecting clarity to quantitative measure presents obvious difficulties...[T]he inner morality of law is condemned to remain largely a morality of aspiration and not of duty. Its primary appeal must be to a sense of trusteeship and to the pride of craftsman.⁹⁶

This seems to me suggesting that the criteria of law, except from promulgation, are inevitably underdetermined and require continued effort of “crafting”. Hence, the inner morality

⁹⁴ *Ibid* at 132.

⁹⁵ Fuller, *supra* note 58 at 5.

⁹⁶ *Ibid* at 43.

of law can be understood as alluding to a Levinasian-Arendtian account of law that constantly renews its conceptions and boundaries as responsibility for human plurality and infinity. And “crafting” should be understood from an Arendtian perspective, which means that it takes collective action rather than “fabrication” by a sovereign will.⁹⁷ Accepting the rule of law as embracing the morality of aspiration would oppose an instrumentalist view of the need for clarity and certainty of law. It would furthermore oppose a mechanical realization of transparency and accountability of the institution through positivist law. Taking the instrumentalist view of clarity and certainty of law to the extreme, surveillance-based governing could arguably be a much better and more rational form of governing than law because of the certainty and clarity inscribed in coding and programming. It then would raise not only epistemological questions about law but also ontological questions about legal institutions.

⁹⁷ Loidolt, *supra* note 18 at 199–200.

Concluding Remarks

This study has investigated the elimination of the human rights encounter in digital surveillance. The investigation moved from being descriptive and explicative to prescriptive. This study has tried to do three things. First and foremost, it embedded the notion of the human rights encounter in Levinas' ethics and Arendt's political theory. In doing so, this study demonstrated the normative implications of the loss of the human rights encounter. Second, this loss of the human rights encounter was discussed as a joint accomplishment of surveillance-based governing and formal legalism. This joint accomplishment was placed in the larger background of modernization and pastoral liberalism. Third, the joint accomplishment allowed me to critique current mainstream problem framing of the challenges posed by digital surveillance. The convergence of human rights protection with the taming of surveillance practices is a manifestation of the proceduralisation of human rights protection. This proceduralization, underpinned by formal legalism and bureaucratic rationalism, reinforces the intrinsic power asymmetries between the surveillance institution and the individual subject to surveillance.

A recurrent theme in this study is the normative importance of appreciating uncertainty and insecurity. As discussed in Chapter 6, uncertainty and insecurity in human relations are constitutive of individual and collective identity. Uncertainty and insecurity are why we need political and legal institutions to organize collective life, but also why these institutions are inevitably insufficient and even violent. Hence, I argued that legal enterprise needs continued crafting. Without appreciating this, we can simply discard our legal and political institutions and replace legal ruling with surveillance-based ruling. Doing so will turn the double-inscription of the Frankenstein myth on its head, which makes law the primary monster to be deposed by surveillance-based ruling. The problem with such replacement is of course not just a power transfer from lawyers to computer scientists, but also more fundamentally the reduction and abstraction of law, human beings and collective life, and exclusion of what is affective, experiential and irrational. Such a reduction has already been discussed by Horkheimer and Adorno: "The actual is validated, knowledge confines itself to repeating it, thought makes itself mere

tautology. The more completely the machinery of thought subjugates existence, the more blindly it is satisfied with reproducing it.”¹

The reduction and abstraction of human beings and collective life, to a great degree, are what law does. As discussed in Chapter 5, modern law and in particular, human rights law, rationalizes individual-institution encounters, subjectivates individuals as rational and formally equal legal subjects, and enables individuals to perceive injustice and grievance in legal terms. But such reduction and abstraction also means excluding other aspects of the human experience and other forms of social struggle. Indeed, law excludes, but by recovering and intensifying law’s root in plural and infinite human encounters, law becomes ambivalent and oscillates between propositional content and anarchic interpretations. Precisely this ambivalence also contains the possibility of emancipation.

I have argued that the current regulatory regimes for digital surveillance, even specifically engaging in human rights protection, lead to more smoke screens, which makes principled challenges against surveillance-based governing more difficult. I have also emphasized dialectical thinking, which sought to revive the possibility of emancipation in human rights and the rule of law. This requires not an acceptance of the linear way of problem framing, not to see law as only reactive and only as an instrument to tame surveillance technologies. Instead, we can try to look for the strange and subversive Other who is already within the ambivalence of law and defeats datafication and reduction by surveillance-based governance. To re-emphasize the idea from Chapter 6, the possibility of emancipation is not a given, but created and tested in such dialectical thinking and practice.

In Chapters 5 and 6, I alluded to such possibilities when formal legal requirements such as legitimate purpose, necessity and proportionality of surveillance measures are not just window dressing but an invitation to highly complex normative discussions. Such discussion, from a Levinasian perspective, does not aim for consensus; rather, truly strange and unintelligible claims are made and heard, which disquiets the pre-existing legal decision-making. Still from a Levinasian perspective, the operation of law which is moved by the strange and unintelligible claims does not appropriate those claims and make them intelligible, but comes to realize its

¹ Theodor W Adorno & Max Horkheimer, *Dialectic of Enlightenment* (Verso, 1997) at 27.

inherent limits and that justice is always yet-to-come and hence, welcomes more such discussion and anarchic human rights encounters. In addition, when these legal requirements become an enabler for the encounter with the Other, human rights subjects are elevated to make human rights claims based on anarchic experiences in human rights encounters. Putting forward strange and unintelligible human rights claims is also performative, rejecting the presumption of empty-vessel-like rights subjects. This actualization of being a rights subject by making strange human rights claims is informed by Arendt's idea of human natality, the bringing of something new as a response to being born in the world.²

I was interested in crypto-anarchist and hacktivist movements for a while. But having been influenced so much by Levinas and Arendt, I think there needs to be more than the decentralization of power and ridding people of states and bureaucrats. More work needs to be done to explore how such possibility of encountering and engaging with the strange Other can be enacted in daily legal practices. This study, by engaging with eclectic theorists and provoking alternative ways of observing and questioning, is, in a sense, a performance of initiating anarchic human encounter, and I hope it forms part of a larger ongoing conversation on actualizing human plurality against surveillance-based governance.

² Hannah Arendt, *The Human Condition* (Chicago: University of Chicago Press, 1958) at 176–177.

Bibliography

Domestic instruments

Domestic legislations

China

Cybersecurity Law of the People's Republic of China, 7 November 2016 [Cybersecurity Law of the People's Republic of China].

UK

Data Retention and Investigatory Powers Act 2014 (UK).

Intelligence Service Act 1994 (UK).

Regulation of Investigatory Power Act 2000 (UK).

Secret Service Act 1989 (UK).

The Investigatory Powers Tribunal Rules 2000, 2000 No 2665, s 6(1).

The Regulation of Investigatory Power (Interception of Communications: Code of Practice) Order 2016, SI 2016/37

Vagrancy Act 1824 (UK), 5 Geo IV, c83.

US

Fair Credit Reporting Act, 15 USC §1681 (1970).

Foreign Intelligence Surveillance Act, 50 USC §1801 (1978).

Governmental reports

UK

Anderson, David. Report of the Bulk Powers Review (Independent Reviewer of Terrorism Legislation, 2016).

Home Office. Interception of Communications Code of Practice, Pursuant to section 71 of the Regulation of Investigatory Powers Act 2000 (London, 2016).

House of Lords, Select Committee on the Constitution. *Surveillance: Citizens and the State* (London: House of Lords, 2009).

Intelligence and Security Committee of Parliament. Privacy and Security: A modern and transparent legal framework (2015).

———. Report on the Draft Investigatory Powers Bill (2016).

US

Bipartisan Policy Center & the Annenberg Public Policy Center of the University of Pennsylvania. *Today's Rising Terrorist Threat and the Danger to the United States: Reflections on the Tenth Anniversary of the 9/11 Commission Report* (2014).

Foreign Intelligence Gathering Laws: Belgium, France, Germany, Portugal, Romania, Netherlands, Sweden, United Kingdom and European Union (The Law Library of Congress).

Office of Oversight and Investigations Majority Staff. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller (Committee on Commerce, Science, and Transportation, 2013).

Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (Federal Trade Commission, 2012).

Ramirez, Edith et al. Data Brokers: A Call for Transparency and Accountability (Federal Trade Commission, 2014).

The White House. "Obama Administration Unveils 'Big Data' Initiative: Announces \$200 Million in New R&D Investments", (29 March 2012), online:
<<https://obamawhitehouse.archives.gov/the-press-office/2015/11/19/release-obama-administration-unveils-big-data-initiative-announces-200>>.

White House Report. "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy" (2012) 4:2 Journal of Privacy and Confidentiality 95.

Domestic cases

UK

Human Rights Watch Inc. et al. v Secretary of State for the Foreign & Commonwealth Office et al. [2016] UKIPTrib15-165-CH.

Liberty and others v GCHQ and others [2014] UKIPTrib 13_77-H.

Rulings of the Tribunal on Preliminary Issues of Law [2003] UKIPTrib 01_62 & 01_77.

The Special Immigration Appeal Commission (Procedure) Rules 2003, 2003 No1034.

US

Clapper v Amnesty International USA, et al, 568 US 398 (2013).

State v. Loomis, 881 NW (2d) 749 (2016).

International instruments

Treaties

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 Jan 1981, ETS No.108 (entered into force 1 Oct 1985).

Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, 213 UNTS 221 art 6 (entered into force 3 September 1953).

International Covenant on Economic, Social and Cultural Rights, 19 December 1966, 993 UNTS 3, art 2(1) (entered into force 3 January 1976).

International Covenant on Civil and Political Rights, 19 December 1966, 999 UNTS 171 art14 (entered into force 23 March 1976).

Statute of the International Atomic Energy Agency, 26 October 1956, 276 UNTS 3 (entered into force 29 July 1957).

Reports and resolutions

Cannataci, Joseph. *Report of the Special Rapporteur on the right to privacy*, 34 Sess, UN Doc A/HRC/35/60 (2017).

General Comment 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 32nd Sess, (1988).

General Comment No.20: Non-discrimination in economic, social and cultural rights (art.2, para.2 of the International Covenant on Economic, Social and Cultural Rights), UNCESCR, 42nd Sess, Agenda Item 3, UN Doc E/C.12/GC/20 (2009).

Kaye, David. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 34 Sess, UN Doc A/HRC/35/22 (2017).

La Rue, Frank. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression*, 17 Sess, UN Doc A/HRC/17/27 (2011).

La Rue, Frank. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 23 Sess, UN Doc A/HRC/23/40 (2013).

Mendel, Toby et al. *Global survey on internet privacy and freedom of expression* (UNESCO, 2012).

Office of the High Commissioner for Human Rights, *The Right to Privacy in the Digital Age: Report of the OHCHR*, UNHRC, 27th Sess, UN Doc A/HRC/27/37 (2014).

Organization of African Unity “Border Disputes among African States.” Resolutions Adopted by the First Ordinary Session of the Assembly of Heads of State and Government Held in Cairo, UAR, from 17 to 21 July 1964, AHG/Res.16(I), available at https://au.int/sites/default/files/decisions/9514-1964_ahg_res_1-24_i_e.pdf.

Philip Alston, *Report of the Special Rapporteur on extreme poverty and human rights*, 73 Sess, UN Doc A/73/396 (2018).

SC Res 1373, UNSC, 2001, UN Doc S/RES/1373.

Scheini, Martin. *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, 13th Sess, UN Doc A/HRC/13/37 (2009).

Schmid, Gerhard. Report on the Existence of A Global System for the Interception of Private and Commercial Communications (ECHELON Interception System) (2001/2098(INI)), A5-0264/2001 (Temporary Committee on the ECHELON Interception System, European Parliament, 2001).

Schwab, Klaus et al. *Personal Data: The Emergence of a New Asset Class* (World Economic Forum, 2011).

The Right to Privacy in the Digital Age, GA Res 68/167, UNGAOR, 68 Sess, UN Doc A/RES/68/167 (2013).

The right to privacy in the digital age, HRC Res 28/16, UNHRC, 28 Sess, UN Doc A/HRC/RES/28/16 (2015).

Voule, Clément Nyaletsossi. *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*, 68 Sess, UN Doc A/HRC/28/24 (2018).

UN Commission on Human Rights, *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, Commission on Human Rights, 41st Sess, UN Doc E/CN.4/1985/4, Annex (28 September 1984).

United Nations Conference on Trade and Development. *World Investment Report 2013: Global Value Chains: Investment and Trade for Development* (UN, 2013).

International cases

Francesco Madafferi v Australia, UN Human Rights Committee, Communication No 1011.2001, UN Doc CCPR/C/81/D/1011/2001 (2004)

Regional instruments

Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision Making and Profiling*, 3 October 2017, WP251rev.01.

———. *Guidelines on the Implementation of the Court of justice of the European Union Judgment on “Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” C-131/12*, 26 November 2014, WP225.

———. *Article 29 Working Party Guidelines on consent under Regulation 2016/679*, 28 November 2017, WP259 rev.01.

Article 29 Data Protection Working Party and Working Party on Police and Justice, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, 1 December 2009, WP 168.

Bigo, Dider et al. *National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges*, Study for the LIBE Committee (Directorate-General for Internal

Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, European Parliament, 2014).

Council of Europe PA, Resolution No 2045, *Mass Surveillance*, 2nd part Sess, Texts Adopted (2015).

Council of Europe, European Commission for Democracy Through Law (Venice Commission), *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*, 102nd Plen Sess, CDL-AD (2015) 006.

European Commission, *Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC [SEC(2005) 1131]*, COM-2005-492 (Brussels, 21 September 2005).

European Commission, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, COM (2017) 10, 2017/0003 (cod) (Brussels, 1 Oct 2017).

European Commission for Democracy Through Law (Venice Commission). *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*, CDL-AD(2015)006 (Venice: Council of Europe, 2015).

EU, *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*, [2016] OJ, L119/1.

EU, *Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, [2016] OJ, L 119/ 89.

Omtzigt, Pieter. *Mass Surveillance*, AS/Jur (2015) 01 (Committee on Legal Affairs and Human Rights, Parliament Assembly of the Council of Europe, 2015).

Regional cases

CJEU

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, [2014] ECLI:EU:C:2014:317.

Maximilliam Schrems v. Data Protection Commissioner, C-362/14, [2015] ECLI:EU:C:2015:650

Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis, Joined Cases C-203/15 and C-698/15, [2016] ECLI:EU:C:2016:970.

Digital Rights Ireland Ltd v. Minister for Communications and Others, Joined Cases C-293/12 and C-594/12, [2014] ECLI:EU:C:2014:238.

ECtHR

Big Brothers Watch and Others v. the United Kingdom, nos.58170/13, 62322/14/14, 24960/15, 13 September 2018.

Chahal v. United Kingdom (1996), Reports of Judgments and Decisions, 1996-V 1853, 23 EHRR 413

Judge Pinto De Albuquerque, Concurring Opinion, *Szabó and Vissy v Hungary*, No 37138/14 (12 January 2016).

Kennedy v the United Kingdom, No 26839/05 (18 May 2010).

Leander v Sweden (1987), 116 ECHR 9Ser A), 9 EHRR 433

Malone v the United Kingdom, No 8691/79 [1984] ECHR10, 7 EHRR 14.

Roman Zakharov v Russisa, No 47143/06 (4 December 2015).

Rotaru v Romania, No 28341/95 [2000] V ECHR109.

S and Marper v the United Kingdom, No 30562/04 [2008] V ECHR 167.

Silver and others v United Kingdom (1983), 61 ECHR (Ser A) 161, 5EHRR347

Szabó and Vissy v Hungary, No 37138/14 (12 January 2016).

10 Human Rights Organisations v the United Kingdom, no.24960/15.

Weber and Saravia v Germany, No 54934/00 [2006] XI ECHR 1173.

Secondary sources

Books

- Arendt, Hannah. *The Human Condition* (Chicago: University of Chicago Press, 1958).
- . *Crises of the Republic: Lying in Politics, Civil Disobedience on Violence, Thoughts on Politics, and Revolution* (Houghton Mifflin Harcourt, 1972).
- . *The Origins of Totalitarianism: New Edition with Added Prefaces* (New York: Harcourt Brace Jovanovich, 1973).
- . *The Life of the Mind: The Groundbreaking Investigation on How We Think* (New York: Harcourt Brace Jovanovich, 1981).
- . *On Revolution* (Penguin Books, 1990).
- Acemoglu, Daron & James A Robinson, *Why Nations Fail: The Origins of Power, Prosperity, and Poverty* (Crown Publishers, 2013).
- Baudrillard, Jean. *The Gulf War Did Not Take Place* (Indiana University Press, 1995).
- Bauman, Zygmunt. *Modernity and the Holocaust*, repr ed (Cambridge: Polity Press, 1989).
- Bogard, William. *The Simulation of Surveillance: Hypercontrol in Telematic Societies* (Cambridge University Press, 1996).
- Brandeis, Louis D. *Other People's Money and How the Bankers Use It* (New York: Cosimo, Inc., 2009).
- Breen, Keith. *Under Weber's Shadow: Modernity, Subjectivity and Politics in Habermas, Arendt and MacIntyre* (Farnham, Surrey, England; Burlington, VT: Ashgate, 2012).
- Burchell, Graham, Colin Gordon & Peter Miller, eds. *The Foucault Effect: Studies in Governmentality* (University of Chicago Press, 1991).
- Chamayou, Grégoire. *Manhunts: A Philosophical History*, translated by Steven Rendall (Princeton University Press, 2012).
- Charlesworth, Hilary & Christine Chinkin. *The Boundaries of International Law: A feminist analysis* (Manchester: Manchester University Press, 2000).
- Cohen, Richard A. *Face to face with Levinas* (Albany, N.Y.: State University of New York Press, 1986).

Confucian Analects, the Great Learning, and the Doctrine of the Mean, translated by James Legge (Hong Kong: Lane, Crawford & Company, 1861).

Dobb, Maurice. *Studies in the development of capitalism* (International Publishers, 1964).

Dubber, Markus Dirk & Mariana Valverde, eds. *The New Police Science: The Police Power in Domestic and International Governance* (Stanford University Press, 2006).

———, eds. *Police and the Liberal State* (Stanford University Press, 2008).

Dworkin, Ronald. *Law's Empire* (Harvard University Press, 1986).

EU Agency for Fundamental Rights and Council of Europe. *Handbook on European data protection law*, 2018 edition ed (Luxembourg: Publications Office of the EU, 2018).

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*, translated by Alan Sheridan (New York: Vintage Books, 1995).

———. *Security, Territory, Population: Lectures at the Collège de France, 1977-1978*, translated by Graham Burchell, Michel Senellart, François Ewald & Alessandro Fontana, eds. (Basingstoke; New York: Palgrave Macmillan: République Française, 2007).

———. *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977*, 1st American ed, Colin Gordon, ed. (New York: Pantheon Books, 1980)

Fuller, Lon L. *The Morality of Law* (Yale University Press, 1969).

Galligan, D J. *Due Process and Fair Procedures: A Study of Administrative Procedures* (Oxford University Press, 1997).

Gates, Bill, Nathan Myhrvold & Peter Rinearson. *The Road Ahead* (New York: Penguin Books, 1996).

Genova, Nicholas De, ed. *The Borders of "Europe": Autonomy of Migration, Tactics of Bordering* (Duke University Press, 2017).

Gerards, Janneke & Eva Brems. *Procedural Review in European Fundamental Rights Cases* (Cambridge University Press, 2017).

Gibbs, Robert. *Correlations in Rosenzweig and Levinas* (Princeton, N.J: Princeton University Press, 1992).

Golder, Ben & Peter Fitzpatrick, eds. *Foucault and law* (London: Routledge, 2016).

Habermas, Jürgen. *The Theory of Communicative Action: Volume 2: Lifeworld and System: A Critique of Functionalist Reason* (Boston: Beacon Press, 1987).

Haraway, Donna. "A Manifesto for Cyborgs: Science, Technology, and Socialist-Feminism in the 1980s" (1985).

Harris, Andrew Todd. *Policing the City: Crime and Legal Authority in London, 1780-1840* (Ohio State University Press, 2004).

Heisler, Helmuth, ed. *Foundations of Social Administration* (London and Basingstoke: Macmillan Press LTD, 1977).

Hildebrandt, Mireille. *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing, 2015).

Hunt, Alan & Gary Wickham. *Foucault and Law: Towards a Sociology of Law as Governance* (Pluto Press, 1994).

Ihde, Don. *Experimental Phenomenology: Multistabilities*, 2nd ed (Albany: State University of New York Press, 2012).

———. *Technics and praxis*, Boston studies in the philosophy of science 24 (Dordrecht: Reidel, 1979).

———. *Technology and the Lifeworld: from Garden to Earth* (Indiana University Press, 1990).

Indaimo, J A. *The Self, Ethics and Human Rights: Lacan, Levinas & Alterity* (Abingdon, New York: Routledge, 2015).

Jasanoff, Sheila, ed. *States of knowledge: the co-production of science and social order*, International library of sociology (London ; New York: Routledge, 2004).

———. *Science and Public Reason* (Routledge, 2012).

Johns, Fleur. *Non-Legality in International Law: Unruly Law* (Cambridge University Press, 2013).

Kapur, Ratna. *Gender, alterity and human rights: freedom in a fishbowl* (Edward Elgar Publishing, 2018).

Levinas, Emmanuel. *Alterity & transcendence* (Linton: Athlone, 1999).

———. *Ethics and infinity: Conversations with Philippe Nemo*, 1st ed, translated by Richard A. Cohen (Pittsburgh: Duquesne University Press, 1985).

———. *Existence and existents* (The Hague: Nijhoff, 1978).

———. *Otherwise Than Being or Beyond Essence*, translated by Alphonso Lingis (Martinus Nijhoff, 1981).

———. *Totality and Infinity: An Essay on Exteriority*, translated by Alphonso Lingis (Pittsburgh: Duquesne University Press, 2007).

Lévinas, Emmanuel & Seán Hand. *The Levinas reader*, Blackwell readers (B. Blackwell, 1989).

Lindahl, Hans. *Fault Lines of Globalization: Legal Order and the Politics of A-legality* (Oxford, United Kingdom: Oxford University Press, 2013).

Loidolt, Sophie. *Phenomenology of Plurality: Hannah Arendt on Political Intersubjectivity*, Routledge research in phenomenology 7 (New York: Routledge, Taylor & Francis Group, 2018).

Lorch, Robert Stuart. *Democratic Process and Administrative Law* (Wayne State University Press, 1969).

Lukes, Steven. *Moral Conflict and Politics* (Oxford: Clarendon Press, 1991).

Lyon, David. *The Culture of Surveillance: Watching as a Way of Life* (John Wiley & Sons, 2018).

MacCormick, Neil. *Legal Reasoning and Legal Theory* (Clarendon Press, 1994).

Manderson, Desmond. *Proximity, Levinas, and the Soul of Law* (McGill-Queen's Press - MQUP, 2006).

Mann, Itamar. *Humanity at Sea: Maritime Migration and the Foundations of International Law* (Cambridge: Cambridge University Press, 2016).

Martire, Jacopo. *A Foucauldian Interpretation of Modern Law: From Sovereignty to Normalisation and Beyond* (Edinburgh: Edinburgh University Press, 2017).

Marx, Karl. *The Eighteenth Brumaire of Louis Bonaparte* (New York: International Publishers, 1969).

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*, 1st ed (Cambridge University Press, 2018).

Mayer-Schönberger, Viktor & Kenneth Cukier. *Big Data: A Revolution that Will Transform how We Live, Work, and Think* (Houghton Mifflin Harcourt, 2013).

Orwell, George. *The Collected Essays, Journalism and Letters of George Orwell: In front of your nose, 1945-1950* (Secker & Warburg, 1968).

Pasquale, Frank. *The black box society: the secret algorithms that control money and information* (Cambridge: Harvard University Press, 2015).

Pugliese, Joseph. *State Violence and the Execution of Law: Biopolitical Caesurae of Torture, Black Sites, Drones* (Routledge, 2013).

John Rawls, *A Theory of Justice*, revised edition ed (Cambridge, Mass: Harvard University Press, 2009).

Richelson, Jeffrey. *The US Intelligence Community*, 7th edition ed (Boulder: Westview Press, 2016).

Scarry, Elaine. *The Body in Pain: The Making and Unmaking of the World* (Oxford University Press, 1987).

Schmitt, Carl. *Political Theology: Four Chapters on the Concept of Sovereignty* (University of Chicago Press, 2010).

Shapiro, Carl & Hal Varian. *Information Rules: A Strategic Guide to the Network Economy* (Harvard Business Press, 1998).

Smith, Adam. *Lectures on Jurisprudence*, R. L. Meek, D. D. Raphael & P. G. Stein, eds. (Liberty Fund, 1982).

Streeck, Wolfgang. *Buying Time: The Delayed Crisis of Democratic Capitalism* (Verso, 2014).

Supiot, Alain. *Governance by numbers: the making of a legal model of allegiance*, translated by Saskia Brown (Oxford; Portland: Hart Publishing, 2017).

Svendsen, Adam DM. *Intelligence Cooperation and the War on Terror: Anglo-American Security Relations after 9/11* (New York: Routledge, 2009).

———. *Understanding the Globalization of Intelligence* (London/Basingstoke: Palgrave Macmillan, 2012).

Thaler, Richard H. *Nudge: Improving Decisions about Health, Wealth and Happiness* (Yale University Press, 2008).

Thompson, E P. *Whigs and Hunters: Origin of the Black Act* (Penguin Books, 1977).

Tranberg, Pernille & Steffan Heuer. *Fake It: Your Online Identity Is Worth Gold. Guide to Digital Self Defense* (Art People, 2012).

Tucker, Robert, ed. *The Marx-Engels Reader* (New York: Norton & Company, 1978).

Unger, Roberto Mangabeira. *Free Trade Reimagined: The World Division of Labor and the Method of Economics* (Princeton University Press, 2007).

Urueña, René. *No Citizens Here: Global Subjects and Participation in International Law* (Martinus Nijhoff, 2012).

Vaidhyathan, Siva. *The Googlization of Everything: (And Why We Should Worry)* (University of California Press, 2012).

Valverde, Mariana. *Chronotopes of Law* (Routledge, 2015).

Vaughan-Williams, Nick. *Europe's Border Crisis: Biopolitical Security and Beyond* (New York: Oxford University Press, 2015).

Verbeek, Peter-Paul. *Moralizing technology: understanding and designing the morality of things* (Chicago; London: The University of Chicago Press, 2011).

Wu, Tim. *The Master Switch: The Rise and Fall of Information Empires* (Knopf Doubleday Publishing Group, 2010).

———. *The Attention Merchants: The Epic Scramble to Get Inside Our Heads* (Knopf Doubleday Publishing Group, 2017).

Zikopoulos, Paul et al. *Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data* (McGraw-Hill, 2011).

Žižek, Slavoj. *The Courage of Hopelessness: Chronicles of a Year of Acting Dangerously* (Penguin UK, 2017).

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).

Articles and book chapters

Ananny, Mike & Kate Crawford. "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability" (2018) 20:3 *New Media & Society* 973.

Andrejevic, Mark. "Surveillance in the Digital Enclosure" (2007) 10:4 *Commun Rev* 295.

———. "The Big Data Divide" (2014) 8 *Int J Commun* 1673.

Arnardóttir, Oddný Mjöll. "The 'procedural turn' under the European Convention on Human Rights and presumptions of Convention compliance" (2017) 15:1 *Int J Const Law* 9.

Asad, Asad L & Eva Rosen. "Hiding within racial hierarchies: how undocumented immigrants make residential decisions in an American city" (2018) *J Ethn Migr Stud*, online: <<https://doi.org/10.1080/1369183X.2018.1532787>>.

Bantwal Rao, Mithun et al. "Technological Mediation and Power: Postphenomenology, Critical Theory, and Autonomist Marxism" (2015) 28:3 *Philos Technol* 449.

Beetham, David. "Market economy and democratic polity: Democratization" (1997) 4:1 Democratization 76.

Benvenisti, Eyal. "Upholding Democracy Amid the Challenges of New Technology: What Role for the Law of Global Governance?" (2018) 29:1 Eur J Int Law 9.

Bovens, Mark & Stavros Zouridis. "From Street-Level to System-Level Bureaucracies: How Information and Communication Technology is Transforming Administrative Discretion and Constitutional Control" (2002) 62:2 Public Adm Rev 174.

Breen, Keith. "Law beyond Command? An Evaluation of Arendt's Understanding of Law" in Marco Goldoni & Christopher McCorkindale, eds, *Hannah Arendt Law* (Oxford; Portland: Hart Publishing, 2012) 15.

boyd, danah & Kate Crawford. "Critical Questions for Big Data: Provocations for a cultural, technological, and scholarly phenomenon" (2012) 15:5 Inf Commun Soc 662.

Brakel, Rosamunde van & Paul De Hert. "Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies" (2011) 20:3 J Police Stud 163.

Branch, Jordan. "Mapping the sovereign state: Technology, authority, and systemic change" (2011) 65:1 Int Organ 1;

Brin, Sergey & Lawrence Page. "The Anatomy of A Large-Scale Hypertextual Web Search Engine" (1998) 30:1-7 Comput Netw ISDN Syst 107.

Buckley, Philip. "Phenomenology as Soteriology: Husserl and the call for 'Erneuerung' in the 1920s" (2019) 35:1 Mod Theol 5.

Casas-Cortes, Maribel, Sebastian Cobarrubias & John Pickles. "Riding Routes and Itinerant Borders: Autonomy of Migration and Border Externalization: Riding Routes and Itinerant Borders" (2015) 47:4 Antipode 894.

Chesterman, Simon. "Intelligence Cooperation in International Operations: Peacekeeping, Weapons Inspections, and the Apprehension and Prosecution of War Criminals" in Hans Born, Ian Leigh & Aidan Wills, eds, *Int Intell Coop Account* (Routledge, 2011) 124.

Citron, Danielle Keats. "Technological Due Process" (2008) 85:6 Wash Univ Law Rev 1249.

Cohen, Julie E. "What Privacy is For" (2013) 126 Harv Law Rev 1904.

Crain, Matthew. "The limits of transparency: Data brokers and commodification" (2018) 20:1 New Media Soc 88.

Crawford, Kate & Jason Schultz. "Big data and due process: Toward a framework to redress predictive privacy harms" (2014) 55 BCL Rev 93.

Critchley, Simon. "Anarchic Law" in Desmond Manderson, ed, *Essays Levinas Law Mosaic* (Palgrave Macmillan, 2009) 203.

Dean, Mitchell. "Military Intervention as 'Police' Action?" in Markus Dirk Dubber & Mariana Valverde, eds, *New Police Sci* (Stanford University Press, 2006) 185.

Deleuze, Gilles. "Postscript on the Societies of Control" (1992) 59 October 3.

Derrida, Jacques. "The Force of Law: 'The Mystical Foundation of Authority'" (1989) 11 Cardozo Rev 920.

Dencik, Lina, Arne Hintz & Jonathan Cable. "Towards data justice? The ambiguity of anti-surveillance resistance in political activism" (2016) 3:2 Big Data Soc 1.

Diggelmann, Oliver & Maria Nicole Cleis. "How the Right to Privacy Became a Human Right" (2014) 14:3 Human Rights Law Review 441.

Dubois, Vincent, Morgane Paris & Pierre-Edouard Weill. "Targeting by Numbers. The Uses of Statistics for Monitoring French Welfare Benefit Recipients" in Lorenzo Barrault-Stella & Pierre-Edouard Weill, eds, *Creat Target Publics Welf Policies Comp Multi-Level Approach, Logic, Argumentation & Reasoning* (Cham: Springer International Publishing, 2018) 93.

Dusza, Karl. "Max Weber's Conception of the State" (1989) 3:1 Int J Polit Cult Soc 71.

Edwards, Lilian & Michael Veale. "Slave to the Algorithm? Why a 'Right to Explanation' Is Probably Not the Remedy You Are Looking For" (2017) 16:1 Duke Law Technol Rev 19.

Engle, Karen. "International Human Rights and Feminism: When Discourses Meet" (1992) 13:3 Mich J Int Law 517.

Ferguson, Andrew Guthrie. "Big Data and Predictive Reasonable Suspicion" (2015) 163:2 University of Pennsylvania Law Review 327.

Felstiner, William LF, Richard L Abel & Austin Sarat, "The Emergence and Transformation of Disputes: Naming, Blaming, Claiming . . ." (1980) 15:3/4 Law Soc Rev 631.

Foucault, Michel. "The Subject and Power" (1982) 8:4 Crit Inq 777.

Galbraith, Jay R. "Organizational Design Challenges Resulting From Big Data" (2014) 3:1 J Organ Des 2.

Galetta, Antonella. "The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?" (2013) 4:2 European Journal of Law and Technology, online: <<http://ejlt.org/article/view/221>>.

Gordon, Colin. "The Soul of the Citizen: Max Weber and Michel Foucault on Rationality and Government" in Sam Whimster & Scott Lash, eds, *Max Weber Ration Mod* (293-316: Routledge, 2006).

Hamilton, Melissa. "Adventures in Risk: Predicting Violent and Sexual Recidivism in Sentencing Law" (2015) 47:1 *Ariz State Law J* 1.

Hardin, Russell. "The Morality of Law and Economics" 11:4 *Law Philos* 331.

Helfer, L R. "Redesigning the European Court of Human Rights: Embeddedness as a Deep Structural Principle of the European Human Rights Regime" (2008) 19:1 *Eur J Int Law* 125.

Hildebrandt, Mireille. "Governance, Governmentality, Police, and Justice: A New Science of Police?" (2008) 56 *Buffalo Law Rev* 557.

———. "Profiling and the rule of law" (2008) 1:1 *Identity Inf Soc* 55.

———. "Who is Profiling Who? Invisible Visibility" in Serge Gutwirth et al, eds, *Reinventing Data Prot* (Springer, Dordrecht, 2009) 239.

Hirsch, Dennis D. "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?" 34 *Seattle University Law Review* 439.

Hyatt, Jordan & Steven L Chanenson. "The Use of Risk Assessment at Sentencing: Implications for Research and Policy" (2016) Villanova LawPublic Policy Res Pap No2017-1040.

Jacobs, Adam. "The pathologies of big data" (2009) 52:8 *Commun ACM* 36.

Jasanoff, Sheila. "Virtual, visible, and actionable: Data assemblages and the sightlines of justice" (2017) 4:2 *Big Data Soc* 1.

Jasserand, Catherine. "Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?" (2018) 34:1 *Computer Law & Security Review* 154.

Joergensen, Rikke Frank. "The unbearable lightness of user consent" (2014) 3:4 *Internet Policy Rev* 1.

Johns, Fleur. "Global governance through the pairing of list and algorithm" (2016) 34:1 *Environ Plan Soc Space* 126.

Kapur, Ratna. "Precarious desires and ungrievable lives: human rights and postcolonial critiques of legal justice" (2015) 3:2 *Lond Rev Int Law* 267.

Klabbers, Jan. "Hannah Arendt and the Languages of Global Governance" in Marco Goldoni & Christopher McCorkindale, eds, *Hannah Arendt Law* (Hart Publishing, 2012) 229.

———. “Possible Islands of Predictability: The Legal Thought of Hannah Arendt” (2007) 20:01 Leiden J Int Law 1.

Kleinlein, Thomas. “Consensus and Contestability: The ECtHR and the Combined Potential of European Consensus and Procedural Rationality Control” (2017) 28:3 Eur J Int Law 871.

———. “The Procedural Approach of the European Court of Human Rights: Between Subsidiarity and Dynamic Evolution” (2019) 68:1 International & Comparative Law Quarterly

Knox, John H. “Horizontal Human Rights Law” (2008) 102:1 Am J Int Law 1.

Kramer, Matthew H. “Questions Raised and Questions Begged: Some Doubts about Ronald Dworkin’s Approach to Law-and-Economics” (1993) 6:01 Can J Law Jurisprud 139.

Kroll, Joshua A et al. “Accountable algorithms” (2017) 165:3 Univ Pa Law Rev 633.

Laperdrix, Pierre, Walter Rudametkin & Benoit Baudry. *Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints* (San Jose, CA: IEEE, 2016).

Latour, Bruno. “On Technical Mediation: Philosophy, Sociology, Genealogy” (1994) 3 Common Knowl 29.

Maglione, Giuseppe. “Embodied Victims: An Archaeology of the ‘Ideal Victim’ of Restorative Justice” (2017) 17:4 Criminol Crim Justice 401.

Malgieri, Gianclaudio & Giovanni Comandé. “Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation” (2017) 7:4 International Data Privacy Law 243.

Malleson, Nick & Martin A Andresen. “The impact of using social media data in crime rate calculations: shifting hot spots and changing spatial patterns” (2015) 42:2 Cartogr Geogr Inf Sci 112.

Manokha, Ivan. “Foucault’s Concept of Power and the Global Discourse of Human Rights” (2009) 23:4 Glob Soc 429.

Mégret, Frédéric. “The Humanitarian Problem with Drones” (2013) 2013:5 Utah Law Rev 1283.

———. “An International Law Theory of Inherently Governmental Functions” (2019), unpublished manuscript.

Mendoza, Isak & Lee A Bygrave. “The Right Not to be Subject to Automated Decisions Based on Profiling” in Tatiana-Eleni Synodinou et al, eds, *EU Internet Law: Regulation and Enforcement* (Springer International Publishing, 2017) 77.

Moses, Lyria B, Fleur Johns & Daniel Joyce. "Data associations in global law and policy" (2018) 5:1 Big Data Soc 1.

Moses, Lyria Bennett & Janet Chan. "Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools" 37:2 UNSW Law J 643.

Mutua, Makau. "Savages, Victims, and Saviors: The Metaphor of Human Rights" (2001) 42 Harv Int Law J 201.

Neocleous, Mark. "Theoretical Foundations of the 'New Police Science'" in Markus Dirk Dubber & Mariana Valverde, eds, *New Police Sci* (Stanford University Press, 2006) 17.

Nissenbaum, Helen. "A Contextual Approach to Privacy Online" (2011) 140:4 Daedalus 32.

Olsen, Niklas. *The Sovereign Consumer: A New Intellectual History of Neoliberalism* (Palgrave Macmillan, 2019).

Oosterloo, Serena & Gerwin van Schie. "The Politics and Biases of the 'Crime Anticipation System' of the Dutch Police" 12.

Peeters, Rik & Marc Schuilenburg. "Machine justice: Governing security through the bureaucracy of algorithms" (2018) 23:3 Inf Polity Int J Gov Democr Inf Age 267.

Purtova, Nadezhda. "The law of everything. Broad concept of personal data and future of EU data protection law" (2018) 10:1 Law, Innovation and Technology 40.

Randeria, Shalini. "Cunning States and Unaccountable International Institutions: Legal Plurality, Social Movements and Rights of Local Communities to Common Property Resources" (2003) 44:1 Eur J Sociol 27.

Rajkovic, Nikolas M. "The Visual Conquest of International Law: Brute Boundaries, the Map, and the Legacy of Cartogenesis" (2018) Leiden J Int Law 1.

Raz, Joseph. "Rule of Law and its Virtue" in *The Authority of Law: Essays on Law and Morality* (Oxford: Clarendon Press, 1979).

Roberts-Cady, Sarah E. "Rethinking Justice with Levinas" in Desmond Manderson, ed, *Essays Levinas Law Mosaic* (Palgrave Macmillan, 2009) 240.

Ronzitti, Natalino. "The Treaty on Friendship, Partnership and Cooperation between Italy and Libya: New Prospects for Cooperation in the Mediterranean?" (2009) 1:1 Bull Ital Polit 125.

Rouvroy, Antoinette & Yves Poullet. "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy" in Serge Gutwirth et al, eds, *Reinventing Data Prot* (Dordrecht: Springer Netherlands, 2009) 45.

Scheper, Christian. “‘From naming and shaming to knowing and showing’: human rights and the power of corporate practice” (2015) 19:6 *The International Journal of Human Rights* 737.

Schwöbel-Patel, Christine. “Spectacle in International Criminal Law: the Fundraising Image of Victimhood” (2016) 4:2 *Lond Rev Int Law* 247.

———. “Nils Christie’s ‘Ideal Victim’ Applied: From Lions to Swarms”, (5 August 2015), online: Crit Leg Think <<http://criticallegalthinking.com/2015/08/05/nils-christies-ideal-victim-applied-from-lions-to-swarms/>>.

Selbst, Andrew D & Julia Powles. “Meaningful information and the right to explanation” (2017) 7:4 *International Data Privacy Law* 233.

Shear, Michael D & Julie Hirschfeld Davis. “Trump Moves to End DACA and Calls on Congress to Act”, *N Y Times* (20 January 2018), online: <<https://www.nytimes.com/2017/09/05/us/politics/trump-daca-dreamers-immigration.html>>.

Thatcher, Jim, David O’Sullivan & Dillon Mahmoudi. “Data colonialism through accumulation by dispossession: New metaphors for daily data” (2016) 34:6 *Environ Plan Soc Space* 990.

Torre, Massimo La. “Hannah Arendt and the Concept of Law. Against the Tradition” (2013) 99:3 *ARSP Arch Für Rechts- Sozialphilosophie Arch Philos Law Soc Philos* 400.

Tranter, Kieran. “Nomology, Ontology, and Phenomenology of Law and Technology” (2007) 8:2 *Minn J Law Sci Technol* 449.

Turing, A M. “Computing Machinery and Intelligence” (1950) 59:236 *Mind New Ser* 433.

Vaughan-Williams, Nick. “Borderwork beyond Inside/Outside? Frontex, the Citizen–Detective and the War on Terror” (2008) 12:1 *Space Polity* 63.

Vedder, Anton. “KDD: The challenge to individualism” (1999) 1:4 *Ethics Inf Technol* 275 at 277

Wachter, Sandra, Brent Mittelstadt & Luciano Floridi. “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation” (2017) 7:2 *International Data Privacy Law* 76.

Waldron, Jeremy. “The Concept and the Rule of Law” (2008) 43:1 *Ga Law Rev* 1.

Weiler, Joseph HH. “The geology of international law–governance, democracy and legitimacy” (2004) 64:3 *Z Für Ausländisches Öffentl Recht Völkerr* 547.

Williams, Matthew L, Pete Burnap & Luke Sloan. “Crime Sensing With Big Data: The Affordances and Limitations of Using Open-source Communications to Estimate Crime Patterns” (2017) 57:2 *Br J Criminol* 320.

Wills, Aidan & Hans Born. "International Intelligence Cooperation and Accountability: Formidable Challenges and Imperfect Solutions" in Hans Born, Ian Leigh & Aidan Wills, eds, *Int Intell Coop Account* (Routledge, 2011) 277.

Willis, Peter. "The 'Things Themselves' in Phenomenology" (2001) 1:1 *Indo-Pac J Phenomenol* 1.

Wright, David, David Barnard-Wills & Inga Kroener. *Deliverable 4: Findings and recommendations* (PHAEDRA, 2015).

Yannopoulos, Angelos, Vassiliki Andronikou & Theodora Varvarigou. "Behavioural Biometric Profiling and Ambient Intelligence" in Mireille Hildebrandt & Serge Gutwirth, eds, *Profiling Eur Citiz* (Dordrecht: Springer Netherlands, 2008) 89.

Yeung, Karen. "'Hypernudge': Big Data as a mode of regulation by design" (2017) 20:1 *Inf Commun Soc* 118.

Zahavi, Dan. "Beyond Empathy: Phenomenological Approaches to Intersubjectivity" 8:5–7 *J Conscious Stud* 151.

Zegart, Amy B. "The Domestic Politics of Irrational Intelligence Oversight" (2011) 126:1 *Political Science Quarterly* 1.

Zuboff, Shoshana. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization" (2015) 30:1 *J Inf Technol* 75.

News and media reports

Anderson, Chris. "The End of Theory: The Data Deluge Makes the Scientific Method Obsolete", (23 June 2008), online: WIRED <<https://www.wired.com/2008/06/pb-theory/>>.

Angwin, Julia. "Google faces new privacy probes", *The Wall Street Journal* (16 March 2012), online: <<https://www.wsj.com/articles/SB10001424052702304692804577283821586827892>>.

Angwin, Julia et al. "Machine Bias", (23 May 2016), online: ProPublica <<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>>.

"Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine", (18 July 2018), online: *European Commission - Press release* <http://europa.eu/rapid/press-release_IP-18-4581_en.htm>.

Arthur, Charles. "Google facing legal threat from six European countries over privacy", *The Guardian* (2 April 2013), online:

<<https://www.theguardian.com/technology/2013/apr/02/google-privacy-policy-legal-threat-europe>>.

Bachman, Katy. “Senate Commerce Report Says Data Brokers ‘Operate Behind a Veil of Secrecy’”, (18 December 2013), online: Adweek <<https://www.adweek.com/digital/senate-commerce-report-says-data-brokers-operate-behind-veil-secrecy-154579/>>.

Binns, Reuben et al. “It’s Reducing a Human Being to a Percentage”: Perceptions of Justice in Algorithmic Decisions (ACM Press, 2018).

Bullock, Tom. “Big Data And Bad Cops: Can An Algorithm Predict Police Misconduct? (Part 2)”, (24 August 2016), online: WFAE <<https://www.wfae.org/post/big-data-and-bad-cops-can-algorithm-predict-police-misconduct-part-2>>.

“Bundeskartellamt prohibits Facebook from combining user data from different sources”, (7 February 2019), online: *Bundeskartellamt* <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html>.

CNBC. “Dianne Feinstein reveals FBI paid 900000 to hack into killers iphone”, (5 May 2017), online: <<https://www.cnn.com/2017/05/05/dianne-feinstein-reveals-fbi-paid-900000-to-hack-into-killers-iphone.html>>.

Dallke, Jim. “Chicago Police Sued Over ‘Heat List’ Algorithm by Journalists”, (8 June 2017), online: *American Inno* <<https://www.americaninno.com/chicago/chicago-pd-sued-over-crime-prediction-algorithm/>>.

“European Commission - PRESS RELEASES - Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service”, (27 June 2017), online: *European Commission - Press release* <https://europa.eu/rapid/press-release_IP-17-1784_en.htm>.

Gellman, Barton & Ashkan Soltani. “NSA Collects Millions of E-mail Address Books Globally”, Wash Post (14 October 2013), online: <https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html?utm_term=.46f442cb300e>.

———. “NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say”, Wash Post (30 October 2013), online: <https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?utm_term=.b3c3cb444959>.

Greenwald, Glenn & Ewen MacAskill. “NSA Prism Program Taps in to User Data of Apple, Google and Others”, *The Guardian* (7 June 2013), online: <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>>.

Heerden, Oscar Van. “Africa remains a captive market – are we truly au fait with technology?”, (27 June 2018), online: *Daily Maverick* <<https://www.dailymaverick.co.za/opinionista/2018-06-27-africa-remains-a-captive-market-are-we-truly-au-fait-with-technology/>>.

“IAB Europe Press release: Proposed ePrivacy Regulation Fails To Improve Cookie Rules | IAB Europe”, (10 January 2017), online: <<https://www.iabeurope.eu/policy/press-release-proposed-eprivacy-regulation-fails-to-improve-cookie-rules/>>.

Kofman, Ava. “Are New York’s Free LinkNYC Internet Kiosks Tracking Your Movements?”, (8 September 2018), online: *The Intercept* <<https://theintercept.com/2018/09/08/linknyc-free-wifi-kiosks/>>.

Joseph, George. “Justice by Algorithm”, (8 December 2016), online: CityLab <<http://www.citylab.com/crime/2016/12/justice-by-algorithm/505514/>>.

Langford, Malcolm & Mikael Rask Madsen, “France Criminalises Research on Judges”, (22 June 2019), online: *Verfassungsblog* <<https://verfassungsblog.de/france-criminalises-research-on-judges/>>.

Levy, Steven. “Secret of Googlenomics: Data-Fueled Recipe Brews Profitability”, *Wired* (22 May 2009), online: <<https://www.wired.com/2009/05/nep-googlenomics/>>.

MacAskill, Ewen et al. “GCHQ Taps Fibre-Optic Cables for Secret Access to World’s Communications”, *The Guardian* (21 June 2013), online: <<https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>>.

Marczak, Bill et al. *Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware* (The Citizen Lab, 2017).

Mitter, Rana et al. *BBC World Service - The Real Story, China’s Big Social Experiment*.

Nakashima, Ellen. “FBI paid professional hackers one-time fee to crack San Bernardino iPhone”, (12 April 2016), online: <https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html?noredirect=on&utm_term=.9f390be41c63>.

O’Shea, Sean. “Ann Cavoukian, former Ontario privacy commissioner, resigns from Sidewalk Labs”, (21 October 2018), online: *Glob News* <<https://globalnews.ca/news/4579265/ann-cavoukian-resigns-sidewalk-labs/>>.

Panzarino, Matthew. “Apple’s Tim Cook Delivers Blistering Speech On Encryption, Privacy”, (2 June 2015), online: *Tech Crunch* <<https://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/>>.

Pierson, David. “While It Defies U.S. Government, Apple Abides by China’s Orders — And Reaps Big Rewards”, online: *latimes.com* <<http://www.latimes.com/business/technology/la-fi-apple-china-20160226-story.html>>.

Price Jr, William Ray. Chief justice delivers 2010 state of the Judiciary address (Jefferson City, Missouri, 2010).

Privacy International. Submission to the Information Commissioner: Request for an Assessment Notice of Data Brokers Acxiom & Oracle (2018).

———. Submission to the Information Commissioner: Request for an Assessment Notice of Data Brokers Experian & Equifax (2018).

———. Submission to the Information Commissioner: Request for an Assessment Notice / Complaint of AdTech Data Brokers Criteo, Quantcast and Tapad (2018).

“Researchers Shut Down AI that Invented Its Own Language”, (21 July 2017), online: <<http://www.digitaljournal.com/tech-and-science/technology/a-step-closer-to-skynet-ai-invents-a-language-humans-can-t-read/article/498142>>.

Scahill, Jeremy. “Find, Fix, Finish”, (15 October 2015), online: *The Intercept* <<https://theintercept.com/drone-papers/find-fix-finish/>>.

Scola, Nancy. “Obama, the ‘big data’ president - The Washington Post”, (14 June 2013), online: <https://www.washingtonpost.com/opinions/obama-the-big-data-president/2013/06/14/1d71fe2e-d391-11e2-b05f-3ea3f0e7bb5a_story.html?utm_term=.050d06cc9c61>.

Sicular, Svetlana. “Gartner’s Big Data Definition Consists of Three Parts, Not to Be Confused with Three ‘V’s”, (27 March 2013), online: *Forbes* <<https://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/#6106aeaa42f6>>.

Sledge, Matt. “Convicted gang leader can challenge NOPD’s use of crime-fighting software, judge rules”, (14 March 2018), online: *The Advocate* <https://www.theadvocate.com/new_orleans/news/courts/article_3a68a838-27bb-11e8-8b07-178e270926d4.html>.

Steel, Emily. “Financial worth of data comes in at under a penny a piece”, (12 June 2013), online: *Financ Times* <<https://www.ft.com/content/3cb056c6-d343-11e2-b3ff-00144feab7de>>.

———. “How much is your personal data worth?”, (12 June 2013), online: <<https://ig.ft.com/how-much-is-your-personal-data-worth/>>.

Stein, Michael Isaac. “‘Holy cow’: the powerful software behind the city’s surveillance system | The Lens”, (20 December 2018), online: *The Lens* <<https://thelensnola.org/2018/12/20/holy-cow-the-powerful-software-behind-the-citys-surveillance-system/>>.

Stewart, Jack. “It Takes a Single Autonomous Car to Prevent Phantom Traffic Jams”, *Wired* (16 May 2018), online: <<https://www.wired.com/story/one-autonomous-car-prevent-traffic-jams/>>.

Vaas, Lisa. “Politicians in Iowa City reluctantly pass ban on drones, automatic traffic surveillance”, (6 June 2013), online: *Naked Secur* <<https://nakedsecurity.sophos.com/2013/06/06/iowa-ban-drones-traffic-surveillance/>>.

Winston, Ali. “Palantir has secretly been using New Orleans to test its predictive policing technology”, (27 February 2018), online: *The Verge* <<https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd>>.

Zuboff, Shoshana. “Google as a Fortune Teller: The Secrets of Surveillance Capitalism”, *FAZNET* (3 May 2016), online: <<http://www.faz.net/1.4103616>>.

Websites

Access Now. *Creating a Data Protection Framework: a Do’s and Don’ts Guide for Lawmakers* (Access Now, 2018).

“ACLU of Massachusetts v. Boston Police Department”, (14 November 2018), online: *ACLU Massachusetts* <<https://www.aclum.org/en/cases/aclu-massachusetts-v-boston-police-department>>.

Acxiom Corporation Annual Report 2014 (Acxiom, 2014).

Acxiom Corporation Annual Report 2017 (Acxiom, 2017).

Amnesty International, *Left in the Dark: The Use of Secret Evidence in the United Kingdom* (Amnesty International, 2012).

“An Act to Promote Transparency and Protect Civil Rights and Civil Liberties With Respect to Surveillance Technology”, online: *ACLU* <<https://www.aclu.org/files/communitycontrol/ACLU-Local-Surveillance-Technology-Model-City-Council-Bill-January-2017.pdf>>.

Big Data Business Impact: Achieving Business Results through Innovation and Disruption (New Vantage Partners LLC, 2017).

Brighter AI, “How to increase the value of your anonymized data? - Generate Vision”, (15 October 2018), online: *Medium* <<https://medium.com/generate-vision/how-to-increase-the-value-of-your-anonymized-data-c182ba4fc8db>>.

“Community Control Over Police Surveillance + Militarization (CCOPS+M) Model Bill”, (October 2018), online: *American Civil Liberties Union* <<https://www.aclu.org/other/community-control-over-police-surveillance-militarization-ccopsm-model-bill>>.

Electronic Privacy Information Center & Consumer Privacy Organizations. Letter to Federal Trade Commission, Re: How tech companies nudge users to choose less privacy-friendly options (2018).

EPIC. In re: Facebook, Inc. Internet Tracking Litigation (Electronic Privacy Information Center, 2018).

Brandeis, Louis D. *Other People's Money and How the Bankers Use It* (New York: Cosimo, Inc., 2009).

EU Agency for Fundamental Rights and Council of Europe. *Handbook on European data protection law*, 2018 edition ed (Luxembourg: Publications Office of the EU, 2018).

Hildebrandt, Mireille. *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing, 2015).

Ihde, Don. *Technics and praxis*, Boston studies in the philosophy of science 24 (Dordrecht: Reidel, 1979).

Lindahl, Hans. *Fault Lines of Globalization: Legal Order and the Politics of A-legality* (Oxford, United Kingdom: Oxford University Press, 2013).

Mayer-Schönberger, Viktor & Kenneth Cukier. *Big Data: A Revolution that Will Transform how We Live, Work, and Think* (Houghton Mifflin Harcourt, 2013).

Mendel, Toby et al. *Global survey on internet privacy and freedom of expression* (UNESCO, 2012).

Pasquale, Frank. *The black box society: the secret algorithms that control money and information* (Cambridge: Harvard University Press, 2015).

Ananny, Mike & Kate Crawford. “Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability” (2018) 20:3 *New Media & Society* 973.

Angwin, Julia. "Google faces new privacy probes", *The Wall Street Journal* (16 March 2012), online: <<https://www.wsj.com/articles/SB10001424052702304692804577283821586827892>>.

Arnardóttir, Oddný Mjöll. "The 'procedural turn' under the European Convention on Human Rights and presumptions of Convention compliance" (2017) 15:1 *Int J Const Law* 9.

Arthur, Charles. "Google facing legal threat from six European countries over privacy", *The Guardian* (2 April 2013), online: <<https://www.theguardian.com/technology/2013/apr/02/google-privacy-policy-legal-threat-europe>>.

Beetham, David. "Market economy and democratic polity: Democratization" (1997) 4:1 *Democratization* 76.

Brakel, Rosamunde van & Paul De Hert. "Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies" (2011) 20:3 *Journal of Police Studies* 163.

Crain, Matthew. "The limits of transparency: Data brokers and commodification" (2018) 20:1 *New Media & Society* 88.

Diggelmann, Oliver & Maria Nicole Cleis. "How the Right to Privacy Became a Human Right" (2014) 14:3 *Human Rights Law Review* 441.

Edwards, Lilian & Michael Veale. "Slave to the Algorithm? Why a 'Right to Explanation' Is Probably Not the Remedy You Are Looking For" (2017) 16:1 *Duke Law and Technology Review* 19.

Ferguson, Andrew Guthrie. "Big Data and Predictive Reasonable Suspicion" (2015) 163:2 *University of Pennsylvania Law Review* 327.

Galetta, Antonella. "The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?" (2013) 4:2 *European Journal of Law and Technology*, online: <<http://ejlt.org/article/view/221>>.

Hildebrandt, Mireille. "Who is Profiling Who? Invisible Visibility" in Serge Gutwirth et al, eds, *Reinventing Data Protection?* (Springer, Dordrecht, 2009) 239.

Hirsch, Dennis D. "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?" 34 *Seattle University Law Review* 439.

Jasserand, Catherine. "Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?" (2018) 34:1 *Computer Law & Security Review* 154.

Joergensen, Rikke Frank. “The unbearable lightness of user consent” (2014) 3:4 Internet Policy Review 1.

Kleinlein, Thomas. “Consensus and Contestability: The ECtHR and the Combined Potential of European Consensus and Procedural Rationality Control” (2017) 28:3 Eur J Int Law 871.

———. “The Procedural Approach of the European Court of Human Rights: Between Subsidiarity and Dynamic Evolution” (2019) 68:1 International & Comparative Law Quarterly 91.

Malgieri, Gianclaudio & Giovanni Comandé. “Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation” (2017) 7:4 International Data Privacy Law 243.

Mendoza, Isak & Lee A Bygrave. “The Right Not to be Subject to Automated Decisions Based on Profiling” in Tatiana-Eleni Synodinou et al, eds, *EU Internet Law: Regulation and Enforcement* (Springer International Publishing, 2017) 77.

Nissenbaum, Helen. “A Contextual Approach to Privacy Online” (2011) 140:4 Daedalus 32.

Purtova, Nadezhda. “The law of everything. Broad concept of personal data and future of EU data protection law” (2018) 10:1 Law, Innovation and Technology 40.

Raz, Joseph. “Rule of Law and its Virtue” in *The Authority of Law: Essays on Law and Morality* (Oxford: Clarendon Press, 1979).

Redish, Martin H & Lawrence C Marshall. “Adjudicatory Independence and the Values of Procedural Due Process” (1986) 95:3 The Yale Law Journal 455.

Rouvroy, Antoinette & Yves Poullet. “The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy” in Serge Gutwirth et al, eds, *Reinventing Data Protection?* (Dordrecht: Springer Netherlands, 2009) 45.

Scheper, Christian. “‘From naming and shaming to knowing and showing’: human rights and the power of corporate practice” (2015) 19:6 The International Journal of Human Rights 737.

Selbst, Andrew D & Julia Powles. “Meaningful information and the right to explanation” (2017) 7:4 International Data Privacy Law 233.

Wachter, Sandra, Brent Mittelstadt & Luciano Floridi. “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation” (2017) 7:2 International Data Privacy Law 76.

White House Report. “Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy” (2012) 4:2 Journal of Privacy and Confidentiality 95.

Wills, Aidan & Hans Born. “International Intelligence Cooperation and Accountability: Formidable Challenges and Imperfect Solutions” in Hans Born, Ian Leigh & Aidan Wills, eds, *International Intelligence Cooperation and Accountability* (Routledge, 2011) 277.

Zegart, Amy B. “The Domestic Politics of Irrational Intelligence Oversight” (2011) 126:1 *Political Science Quarterly* 1.

Access Now. *Creating a Data Protection Framework: a Do’s and Don’ts Guide for Lawmakers* (Access Now, 2018).

Bigo, Dider et al. *National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges*, Study for the LIBE Committee (Directorate-General for Internal Policies, Policy Department C: Citizens’ Rights and Constitutional Affairs, European Parliament, 2014).

Bipartisan Policy Center & the Annenberg Public Policy Center of the University of Pennsylvania. *Today’s Rising Terrorist Threat and the Danger to the United States: Reflections on the Tenth Anniversary of the 9/11 Commission Report* (2014).

Dallke, Jim. “Chicago Police Sued Over ‘Heat List’ Algorithm by Journalists”, (8 June 2017), online: *American Inno* <<https://www.americaninno.com/chicago/chicago-pd-sued-over-crime-prediction-algorithm/>>.

European Commission for Democracy Through Law (Venice Commission). *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*, CDL-AD(2015)006 (Venice: Council of Europe, 2015).

Gray, Megan. “Understanding & Improving Privacy ‘Audits’ under FTC Orders”, (18 April 2018), online: *The Center for Internet and Society of Stanford Law School* <[/blog/2018/04/understanding-improving-privacy-audits-under-ftc-orders](https://blog/2018/04/understanding-improving-privacy-audits-under-ftc-orders)>.

Heerden, Oscar Van. “Africa remains a captive market – are we truly au fait with technology?”, (27 June 2018), online: *Daily Maverick* <<https://www.dailymaverick.co.za/opinionista/2018-06-27-africa-remains-a-captive-market-are-we-truly-au-fait-with-technology/>>.

House of Lords, Select Committee on the Constitution. *Surveillance: Citizens and the State* (London: House of Lords, 2009).

La Rue, Frank. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression*, A/HRC/17/27 (Human Rights Council, 2011).

O’Connor, Nuala. “Reforming the U.S. Approach to Data Protection and Privacy”, (30 January 2018), online: *Council on Foreign Relations* <<https://www.cfr.org/report/reforming-us-approach-data-protection>>.

Sledge, Matt. “Convicted gang leader can challenge NOPD’s use of crime-fighting software, judge rules”, (14 March 2018), online: *The Advocate* <https://www.theadvocate.com/new_orleans/news/courts/article_3a68a838-27bb-11e8-8b07-178e270926d4.html>.

Stein, Michael Isaac. “‘Holy cow’: the powerful software behind the city’s surveillance system | The Lens”, (20 December 2018), online: *The Lens* <<https://thelensnola.org/2018/12/20/holy-cow-the-powerful-software-behind-the-citys-surveillance-system/>>.

-Waldman, Rachel & Erica Posey. “Court Rejects NYPD Attempts to Shield Predictive Policing from Disclosure”, (26 January 2018), online: *Brennan Center for Justice* <<https://www.brennancenter.org/blog/court-rejects-nypd-attempts-shield-predictive-policing-disclosure>>.

Winston, Ali. “Palantir has secretly been using New Orleans to test its predictive policing technology”, (27 February 2018), online: *The Verge* <<https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd>>.

Wright, David, David Barnard-Wills & Inga Kroener. *Deliverable 4: Findings and recommendations* (PHAEDRA, 2015).

Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (Federal Trade Commission, 2012).

“IAB Europe Press release: Proposed ePrivacy Regulation Fails To Improve Cookie Rules | IAB Europe”, (10 January 2017), online: <<https://www.iabeurope.eu/policy/press-release-proposed-eprivacy-regulation-fails-to-improve-cookie-rules/>>.

“European Commission - PRESS RELEASES - Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service”, (27 June 2017), online: *European Commission - Press release* <http://europa.eu/rapid/press-release_IP-17-1784_en.htm>.

“Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google’s search engine”, (18 July 2018), online: *European Commission - Press release* <http://europa.eu/rapid/press-release_IP-18-4581_en.htm>.

“Community Control Over Police Surveillance + Militarization (CCOPS+M) Model Bill”, (October 2018), online: *American Civil Liberties Union* <<https://www.aclu.org/other/community-control-over-police-surveillance-militarization-ccopsm-model-bill>>.

“ACLU of Massachusetts v. Boston Police Department”, (14 November 2018), online: *ACLU Massachusetts* <<https://www.aclum.org/en/cases/aclu-massachusetts-v-boston-police-department>>.

“Bundeskartellamt prohibits Facebook from combining user data from different sources”, (7 February 2019), online: *Bundeskartellamt* <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html>.

“Restrictions on Military Gear to Local Police Are Lifted”, online: *Equal Justice Initiative* <<https://ejl.org/news/restrictions-military-gear-local-police-are-lifted>>.

“An Act To Promote Transparency and Protect Civil Rights and Civil Liberties With Respect to Surveillance Technology”, online: *ACLU* <<https://www.aclu.org/files/communitycontrol/ACLU-Local-Surveillance-Technology-Model-City-Council-Bill-January-2017.pdf>>.

“PIA & DPIA Automation | Products”, online: *OneTrust* <<https://www.onetrust.com/products/assessment-automation/>>.

“Nymity’s Software Solutions for the privacy office”, online: *Nymity* <<https://www.nymity.com/solutions/>>.

“GDPR Compliance Solutions - Platform and Consulting”, online: *TrustArc* <<https://www.trustarc.com/products/gdpr-compliance/>>.

“Evidon | Universal Consent Platform for Site, App, and Ad Compliance”, online: *Evidon* <<https://www.evidon.com/solutions/universal-consent/>>.

“Frequently Asked Questions”, online: *LinkNYC* <<https://www.link.nyc>>.

“GDPR Compliance Solutions - Platform and Consulting”, online: *TrustArc* <<https://www.trustarc.com/products/gdpr-compliance/>>.

Gray, Megan. “Understanding & Improving Privacy ‘Audits’ under FTC Orders”, (18 April 2018), online: *The Center for Internet and Society of Stanford Law School* <blog/2018/04/understanding-improving-privacy-audits-under-ftc-orders>.

Introduction to the Google Ad Auction.

Laney, Doug. “To Facebook You’re Worth \$80.95”, (3 May 2012), online: *Wall Str J* <<https://blogs.wsj.com/cio/2012/05/03/to-facebook-youre-worth-80-95/>>.

LinkNYC. “Privacy Policy”, (17 March 2017), online: *LinkNYC* <<https://www.link.nyc/privacy-policy.html>>.

Mauldin, Alan. *What the Internet looks like: Undersea cables wiring ends of the Earth* (2015).

McGuire, Tim, James Manyika & Michael Chui. “Why Big Data is the new competitive advantage •”, (August 2012), online: <<https://iveybusinessjournal.com/publication/why-big-data-is-the-new-competitive-advantage/>>.

“Nymity’s Software Solutions for the privacy office”, online: *Nymity* <<https://www.nymity.com/solutions/>>.

O’Connor, Naula. “Reforming the U.S. Approach to Data Protection and Privacy”, (30 January 2018), online: *Council on Foreign Relations* <<https://www.cfr.org/report/reforming-us-approach-data-protection/>>.

O’Donovan, Dave. *Harnessing the Data Exhaust Stream: Changing the Way the Insurance Game is Played* (Accenture, 2016).

“PIA & DPIA Automation | Products”, online: *OneTrust* <<https://www.onetrust.com/products/assessment-automation/>>.

Project Vision (Sidewalk Labs, 2017).

PwC. “In which areas are you using big data analytics today? In which additional areas will your company use data analytics in five years?”, (2016), online: Statista <<https://www.statista.com/statistics/549712/worldwide-survey-use-of-data-analytics-by-business-area/>>.

“Restrictions on Military Gear to Local Police Are Lifted”, online: *Equal Justice Initiative* <<https://eji.org/news/restrictions-military-gear-local-police-are-lifted/>>.

SliconANGLE, Wikibon. “Forecast of Big Data market size, based on revenue, from 2011 to 2027 (in billion U.S. dollars)”, online: Statista <<https://www.statista.com/statistics/254266/global-big-data-market-forecast/>>.

Sidewalk Project Update (Sidewalk Labs, 2019).

Transparency Market Research. “Data Broker Market is expected to surge at 11.5% CAGR between 2017 & 2026 - TMR”, (7 December 2017), online: GlobeNewswire News Room <<http://globenewswire.com/news-release/2017/12/07/1247221/0/en/Data-Broker-Market-is-expected-to-surge-at-11-5-CAGR-between-2017-2026-TMR.html>>.

“Using Quality Score to Guide Optimisations: Google Best Practices”, online: Google Ads Help <<https://support.google.com/google-ads/answer/6167123>>.

Waldman, Rachel & Erica Posey. “Court Rejects NYPD Attempts to Shield Predictive Policing from Disclosure”, (26 January 2018), online: *Brennan Center for Justice* <<https://www.brennancenter.org/blog/court-rejects-nypd-attempts-shield-predictive-policing-disclosure>>.