

Columbia University
Graduate School of Arts and Sciences
Human Rights Studies Master of Arts Program

Our Vulnerable Privacy: The Effects of Ubiquitous Techno-Surveillance Programs on
Sociological Expectations of Privacy

Madiha Zahrah Choksi

Thesis Advisor: Eben Moglen

Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Arts

January, 2019



This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Abstract

Our Vulnerable Privacy: The Effects of Ubiquitous Techno-Surveillance Programs on Sociological Expectations of Privacy

Madiha Zahrah Choksi

In the 21st century, ubiquitous technologies strengthen ubiquitous surveillance. Although the right to privacy is protected by the Constitution, challenges persist with respect to how it is interpreted in an age of data-rich technologies. This paper examines how the deficiencies of the Fourth Amendment in an age of techno-surveillance contribute to the widening scope and success of modern surveillance. The discussion outlines how modern communications technologies have coalesced with surveillance programs of the New York City Police Department, the National Security Agency, and commercial applications such as Facebook, and identifies how intractable institutional programs contribute to a lasting cultural effect in our society. The result is a snowballing effect of normalization: an identifiable cultural change in sociological expectations of privacy. On the one hand, state authorities such as the NSA can monitor and intercept all activity and interactions, with or without a warrant. Along the same lines, data collection on Facebook thrives through its commercialized “opt-out” or pseudo-participatory model, in which consent is assumed or obtained covertly. While technological advances and legal reality are the common denominators of all three institutional models considered in this paper, Facebook’s surveillance structure presents the best opportunity for sociocultural expectations to oscillate. The threats posed by Facebook on freedom and autonomy are causing alarm and panic that, for the first time, are forming ripples of action against pervasive surveillance.

Table of Contents

Acknowledgements		...iv
Chapter 1	Introduction	...1
1.1.	Objective	...2
Chapter 2	Literature Review: Culture, Nature, and Surveillance	...4
2.1.	Culture and Nature	...4
2.2.	Surveillance	...5
2.2.1.	Panoptic vs. Non-Panoptic Surveillance	...5
2.3.	Surveillance Society, Technology, and Culture	...6
Chapter 3	Theoretical Framework, Hypothesis and Methodology	...8
3.1.	Theoretical Framework	...8
3.1.1.	Normalization	...8
3.1.2.	The Fourth Amendment: “Reasonable Expectation of Privacy”	...8
3.2.	Hypothesis and Methodology	...11
Chapter 4	Information Exposure	...13
4.1.	Modern Technologies Overview	...13
4.2.	Metadata Collection	...14
4.3.	Data Storage Capacity	...14
4.4.	Risky by Design: Investigating Design, Processes, and Features	...15
4.4.1.	Closed Source or Proprietary Code	...15
4.4.2.	Cloud Storage	...16

4.4.3.	ICT Convergence and Privacy	...16
Chapter 5	Changes Manifest Themselves: The New York City Police Department’s Domain Awareness System	...20
5.1.	Closed Circuit Television Cameras (CCTV)	...21
5.2.	License Plate Readers (LPRs)	...23
Chapter 6	Edward Snowden and The National Security Agency	...26
6.1.	NSA 215 Bulk Metadata Collection Program and XKeyscore	...27
Chapter 7	Facebook and Algorithmic Surveillance	...32
7.1.	Data Collection, Algorithms and Bias	...33
Chapter 8	Looking Beyond: Cambridge Analytica and Future of “Reasonable Expectation of Privacy”	...37
Bibliography		...40

Figures

5.1	Image from Vigilant Solutions Article “Protect LPR with Positive Legislation”	...24
6.1	Question and Response from Pew Research Center’s “Web IQ Quiz”	...30
7.1	Chart from Pew Research Center Survey “Public Attitudes Towards Computer Algorithms”	...35
8.1	Chart from Pew Research Center Survey “Americans Are Changing Their Relationship with Facebook”	...38

Acknowledgement

I would like to express my sincere gratitude to my thesis advisor, Professor Eben Moglen, without whose continuous support, motivation, and patience, I would be far from where I am today, and even further from where I intend to go. I would like to thank him for being an exceptional teacher, a dedicated editor, and above all, a great friend. His guidance has both challenged and inspired me, and his mentorship is the highlight of my time at Columbia University, an experience I will forever cherish.

كولين ,

إذا كنت ستسألني:
"ما الفرق بيني وبين السماء؟"
الفرق يا حبيبي
هل هذا عندما تضحك
انسى السماء

Chapter 1

Introduction

“Under observation, we act less free, which means we effectively are less free.”

— Edward Snowden

As drafted by the Founding Fathers, the Fourth Amendment seeks to protect individuals from the potentially tyrannical powers of a police force. However, technological advances, the motivations of state actors, and deeply embedded corporate ties have facilitated the expansion of surveillance programs, challenging the Constitution’s ability to protect the privacy of American citizens. Under the Fourth Amendment guidelines, people have the right against all unreasonable searches and seizures, but the objective standard of the “reasonable expectation of privacy” clause also means that it has no bearing on what people actually expect. What, then, are the expectations of privacy in the 21st century? As ubiquitous institutional surveillance in the form of warrantless data and metadata collection becomes increasingly prevalent, how have expectations about privacy within American culture changed to threaten and challenge the fundamental right to privacy?

In 2002, the newly appointed NYPD Commissioner Raymond Kelly set reforming how the department would manage their information technology capabilities as one of his principal objectives. Together, Kelly and his newly appointed deputy commissioner, well acquainted with the commercial information technology industry, revolutionized how the NYPD engaged in policing. In an effort to accelerate the police department’s intelligence gathering, the Information Technology Bureau sought strategic corporate partnerships to create repositories for data storage and querying.¹ In its present form, the Domain Awareness System (DAS) is a tool that delivers analytics both to officers on the ground via a smartphone and to officers stationed in a precinct. Though its complex network of databases, sensors, devices, and software were first designed for the NYPD’s counterterrorism unit, the DAS is now used universally by the department and presents challenging questions about how data is collected, how it is used for predictive analytics, and more general issues surrounding the retention of personal data.²

Similarly, in another model of government surveillance, the documents exposed by Edward Snowden revealed the extent to which the National Security Agency engaged in widespread data collection in the name of homeland security. Following the tragedy of 9/11, the NSA passed legislation to authorize large-scale metadata collection programs under the USA PATRIOT Act, many of which Edward Snowden uncovered in the summer of 2013. The 2001 PATRIOT Act widened the scope of data that the government was able to collect from Internet service providers with subpoenas—information including names, addresses, session times, IP addresses, and bank accounts. The act also extended roving wiretapping practices that were once limited to phones to encompass email and web browsing. Moreover, the regulation was updated

¹ E. S. Levine et al., “The New York City Police Department’s Domain Awareness System,” *Interfaces* 47, no. 1 (February 2017): 70–84.

² *Ibid.*, 74.

to reflect that communication surveillance for the purpose of gathering intelligence by the government must be for a “significant purpose” instead of being its “primary purpose.”³

In a third, parallel realm, collecting information on user behavior constitutes the operational business model of powerhouse search engines and social media companies. On the web, social networking platforms, online shopping websites, and even digital news and media platforms attract millions of users who upload and share personal information that provides useful data about their consumption preferences back to the hosts. On Facebook, algorithmic processes help facilitate this process, and Facebook has become a surveillance engine, tracking, storing, targeting, and influencing all areas of user experience on and off the platform.

Together, local, federal, and corporate exploitation of information and communications technologies (ICTs) in surveillance programs points to a social reality in which technologies have been transformed to work against the individuals for whom they were created to serve. This paper posits that the practical applications of emerging technologies have created a lasting cultural effect on the scope of our expectation of privacy. As society becomes increasingly familiar with the feeling of ubiquitous techno-surveillance, it is easy to forget that this was not inevitable. This reality is an outcome of deliberate actions by actors like the NSA, the NYPD, and Facebook, and there were other possible realities along the way. By examining the contemporary techniques of information collection utilized by local, federal, and commercial institutions, this paper problematizes our quotidian interactions with surveillance technology, assessing why the experience of being surveilled is not normal, even though it is normalized. Ultimately, as a result of the social process of normalization, the threat of the erosion of privacy lies in fragile and shifting sociological expectations of privacy.

1.1 Objective

Privacy is a fundamental human right, as it corresponds to the dignity of all individuals, and forms a critical part in the fulfillment of other equal and inalienable rights such as Freedom of Thought, Freedom of Religion and Freedom of Association outlined in the First Amendment of the United States Constitution. The right to privacy can be found in the Fourth Amendment of the Constitution, and in international human rights law under Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Convention on Civil and Political Rights, and Article 8 of the European Convention on Human Rights. Privacy in the 21st century is a pressing issue, and both domestic and international courts recognize the threats to individual and state privacy posed by data-rich ICTs. As such, this paper investigates the intersection of rights, technologies, and social experience to underline the critical relationship between all three and their role in creating a fragile state of privacy.

In 1440, the invention of mechanical moveable type in Europe initiated the era of mass communication, revolutionizing human society. Among its accomplishments, the printing press allowed for the dissemination of books, which empowered individuals to read and process information in solitude and without an intermediary. Such power, though overlooked in today’s

³ Christian Fuchs, *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (New York: Routledge, 2012), 11.

time of instantaneously available information, was made possible by people's ability to access and process information in private settings and is the foundation of universal freedoms, specifically freedom of thought and of privacy.

The sociocultural effects of modern pervasive surveillance are not commonly linked to the printing press and the early era of mass communication. However, the objective of this thesis is to examine how advancing ICTs and the institutions that depend on them have created a cultural effect on how much and even what type of surveillance society expects. Within the NYPD, the NSA, and the commercial model of surveillance (as represented by Facebook), implementing the tools used to gather data is falsely presented as a necessary undertaking operating within a limited scope. In reality, the asymmetric balance of power between surveillant and the surveilled is such that collecting and processing one's data becomes an end in and of itself—one in which much more than what is sought out is collected.

In contrast with early ICTs, present-day information technologies, through which we not only communicate, but schedule, navigate, and even think, are infused with enormous amounts of personal data and have become central to institutional information collection. Without the capacity to privately, or freely, access information, people effectively cede control of their freedom of thought, and by extension, their individuality and their ability to make decisions—fundamental concepts of humanity. In other words, the printing press represented a mode of mass information dissemination characterized by personal empowerment, free and spontaneous inquiry, and freedom from intermediaries between information and an individual. However, contemporary modes of accessing information are rife with surveillance technologies as benign as cookies and as malicious as warrantless data collection.

Chapter 2

Literature Review: Culture, Nature, and Surveillance

In order to make a meaningful argument about how a cultural shift in 21st-century society has materialized, we must first review the multi-faceted definitions of *culture*, *nature*, and *surveillance*. By doing so, the literature review outlines existing works to establish both the discipline in which this paper falls as well as the ideas and trends to which it seeks to contribute.

2.1. *Culture and Nature*

In *Keywords*, Raymond Williams claims that culture is one of the most complicated words in the English language, tracing its historical development through European languages. In its earliest use, culture was a noun of process which applied to crops or animals and later extended to a process of human development.⁴ A major turning point in the development of the term came in 1660, when John Milton connected government and culture, defining culture as a general social process that is a definitive state of development.⁵ A final transformation of the term designated culture as a concept, which according to Williams, can be categorized into three groups. The first group returns us to the idea of culture as a process, an abstract noun that traces a general process of development. The second, inspired by Herder and Klemm, delineates a lifestyle of either a group of people, a place, or a period in time. The third and final group catalogs the term as one that reports customs and procedures of intellectual and artistic endeavors. Williams points out that the third category has become the most universal, where culture includes literature, painting, and theatre, as well as history, philosophy, and scholarship.⁶

In establishing what it means to exist in and participate in a culture, we accept that culture shares a relationship with nature and that which is accepted to be natural. Nature can be also be identified in three separate categories of meaning. Williams outlines that the first category of nature is the quality or character of something. The second is an innate force that directs the earth, as well as humans, sometimes simultaneously, and the third consists of the material or tangible word both with and without humans.⁷ Nature and reason became connected phenomena through the formation of laws, a system of rules enforced through social or governmental institutions to regulate behavior. Accordingly, nature identifies something that existed prior to human development, a distinction from something created by mankind.⁸ However, Williams adds that if something connected to humans has been artificially created and disseminated over an undefined but extended period of time, it may be classified as a natural entity or experience.⁹ The insidious expansion of surveillance represents the process of anthropogenic phenomena eventually being regarded as natural simply by their transmission by

⁴ Raymond Williams, *Keywords : A Vocabulary of Culture and Society* (New York: Oxford University Press, 1985), 49.

⁵ *Ibid.*, 50.

⁶ *Ibid.*, 54.

⁷ *Ibid.*, 167.

⁸ Williams, *Keywords*, 168.

⁹ *Ibid.*

figures of authority: The more time that passes where surveillance is seen as essential for security, the less it is questioned.

2.2. *Surveillance*

Surveillance is a phenomenon that has accompanied human society since its inception as the “regard or attendance to others (whether a person, a group, or an aggregate as with a national census) or to factors presumed to be associated with these.”¹⁰ A central element to surveillance is the collection of data that can be traced back to a single individual or an individual within a larger group or category.¹¹ We can observe early models of state surveillance for the purpose of maintaining control over the state and its subjects in 16th-century England. People in positions of power used state surveillance to maintain their power, or as Lyon states, as an inherent practice of governance as opposed to crude social control.¹² This earliest appearance of centralized surveillance saw the recording of births, deaths, marriages, and churches, and enshrined a framework for modern central state surveillance practices.

Whereas the earliest forms of surveillance established a practice of recording information in an effort to maintain bureaucratic control over groups and populations,¹³ surveillance practices eventually saturated all areas of human society. According to Karl Marx, surveillance in the workplace relates to maintaining control over laborers in the context of a capitalist economy. Alternatively, Max Weber, or the Weberian theory, asserts that the collection and storage of information in the workplace is linked to efficient practices within the organization. Most critical to this paper, however, is Michel Foucault’s groundbreaking work on surveillance and discipline. Foucault maintains that societies have created means of ordering society at the institutional level that seamlessly integrate fear of discipline as a way to ensure control and regulated, or normalized, patterns of behavior.¹⁴

2.2.1. *Panoptic vs. Non-Panoptic Surveillance*

Jeremy Bentham’s panopticon symbolizes what Foucault describes as the “modern disciplinary society.”¹⁵ The precision in the space’s architectural design enables the enforcer to surveil the prison in its entirety without being seen.¹⁶ The incitement of fear thus provokes self-surveilling and self-disciplinary habits by the subordinate persons surveilled so as to avoid punishment from the all-seeing enforcer. The panoptic view holds that the Internet’s webbed

¹⁰ Gary T. Marx, “Surveillance Studies,” in *International Encyclopedia of the Social & Behavioral Sciences* (Elsevier, 2015), 734.

¹¹ Ibid.

¹² David Lyon, *Surveillance after September 11* (Malden, MA: Distributed in the USA by Blackwell Pub, 2003), 23.

¹³ David Lyon, *Electronic Eye: The Rise of Surveillance Society* (Minneapolis, United States: University of Minnesota Press, 1994), <http://ebookcentral.proquest.com/lib/columbia/detail.action?docID=310274>, 4.

¹⁴ Ibid., 7.

¹⁵ Michel Foucault, *Discipline and Punish: The Birth of the Prison* (New York: Vintage Books, 1995).

¹⁶ Fuchs, *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, 126.

infrastructure allows it to function as a tool through which economic surveillance can occur.¹⁷ Cookies and indexing features are fundamental to search engines that, by design, “collect and categorize human behavior.”¹⁸ Such “identification tools” constitute surveillance mechanisms used to categorize people and also correlate to the interests of political actors who help facilitate their widespread development and implementation.¹⁹ Within this model, users are unable to modify or examine the software mediating their experience, fundamentally depriving them of their autonomy and control. Moreover, in such domains, “controls are exercised on the basis of a space defined on the network,”²⁰ meaning that the operated space is controlled by an external source, such as an Internet service provider.

The non-panoptic outlook argues that centralized Internet surveillance is neutral and creates positive and negative consequences for citizens.²¹ The most cited positive consequences include the safety and protection of citizens, while negative consequences relate to the state’s despotic control.²² However, scholars who hold neutral perspectives admit that the relationship between capitalism and the public sphere buttresses the asymmetrical balance of power²³ at the expense of end users. Through the increasing use of mobile and other tracking devices, the driving forces behind expanding surveillance within society are no longer limited to traditional economic and political forces but involve technological forces as well.²⁴ Some scholars opine that certain types of surveillance can be justified given their intent and attributes,²⁵ while others cite only advantages, such as the “empowering” ability of surveillance that connects people and bolsters social interaction.²⁶ A final perspective that emphasizes the role of users in surveillance practices speaks to the non-panoptic nature of modern surveillance because, by choosing to use mobile devices such as smartphones, users—rather than the unseen enforcer—initiate self-surveillance.²⁷

2.3. Surveillance Society, Technology, and Culture

As surveillance becomes increasingly computerized, Rule et al. state that the objective of modern surveillance is to exert influence through systematic awareness of people’s lives and that this model has become a standard for all modern societies. Such forms of systematic, information-based surveillance practices expand into institutional routines, through which the routine and methodological surveillance of everyday life simultaneously become central to modern social relations. Along these lines, Anthony Giddens asserts that modern societies are

¹⁷ G. Elmer, “Spaces of Surveillance: Indexicality and Solicitation on the Internet,” *Critical Studies in Mass Communication* 14, no. 2 (June 1997): 182.

¹⁸ Ibid.

¹⁹ Manuel Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society* (New York: Oxford University Press, 2001), 168.

²⁰ Ibid., 170.

²¹ Fuchs, *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, 127.

²² David Lyon, ed., *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (London: New York: Routledge, 2003), 164.

²³ Fuchs, *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, 128.

²⁴ Lyon, “Surveillance as Sorting: Privacy, Risk, and Digital Discrimination,” 99.

²⁵ Fuchs, *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, 130.

²⁶ Ibid., 131.

²⁷ Ibid., 132.

inherently information societies and, as such, were always at the brink of becoming surveillance societies.²⁸

David Burnham states that emerging computer technologies are increasingly autonomous and have surpassed the effective control of humans, a theory which inherently limits a meaningful discussion on surveillance culture. Conversely, Kevin Wilson argues that this technological mechanism is a tool of capitalism as a form of social and behavioral control. In sum, while technologies develop thanks to their iterative power to increase their capacity and influence, David Lyon theorizes that the augmentation of technology is a social process. This process is driven by more than just economic and political factors; it also includes institutional powers as willing participants in shaping its trajectory.²⁹

Roger Clarke's term "dataveillance" is critical in this discussion, as it defines a surveillance society as one in which the application of information technologies facilitates the monitoring of the communication and actions of people. This view is confirmed in Gary Marx's report covering undercover policing in the United States. Marx argues that the social implications of computerized or systemized information-based surveillance, or what he calls "new surveillance," are dangerous in that they are powerful and efficient while decreasingly visible.³⁰ "New surveillance" encompasses new techniques such as computer matching, first used in 1970 by governmental departments to match data from a variety of different sources in an attempt to categorize and sort groups of people. Moreover, he asserts that "computers qualitatively alter the nature of surveillance—routinizing, broadening, and deepening it."³¹

Surveillance culture has been cited by William Staples in his work studying day-to-day interactions with surveillance. John McGrath's *Loving Big Brother* applies the term in a discussion of performative surveillance, and Jonathan Finn connects surveillance culture to camera surveillance and the proliferation of cameras for surveillance programs in public spaces.³² While surveillance culture is frequently discussed, according to David Lyon, the term has yet to be defined as a phenomenon treated and applied in a similar manner to the concepts of *state surveillance* or the aforementioned *surveillance society*.³³

²⁸ Thomas J Misa, Philip Brey, and Andrew Feenberg, *Modernity and Technology* (Cambridge: MIT Press, 2014), 167.

²⁹ Lyon, *Electronic Eye: The Rise of Surveillance Society*, 11.

³⁰ *Ibid.*, 168.

³¹ *Ibid.*, 53.

³² Lyon, *Electronic Eye: The Rise of Surveillance Society*, 11.

³³ David Lyon, "Digital Citizenship and Surveillance| Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity," *International Journal of Communication* 11, no. 0 (February 14, 2017): 824.

Chapter 3

Theoretical Framework, Hypothesis, and Methodology

3.1. *Theoretical Framework*

The theoretical framework for this paper is guided by the social process of normalization, as defined by Foucault, and the legal framework of privacy in the United States, as defined by the Fourth Amendment.

3.1.1. *Normalization*

This paper applies Michel Foucault's concept of *normalization* to understand the rise of modern surveillance practices facilitated by data emerging technologies. This perspective on how societies accept change emphasizes that social control over behavioral norms is enforced in two ways. First, this happens through what Foucault calls "discursive practices," which seek to understand how language, social institutions, subjectivity, quotidian social interactions, and power are connected. For example, how can we examine the act of submitting one's fingerprint within drastically different contexts, such as in a police precinct versus via an iPhone?³⁴ Second, institutional sanctions compel people to comply to social norms, such as the recent TSA policy requiring facial scans to fly internationally. Modern surveillance effectively normalizes surveillance technologies, and it occupies all areas of sociological life: emotions, symbolism, and culture.³⁵ Therefore, the normalization of surveillance extends beyond the proliferation of surveillance technologies and determines how technologies are immersed into the norms and institutions of our society and, by extension, are reflected in other areas of modern society.³⁶ With respect to the objective of this paper, the social process of normalization to surveillance culture is best understood by examining the critical relationship between surveillance technologies, institutions, and judicial limitations.

3.1.2. *The Fourth Amendment: "Reasonable Expectation of Privacy"*

The shared obscurity of the surveillance models discussed in this paper pertains to the Fourth Amendment's definition and application of *search* and *seizure*. As written by the Founding Fathers, the Fourth Amendment aims to ensure that American citizens are "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."³⁷ The Fourth Amendment also serves to preserve the "legitimacy of the state"³⁸ against such forms of

³⁴ David Murakami Wood and C. William R. Webster, "Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of Britain's Bad Example," *Journal of Contemporary European Research* 5, no. 2 (August 1, 2009): 259–73.

³⁵ *Ibid.*

³⁶ *Ibid.*, 264.

³⁷ U.S. Constitution, amend. IV.

³⁸ David Gray and Danielle Keats Citron, "The Right to Quantitative Privacy," *Minnesota Law Review*, Business Insights: Essentials, November 2013, 93.

unwarranted search, partially in response to the use of writs of assistance by British agents during the American Revolution. Accordingly, the rights protected under the Fourth Amendment constrain the power available to law enforcement agents in apprehending criminals.³⁹ Moreover, the Fourth Amendment concerns criminal procedure which state parties must follow when conducting searches and seizures in criminal processes. These rules govern how warrants are issued and what happens in criminal prosecutions. Fourth Amendment case law overlooks government activities that conduct searches and seizures, what constitutes the reasonable grounds for searches and seizures, as well as how to deal with violations of the Fourth Amendment. In practice, the legal grounds on which the government can undertake searches and seizures must be warranted by a court that explicitly states the place, person, or thing to be searched.⁴⁰

Following *Katz v. United States* in 1967, the Fourth Amendment abandoned its antecedent requirement for a “trespass” or intrusion on property in order for a search to be of constitutional significance.⁴¹ The question of whether there is a “reasonable expectation of privacy” both in the physical and social context of a search becomes more significant, and the Fourth Amendment now protects both individual privacy as well as physical locations and property. The landmark case redefined the aforementioned understanding of the Fourth Amendment, using an ambiguous interpretation “based on the idea of *reasonable expectations of privacy*.”⁴² In regard to information collection through digital or analog methods, the reasonable expectation of privacy is measured by the court’s interpretation through the use of the “reasonable expectation of privacy” test, which ostensibly determines if and how the Fourth Amendment applies based on subjective and objective factors such as the place, time, and surroundings in which the act in question occurred.⁴³ Since courts define such “reasonable expectations” in different ways, vagueness in the definition’s interpretation persists, complicating its application in modern cases of pervasive surveillance efforts.

Coupled with the inadequacies of the “Katz test” in regulating ever-changing and modernizing surveillance technologies, three doctrines that emerged following *Katz* exclude “most of the tracking, surveillance, and data aggregation technologies . . . beyond the scope of effective Fourth Amendment review.”⁴⁴ The “public observation doctrine” maintains that, in such cases where information has become available in a public space, law enforcement agents are not restricted by the Fourth Amendment’s search criteria because the person has exposed information in a public manner, effectively surrendering any reasonable expectation of privacy. Per the Supreme Court’s ruling on the topic of police eavesdropping, should law enforcement

³⁹ Gray and Citron, “The Right to Quantitative Privacy,” 93.

⁴⁰ Matthew De Voy Jones, “The Orwellian Consequence of Smartphone Tracking: Why a Warrant under the Fourth Amendment Is Required Prior to Collection of GPS Data from Smartphones Note,” *Cleveland State Law Review* 62 (2014): 216.

⁴¹ The FBI incriminated Charles Katz by recording his public phone booth conversations through an electronic eavesdropping device. The courts ruled that the phone booth was a protected area where one could expect reasonable privacy, similar to the home. The FBI made a physical intrusion into a “private” space and the search was “unreasonable.”

⁴² David Gray, “The Fourth Amendment in an Age of Surveillance” (Cambridge: Cambridge University Press, 2017): 249.

⁴³ Orin S. Kerr, “The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution,” *Michigan Law Review* 102, no. 5 (2004): 805.

⁴⁴ David Gray, “The Fourth Amendment in an Age of Surveillance,” 78.

officers intercept information, leads, or observe actions in a public space, they have done so lawfully.

Along the same lines, the “third-party doctrine” holds that the Fourth Amendment does not protect information the government may access through a third party. For example, the NSA’s Section 215 metadata collection program is constitutionally justified under the third-party doctrine, as people do not have a reasonable expectation of privacy in call records generated by telecommunications providers.⁴⁵ As information is shared with a third party voluntarily, a “search” under the Fourth Amendment has not taken place. Lastly, the Katz ruling changed antecedent rules pertaining to Fourth Amendment standing. In order to meet the constitutional requirement of presenting a “case” or “controversy,” federal courts must demonstrate that they have “standing.”⁴⁶ Updated rules governing Fourth Amendment standing heavily constrain who can challenge government searches, how individuals or groups of people can challenge institutional search and seizure programs, the evidence required for a Fourth Amendment standing, as well as the types of remedies that can be pursued.⁴⁷

In an age of ubiquitous technology in which embedded surveillance techniques are complex and interconnected, the Supreme Court acknowledges the challenges in invoking the Fourth Amendment’s critical role in protecting privacy. In the 2012 landmark case *US v. Jones* pertaining to digital means of evidence gathering, the quantity of data collected was the overarching issue insofar as it grossly surpassed the data collection relevant to the case.⁴⁸ The courts considered the “mosaic theory,”⁴⁹ which focuses solely on aggregation and asks whether or not a large number of isolated non-searches (not requiring a warrant), when examined in the aggregate, can constitute a search if the data reveal a “mosaic.” As such, because the location of Jones’ vehicle was collected around the clock for four weeks, the terms of the warrant had been violated.⁵⁰ While a handful of Justices detailed in their opinions on the case to their growing disquietude about modern surveillance and Fourth Amendment rights,⁵¹ they postponed outlining the types of adjustments they would prescribe and how they may be justified and applied under the law to a more appropriate case in the future.⁵²

Although Katz widened the scope of what constitutes a search under the Fourth Amendment, the public observation doctrine and the third-party doctrine impede the efficacy of the law’s ability to protect against pervasive surveillance. The objective legal standard maintained by the Fourth Amendment described here stands in sharp contrast to actual sociological expectations of privacy. In instances where surveillance tools gather data in public spaces and intercept information through “surreptitious eavesdropping,”⁵³ the government is

⁴⁵ David Gray, “The Fourth Amendment in an Age of Surveillance,” 89.

⁴⁶ David Gray, “Collective Standing under the Fourth Amendment,” *American Criminal Law Review* 55 (2018): 86.

⁴⁷ *Ibid.*, 78.

⁴⁸ *Ibid.*, 90.

⁴⁹ The “mosaic theory” in legal scholarship seeks to determine whether the aggregate personal information collected about an individual during an investigation violates their reasonable expectation of privacy.

⁵⁰ *Ibid.*, 91.

⁵¹ Gray, “The Fourth Amendment in an Age of Surveillance,” 100.

⁵² *Ibid.*, 101.

⁵³ Nuzhat Chowdhury, “I, Spy (but Only on You): Raza V. City of New York, the Civil Rights Disaster of Religious & Ethnic-Based Surveillance, and the National Security Excuse,” *Columbia Human Rights Law Review* 46, no. 2 (Winter 2015): 317.

arguably exploiting an individual's assumed expectation of privacy.⁵⁴ In the 21st century, the legal standard and sociological expectations are wholly unconnected as a result of the deficiencies of the Fourth Amendment. While the process of normalization described in this paper cannot inform the standard of Fourth Amendment law directly, the law nevertheless creates rules and norms that shed light on how people and institutions behave. Fourth Amendment deficiencies inform and empower surveillance institutions to wield influence over sociocultural expectations of privacy, lending weight to our interpretations during this crucial time.

3.2. *Hypothesis and Methodology*

Modern ICTs' far-reaching capabilities facilitate 21st-century surveillance, as do their corresponding tendency towards exploitation not yet acknowledged by the Fourth Amendment. As technologies fundamental to surveillance practices using big data (e.g., the Internet of Things, smartphones, and cloud computing) win favor among individual and business customers, those who have an economic or political interest manipulate them in order to maintain power over the public. Examining the integration of modern communications technologies within institutional frameworks of policing, national security, and commercial corporations will help us understand this phenomenon.

This paper seeks to contribute to the discourse on *surveillance culture* by interpreting how the Fourth Amendment's limited application has resulted in the normalization of shifting and undefined sociological expectations of privacy. It posits that sociological expectations of privacy are determined at the oscillating intersection of culture, technology, and legal reality, and it aims to answer the following questions: Can shifts in sociological expectations of privacy be explained as the product of normalization? What opportunities exist for reversing this process?

I hypothesize that the aforementioned institutions are creating and facilitating cultural norms related to information collection by implementing surveillance techniques that use big data that develop in sync with data-gathering consumer technologies that are becoming ever more common among the general public. As such, surveillance becomes as ubiquitous as technology, a shift that directly challenges expectations of privacy. I argue that normalization is the most identifiable cultural effect. The process of normalization is twofold: first, through changes in modern communications technologies, and second, through the application of these technologies in institutional surveillance programs unprotected by the Fourth Amendment. Moreover, I hypothesize that sociological interpretations concerning expectations of privacy can oscillate as society becomes increasingly permeated by institutional surveillance mechanisms, complicating the process of normalization and presenting an opportunity for the process to pause or break.

Chapter 4 begins by outlining the risks inherent in advancing ICTs. Chapters 5, 6, and 7 examine how institutions dependent on the aggregation of information collection have

⁵⁴ Chowdhury, "I, Spy (but Only on You): Raza V. City of New York, the Civil Rights Disaster of Religious & Ethnic-Based Surveillance, and the National Security Excuse," 318.

revolutionized their various listening apparatuses by leveraging emerging communications technologies, prompting sociological changes to the expectation of privacy. Specifically, Chapter 5 focuses on the New York Police Department's DAS, Chapter 6 contains an exploration of the National Security Agency's (NSA) Verizon and XKeyscore metadata collection programs, and Chapter 7 critiques Facebook's data-sharing business model. Chapter 8 concludes the paper by looking beyond Facebook's most recent debacles, pointing to a unique opportunity for an oscillation in expectations. This paper's qualitative analysis draws from documents that outline the internal workings of the organizations implementing ICT-based surveillance programs. These include primary documents published by the New York Police Department and the NSA and critical investigative reports published by *The Intercept*, the Associated Press, and the *New York Times*. Sources intended to capture the public effect of these programs include surveys undertaken by the Pew Research Center, which serve to substantiate claims throughout the paper.

Chapter 4

Information Exposure

“Computation, storage, and communications capacity are in the hands of practically every connected person—and these are the basic physical capital means necessary for producing information, knowledge, and culture in the hands of something like 600 million to a billion people around the planet.”

- Yochai Benkler

4.1. Modern Technologies Overview

This chapter identifies the modern information technologies that expose user information, as well as how and why they do that, and it explains what makes a technological design or mechanism dangerous from a privacy perspective. The most critical features that modern technologies have in common are their connections to computing systems and webbed networks, which, by design, constantly produce data about all inputs and outputs. In other words, a computer is a record-keeping machine that documents every action a user takes. Once connected to the Internet, the amount of data produced is almost unlimited, including the sites visited, how long the user stays on a site, what the user types in search boxes, what the user clicks on, and so forth.⁵⁵ Modern technologies discussed in this thesis are dependent on the relationship between computers, the Internet, and data.

Increasingly, 21st-century American society is co-existing with computers. For example, smartphones are computers; their apps constantly produce and transfer data, GPS sensors pinpoint a user’s exact location, and all networked devices produce and store an unimaginable amount of data and metadata.⁵⁶ In-store purchases, unless paid for by cash, use computers to store data about the transaction: what was purchased, the cost, the time, and the bank card used. In New York City, it is unlikely that one can take a walk in Manhattan without being picked up by one of the city’s over 9,000 CCTV cameras operated by the NYPD.⁵⁷ Video camera technology is everywhere—not just city streets—from grocery stores, to apartment lobbies, to smartphones that create and store photos and videos, therefore producing even more data. The list does not quite end there, as computers and tools connected to the Internet that produce and transfer data also exist in the transportation industry (self-driving cars), in the home (smart appliances such as Nest, Alexa, Google Home, etc.), and even health care (FitBit, Apple Health).⁵⁸ The most dangerous aspect of the change from mass communications technologies such as the printing press, radio, and television to modern networked devices is that information is now received and disseminated with a traceable and identifiable record.⁵⁹

⁵⁵ Bruce Schneier, *Data and Goliath : The Hidden Battles to Collect Your Data and Control Your World* (New York, N.Y.: W.W. Norton & Company, 2015), 11.

⁵⁶ *Ibid.*, 12.

⁵⁷ Levine et al., “The New York City Police Department’s Domain Awareness System,” 74.

⁵⁸ Schneier, *Data and Goliath : The Hidden Battles to Collect Your Data and Control Your World*, 12.

⁵⁹ *Ibid.*, 17.

4.2. Metadata Collection

Metadata has become an indispensable component of modern data collection. In its most elementary definition, “metadata is data about data.”⁶⁰ In the example of email communications, everything from a sender’s address to the receiver’s address, message size, and time sent are some types of metadata that can be collected. Metadata encompasses all of the data surrounding communications, except content⁶¹—information that is arguably equally, if not more, revealing than content itself. Some scholars assert that while metadata has been widely accepted to define the collection of telephony data under NSA’s Section 215 program, discussed later in this paper, the definition is somewhat exclusive of other types of metadata collection that can occur within networked communications, for example, text message metadata, which in some NSA programs also encompasses machine-derived content.⁶²

Metadata surveillance has become far more useful to those collecting data than the actual topics discussed in a communication, or the “about” content of collected data.⁶³ Since the “about” content requires contextual analysis to be useful, metadata maps the patterns of behavior of an individual.⁶⁴ Machine analysis of collected metadata can reveal insights into connections and patterns of behavior⁶⁵ as the quantity of data becomes more valuable than the content of any single conversation. Such aggregation can paint a telling portrait of one’s patterns of association, however misleading or misinterpreted, and can still be used by law enforcement to build a case or by private corporations for the purposes of targeted advertising.⁶⁶

4.3. Data Storage Capacity

As data is constantly produced through computing devices such as smartphones, cameras, and wireless network sensors, data sets also grow constantly. The amount of data created every day in 2015 exceeded 2 quintillion bytes, with the number growing every day.⁶⁷ As the sheer volume of data produced by Internet-connected ICTs increased in the 21st century, the only way business models and government programs based on data and metadata collection could thrive was through parallel advances in storage capacity. Moore’s law posits that the processing power of a central processing unit (CPU) and disk drives doubles approximately every 18 months.⁶⁸ Furthermore, as data continues to accumulate from a wide variety of sources and databases, data

⁶⁰ Margaret Hu, “Metadeath,” in *In Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair*, ed. Russel A. Miller (Cambridge: Cambridge University Press, 2017): 229–56.

⁶¹ *Ibid.*, 235.

⁶² Katherine J. Strandburg, “Membership Lists, Metadata, and Freedom of Association’s Specificity Requirement,” SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, December 15, 2014), <https://papers.ssrn.com/abstract=2538639>.

⁶³ Gray, “The Fourth Amendment in an Age of Surveillance,” 265.

⁶⁴ Hu, “Metadeath,” 236.

⁶⁵ *Ibid.*, 237.

⁶⁶ Strandburg, “Membership Lists, Metadata, and Freedom of Association’s Specificity Requirement,” 329.

⁶⁷ C.L. Philip Chen and Chun-Yang Zhang, “Data-Intensive Applications, Challenges, Techniques and Technologies: A Survey on Big Data,” *Information Sciences* 275 (August 2014): 315.

⁶⁸ Chen and Zhang, “Data-Intensive Applications, Challenges, Techniques and Technologies: A Survey on Big Data,” 318.

“preprocessing” tools designed for cleaning, reducing, integrating, and transforming data are continuously evolve to remedy messy and patchy datasets.

4.4. Risky by Design: Investigating Design, Processes, and Features

4.4.1. Closed Source or Proprietary Code

The development of broadband infrastructure hardware runs parallel to digital infrastructure, or software development. Whereas computer hardware in the form of motherboards, data storage, graphics, and sound cards constitutes the physical make-up of a computer system, software programs tell or direct a machine to carry out a set of instructions.⁶⁹ Software programs regulate a computer’s functionality; in other words, hardware has little to no value without instructions that tell the computer what to do.⁷⁰ Users’ levels of digital literacy, as well as their access to information in the form of a basic conceptualization of a piece of software’s behind-the-interface functionality, wield enormous influence over their experience and agency while interacting with emerging technologies.

Critical debates and lawsuits between Microsoft, Apple, and AOL in the 1990s were principally concerned with the availability of software source code.⁷¹ Whereas closed-source software programs such as Microsoft Office, Adobe Suite, and McAfee Anti-Virus do not publish their source code, open-source programs do. Open-source programs allow average users to view, alter, and enhance the source code to meet their specific needs. Moreover, open-source programs are free and can be widely shared with anyone for any purpose. While open source software is a development methodology, Richard Stallman highlights the differences between open source and the idea of “free software.”⁷² Stallman argues that free software is a social movement, and that “free/open software advocates and media activists recognize software’s double life as integral to safeguarding certain notions about openness, laterality, and by implication, democratic uses and applications of ICTs.”⁷³

The lack of access, knowledge and literacy of source code, perpetuates a cycle by which closed-source programs collect user data. As users increasingly expect a web experience more tailored to their region, data collection, and customized experiences all around the Internet of Things, the corporate economy of the net flourishes. The prioritization of user interests and user capabilities as a way of respecting user privacy is critical to the open-source model, without which control remains outside the grasp of the user.

⁶⁹ M.I. Franklin. *Technologies for Choice* (New York: Oxford University Press, 2013), 35.

⁷⁰ *Ibid.*, 83.

⁷¹ *Ibid.*

⁷² *Ibid.*, 82.

⁷³ *Ibid.*, 84.

4.4.2. Cloud Storage

As briefly introduced above, data sets are growing with new sources, and computing and communications technologies are converging with minimal distinction between the three industries of computing, communications, and storage systems.⁷⁴ Personal computers and smartphones have a built-in storage system, with built-in memory and options for free cloud storage. For example, Microsoft OneDrive offers 15 gigabytes of free storage, and Baidu Cloud offers two terabytes.⁷⁵ There is no longer a need for modern-day ICT users to invest in pricey computing systems with a large amount of memory or storage capabilities because a relatively small device, once connected to a cloud, can help users gain access to anything they may need. While there are open-source hosting services, the trend set by industry leaders to build and market private clouds has become the norm. These cloud systems, owned and operated by private corporations, are effectively out of the control of their end users, who not only lack control but also infrastructure awareness and process.

Early 20th-century databases fingerprinted the incarcerated, conducted psychological screening tests for those enlisted in military services, and organized income tax collection for working citizens.⁷⁶ Within these models, data was collected and stored through an analog system with no data or industry cross-over with respect to how and where the data was stored. In the 21st-century model, cloud computing and data storage are centralized and outsourced to the cloud.⁷⁷ On the one hand, as with any emerging technology, there are advantages to cloud storage models: End users—from students and researchers to government and non-governmental organizations dealing with large amounts of data sets—are unconcerned about how and where to store their data, virtually eliminating the need to spend money on external hardware. On the other hand, there are major security risks associated with cloud storage infrastructure as well as uncertainties about how outsourced data is being used or commercialized. In sum, as the cloud storage model only makes the external-facing infrastructure visible, it separates end users from its operational infrastructure, which is built upon remote machines,⁷⁸ and ultimately ceases end users' control over the fate of their data.

4.4.3. ICT Convergence and Privacy

ICT convergence occurs when emerging technologies intersect with previously defined industry boundaries.⁷⁹ In this section, we address how ICT convergence drives the trend of diminishing privacy and brings formerly disparate technologies together in networked and connected ecosystem.

⁷⁴ P. Fan, "Coping with the Big Data: Convergence of Communications, Computing and Storage," *China Communications* 13, no. 9 (September 2016): 203.

⁷⁵ Martin Hilbert, "Big Data for Development: A Review of Promises and Challenges," *Development Policy Review* 34, no. 1 (January 2016): 157.

⁷⁶ Hilbert, "Big Data for Development: A Review of Promises and Challenges," 159.

⁷⁷ C. Wang et al., "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in *2010 Proceedings IEEE INFOCOM*, 2010, 1.

⁷⁸ Fan, "Coping with the Big Data: Convergence of Communications, Computing and Storage," 711.

⁷⁹ *Ibid.*, 723.

Convergence as a phenomenon has promoted change within various industries,⁸⁰ namely, the merging of technological mechanisms, including ICTs, forming a trajectory in which the bundled services outperform their capabilities as individual entities. For example, a smartphone in 2018 contains technologies that would only have been found in many separate devices only 30 years ago. This process is twofold: It encompasses the convergence of knowledge bases as well as that of technologies, and it is made possible by the modernization of ICTs.⁸¹ At one point in time, the phone line was the apparatus through which one would access the Internet, whereas in 2018, the Internet is used to access the phone and its other connected features.⁸² The declining cost of ICT components is one of the critical forces driving convergence. In the 1980s, for example, joining CPUs and wireless communications technologies on the same chipset offered a combined product unit that functioned better and more efficiently than the two components individually. In other words, as the costs for parts drop, connecting technologies becomes more cost effective than keeping them independent.⁸³ A natural reaction of corporations was to adapt to this model of convergence, where a company concerned with creating and marketing consumer products would effectively survey and gather information from industries that would initially appear unrelated, such as the health, software, and service industries.⁸⁴ The convergence of technologies, as well as new synergies between industries, correlates to unique possibilities for an ICT. Emerging technologies are invented, evolve, and spread, whether as consequences of organizational goals, an effort to establish industry standards, or even a response to competitors, and convergence becomes a self-perpetuating process.

Convergence has been most concentrated in the modern smartphone, as mentioned above. With so much attention focused on its development, the smartphone contains elements of a variety of other technologies, such as telephones, cameras, GPS, web browsers, language translators, CD players, flashlights, alarm clocks, gaming consoles, location trackers, stethoscopes, among others, thanks to the combination of user demand and the promise of connecting analog technologies to the Internet. For example, an analog alarm clock is a fundamentally different technology than the digital version that tracks the quality and duration of a user's sleep and suggests a bedtime, storing this information in a remote cloud. These services have converged in this device because of the commercial potential offered by the data that people produce when using a formerly "airgapped" technology on an Internet-connected platform.

Symbiotically, convergence lays the groundwork for the creation of hybrid applications, such as a camera app that seamlessly shares users photos with their friends. The camera industry needs to react to consumer preferences that did not exist previously. For example, they have to decide whether to embed similar technology into their digital cameras or to pivot and market their cameras to photography connoisseurs only. In the telecommunications industry, companies have to decide how to react to the increased demand for bandwidth to send photos. They also have to determine whether or not business, military, and consumer customers have different demands compared to one another. Convergence provokes changes that ripple across industries,

⁸⁰ Fan, "Coping with the Big Data: Convergence of Communications, Computing and Storage," 723.

⁸¹ *Ibid.*

⁸² *Ibid.*, 725.

⁸³ *Ibid.*

⁸⁴ *Ibid.*, 726.

disrupting hardware as well as service models. Toward that end, the hardware of smartphones, as well as laptops, has improved dramatically in terms of screen size, resolution, brightness, memory size, and computing power.

The process of convergence, in which previously isolated and independent technologies begin to share fundamental design properties and functionality, explains many of the changes in electronics products during the past few decades. Generally, when knowledge bases converge, technologies come together—synergies that are often driven by dynamics internal to the companies that produce them. As a result, the consumer experiences new combinations of previously separate technologies as novel and unexpected opportunities for communication and entertainment. Moreover, as industrial convergence is cemented, the boundaries between areas of technological expansion and growth disappear, and major markets such as consumer electronics, military tools, software, data-processing, and telecommunications become blended.⁸⁵ As technologies are concentrated, the duration of time and the variety of ways in which people interact with their devices increase, inherently generating more data and metadata used for gaining insight into customer behavior as well as for surveillance.

Convergence also creates more detailed and accurate data as more technologies are connected to the Internet and, by extension, connected to platforms that gather data and enhance their collection practices as part of their business models. Therefore, ICT convergence is helpful for surveillance since ICTs are producing and transmitting data that is richer in quality and specificity at all times. Whereas a car was once a metal box with seats and wheels, in 2018, a car is a computerized vehicle that produces and disseminates data about where one is going, when, how fast, and so on, qualifying its collected data for reuse later. Returning to the central argument that these technical changes somehow manifest themselves in social and cultural changes in American society, we hypothesize that this occurs through the institutional adoption and exploitation of changing technologies and their ability to gather, store, and analyze richer data sets—without user consent and, with respect to the Fourth Amendment, without a requirement for a search warrant. As ICTs become increasingly ubiquitous and accessible, these technologies, similar to those available in consumer markets, symbolically reflect the motives of their users.

Pervasive surveillance programs are undefined and complex; they are simultaneously covert and overt, and they exist and thrive in current networked and digitally dependent settings that feed information collection-based business models. Under the surveillance agenda set forth in the aftermath of 9/11, both government and private-sector interests mobilized to monopolize social control.⁸⁶ The surveillance society is supported by this transformation of information flows in which information is a lucrative commodity that simultaneously expedites communication and optimizes the targeted dissemination of goods and services.⁸⁷ Therefore, as emerging and efficient ICTs have connected industries that collect and analyze data, surveillance has become a function of the technologies that organizations use, and society has henceforth reorganized

⁸⁵ Fan, “Coping with the Big Data: Convergence of Communications, Computing and Storage,” 726.

⁸⁶ C. William R. Webster, “Surveillance as X-Ray,” *Information Polity: The International Journal of Government & Democracy in the Information Age* 17, no. 3/4 (September 2012): 254.

⁸⁷ *Ibid.*

around this purpose to the detriment of the public interest.⁸⁸ The next section outlines how the existence and use of the aforementioned technological norms and standards empower surveillance programs that, by design, violate earlier privacy norms rather easily. It also explains how and why the new surveillance programs at various levels of socio-political power (e.g., the NYPD, the NSA, and Facebook) could not have occurred without the technological changes presented in this section.

⁸⁸ Webster, "Surveillance as X-Ray," 255.

Chapter 5

Changes Manifest Themselves: The New York City Police Department's Domain Awareness System

“CCTV is seen either as a symbol of Orwellian dystopia or a technology that will lead to crime-free streets and civil behavior. While arguments continue, there is very little solid data in the public domain about the costs, quantity, and effectiveness of surveillance.”

- Heather Brooke

Changes in ICTs have equipped police departments across the nation with tools to collect data on citizens, including those who are not under investigation, on an unprecedented scale in terms of volume and breadth. While public surveillance is a legitimate tool for the police department to employ, this chapter examines the New York City Police Department's (DAS)—a mass surveillance model that has generated substantial Fourth Amendment-related concerns. Public policing once required police officers to physically surveil an individual, a group of people, or a location for a specific period of time; this model has become obsolete in present-day policing, which consists of constant, remote, and limitless surveillance. Though the police department was once restricted by limited access to resources to generate more efficient surveillance techniques, technological convergence and industry overlap have facilitated mutually beneficial partnerships between the NYPD, Microsoft, IBM, and others, thus cementing a successful and lucrative 21st-century surveillance industry.

The NYPD has a long history of using applied analytics to maximize the efficiency and effectiveness of officers on the ground. In 1993, the NYPD implemented CompStat, a collection of maps that charted crime, to share information between officers, improve their performance, and also hold officers accountable for their work.⁸⁹ Expanding from CompStat, the DAS is the newest data collection analytics program, disseminating “research” to help both officers in the field and in the precinct make decisions.⁹⁰ The police department puts decision making into two categories: tactical and strategic. The first type must be on the spot and quick, often a matter of minutes or seconds. The second type requires more time, a case that is larger in scope and requires a strategy.⁹¹ The DAS, comprised of a network of sensors, databases, devices, software, and infrastructure, delivers tailored information and analytics to mobile devices and desktops, and it assists with both types of decision making. In 2013, DAS software was initialized in everyday policing structures, and in 2014, a mobile version was optimized for smartphones and tablets. As of 2016, every one of the NYPD's 36,000 officers had a smartphone device with the DAS.⁹²

This section closely examines two features of the DAS: CCTV camera surveillance and license plate readers (LPR) and their relationship to predictive technologies.

⁸⁹ Levine et al., “The New York City Police Department's Domain Awareness System,” 70.

⁹⁰ Ibid., 71.

⁹¹ Ibid.

⁹² Ibid., 73.

5.1. Closed-Circuit Television Cameras (CCTV)

As of 2017, the DAS connects to 9,000 CCTV cameras across New York City, which are owned and operated by both the NYPD and private-sector entities such as the New York Stock Exchange.⁹³ The NYPD uses video analytics on some of these cameras to trigger automated alerts when cameras detect suspicious behavior, such as the movement or appearance of a suspicious package. According to a 2017 publication by the NYPD describing the DAS, video analytics algorithms use background subtraction to compare an image to another time-averaged image and generate an alert when an object the size and shape of a package is motionless for a period of time.⁹⁴ The department's policy states that video camera surveillance footage is kept for 30 days unless the footage is critical to an investigation, but questions persist about what happens within those 30 days or what third parties are able to do with the same footage. It is also worth mentioning that the publication did not disclose that the footage is intricately tagged and able to identify human subjects based the color of their clothing or height. However, in press coverage of an unrelated tour of the Lower Manhattan Security Coordination Center in 2011, this feature was specifically mentioned in a reference to the system's ability to search by "people wearing red shirts,"⁹⁵ which raises concern about the department's vague and obscure approach to sharing information about the DAS with the public.

The DAS is simultaneously covert and overt. On the one hand, it is public knowledge that the DAS is a system employed by the NYPD for policing comprised of a number of technical components. On the other hand, however, the institution does not disclose how it shares data with industry partners such as IBM, what is done with the data, how information is retained, and so on. A 2018 investigation conducted by *The Intercept* revealed IBM's use of the NYPD's CCTV-generated footage to develop technology capable of tagging skin color.⁹⁶ The algorithm processed images with differing light quality and environmental features to perfect itself through machine learning. The investigation revealed that, in 2012, IBM tested this software on human subjects captured on CCTV systems and searched camera footage by using new identification features such as hair color, age, gender, and skin tone.⁹⁷ While the NYPD has officially severed ties with IBM and repeatedly emphasized that these analytics were only used for testing and evaluation purposes, this form of collaborative, covert, pervasive watching effectively perpetuates a cultural norm of diminished privacy through public-private partnerships facilitating unregulated data surveillance.

As novel technologies emerge, surveillance techniques simultaneously advance and adapt. In this case, CCTV surveillance infrastructure expands both in the quantity and quality of video cameras and as a tool connected to a greater database. The next step involves refining and expanding the types of identification features the technology consumes. In other words, the changes in data extraction and big data policing techniques through CCTV cameras could not

⁹³ Levine et al., "The New York City Police Department's Domain Awareness System," 73.

⁹⁴ *Ibid.*, 75.

⁹⁵ George Joseph and Kenneth Lipp, "IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color," *The Intercept*, September 6, 2018, <https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/>.

⁹⁶ Joseph and Lipp, "IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color."

⁹⁷ *Ibid.*

have occurred without the changes in remote camera technology and the various ways camera technology can be used. For example, in the *Kyllo v. United States* case, law enforcement agents used a thermal imaging device to track heat patterns in a home suspected of growing illegal marijuana plants.⁹⁸ The court ruled that monitoring radiation constituted a search under the Fourth Amendment, which NYU privacy law professor Katherine Strandburg affirms by stating that “the increasing intrusiveness of video surveillance is primarily a result of technological advances. Video devices have become cheaper, smaller, and easier to hide, and video recordings easier to store and to search, thus making conventional social behavior more amenable to surveillance.”⁹⁹

This speaks to how surveillance programs such as the DAS were able to violate earlier Fourth Amendment privacy norms. Without regulatory protections against ubiquitous surveillance through the use of a number of technologies, privacy perpetually diminishes, as lawmakers lack hard a consensus on how the Fourth Amendment can or should address evolving location-tracking and imaging technologies. On the topic of vehicular tracking, Judge Posner comments, “[s]hould government someday institute programs of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search.”¹⁰⁰ In contrast, Judge Kozinski represents five judges in his long-form dissent:

There is something creepy and un-American about such clandestine and underhanded behavior. To those of us who have lived under a totalitarian regime, there is an eerie feeling of déjà vu. This case, if any, deserves the comprehensive, mature and diverse consideration that an en banc panel can provide. We are taking a giant leap into the unknown, and the consequences for ourselves and our children may be dire and irreversible. Some day, soon, we may wake up and find we’re living in Oceania.¹⁰¹

The enshrinement of sociocultural change in the form of diminishing privacy through ubiquitous technology is a process. Here, the process involves a change in technology through the convergence and dissemination of computer-connected video cameras as accessible consumer goods. This process then complicates the standards and norms of video technology as it becomes widely accessible because virtually anyone in a public space can capture and share video footage. Thus, its subsequent institutional application within a system like the DAS desensitizes society to the technology as an all-seeing surveillance tool. Video camera technology in a smartphone or laptop is able to create, collect, watch, save, and transfer footage, both in the form of content created by its user and content another user has made available on an app like Facebook or Snapchat. Similarly, the NYPD uses CCTV systems to monitor subway platforms, public parks, and more, an extension of an already accessible technology. In other words, CCTV systems are similar to smartphone cameras with different motives, and the norms of the technology align with the motives of the user.

Programs such as the NYPD’s DAS further weaken the expectation of privacy in public spaces by explicitly linking its technical features back to the idea that access to instant databases

⁹⁸ Katherine J Strandburg, “Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change” 70 (n.d.): 615.

⁹⁹ *Ibid.*, 630.

¹⁰⁰ *Ibid.*, 649.

¹⁰¹ *Ibid.*

connected to CCTV systems will provide more safety and security. The contrapositive is also implicitly promoted—that *not* implementing emerging technologies would constitute an irresponsible negligence on behalf of law enforcement. Although all of the above may be true, a lack of transparency about data collection, processing, and transferring contribute to changing expectations of privacy in the public sphere. Furthermore, the closed-source models of information collection and processing leave the public in the dark about what is happening with their data and how.

The simultaneous adoption, growth, and use of these technologies in policing, following the growth and use of “smart” and “handheld” consumer technologies, all degrade expectations of privacy. As harnessing the capabilities of data-surveillance technologies means pervasive public surveillance to monitor and catch a crime as it occurs or before it occurs, there is little to no privacy or freedom to exist and behave as individuals free from other people listening and watching.

5.2. *License Plate Readers (LPRs)*

In addition to CCTV systems, the DAS connects to an organization of license plate readers comprised of at least 250 mobile detectors on police vehicles and at least 50 detectors covering traffic in and out of Manhattan via bridges and tunnels.¹⁰² The sensors are small and mountable; in addition to reading license plate numbers, they register the date, time, and speed of cars passing by. The LPRs then use optical character recognition to extract characters from each plate and compare them against plates of interest and “hot lists” generated by a number of criminal and terrorist watch lists. Furthermore, LPRs collect data on every car passing by, so much so that “the number of license plates that can be read is limited only by the number of vehicles passing the cameras.”¹⁰³ Moreover, LPRs feature automated pattern recognition and predictive analytics algorithms to inform officers where and when a plate of interest is most likely to be scanned in the near future. These custom algorithms search for two patterns: time and place, and routing, a feature that the NYPD maintains is only used to monitor vehicles on a “hot list.” Pattern recognition and predictive analytics are useful forecasting tools that can identify the future location of a suspicious vehicle more efficiently, and officers can use them to instantly access data about the history of the plate through the DAS, which retains its scans for five years. Moreover, the forecasting feature also makes interdiction much more efficient, eliminating the need for field officers to monitor the vehicle over an extended period of time or install a GPS tracking device.

Similar to CCTV cameras, other changes in technology seem intuitive because they are linked to the proliferation of camera and video technology, which society experiences through its increasing availability in consumer electronics. According to a Pew fact sheet about Americans and their Smartphones published in 2015, 92% of respondents were using their smartphones for voice and video calling, and 60% of respondents were using their phones for their photo and

¹⁰² Levine et al., “The New York City Police Department’s Domain Awareness System,” 71.

¹⁰³ “Automatic License Plate Readers,” New York Civil Liberties Union, July 23, 2015, <https://www.nyclu.org/en/automatic-license-plate-readers>.

video features.¹⁰⁴ Again, LPRs contribute to this discussion because they are related to the proliferation of camera technology. As people increasingly possess devices with this capability, they are more accustomed to being recorded because they also record or, at the very least, have access to the technology to do so. In that vein, it is not solely the NYPD or the DAS that normalize the idea of pervasive surveillance; rather it is a question of how the police department as an institution concerned with policing is implementing and disseminating modern ubiquitous technology, creating a powerful and penetrating sociological norm of less or diminished privacy. Furthermore, the change in cultural standards that imply voluntary or even spontaneous public disclosure of private information with respect to the promptness in “providing personal information and the fascination with the personal aspects of other people’s lives is partly a heritage from the more liberal spirit of the 1960s.”¹⁰⁵ However, this trend also reflects the need that modern people have, when in the ubiquitous presence of cameras and similar means, to see and be seen, to know and be known.¹⁰⁶

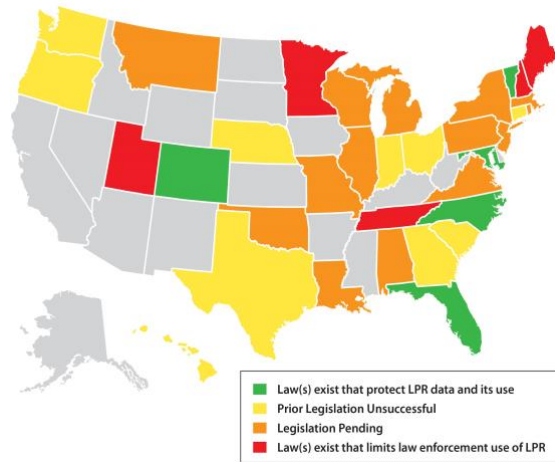


Figure 1. Image from Vigilant Solutions Article “Protect LPR With Positive Legislation”

The normalization of data surveillance by the NYPD as a means of ensuring safety and security as part of the “war on terror” agenda ultimately shapes how these ICTs are understood and experienced. Surveillance can be identified as a “factor of production” whereby society is organized around norms that enhance data surveillance, such as video camera tracking capabilities, which simultaneously normalize day-to-day surveillance as an element of modern society.¹⁰⁷ Camera and video technologies and the various activities linked to them normalize surveillance in public spaces, and “citizens willingly [acquiesce] as surveillance subjects [as] greater levels of surveillance are often portrayed as an acceptable cost for enhanced levels of security.”¹⁰⁸

The breadth of LPRs’ capacity within the DAS does not quite end there. In 2016, the NYPD and Vigilant Solutions signed a contract that would permit the NYPD to use Vigilant’s database.¹⁰⁹ Vigilant Solutions is a private company with a database of billions of LPR records collected from both private and law enforcement readers all across the United States. Vigilant’s database grows by 80 million data points per month, and the contract enables the NYPD to trace vehicles, locations, and travel patterns all around the country, including residential and

¹⁰⁴ Monica Anderson, “6 Facts about Americans and Their Smartphones,” *Pew Research Center* (blog), accessed January 4, 2019, <http://www.pewresearch.org/fact-tank/2015/04/01/6-facts-about-americans-and-their-smartphones/>.

¹⁰⁵ Fábio Rafael Augusto and Maria João Simões, “To See and Be Seen, to Know and Be Known: Perceptions and Prevention Strategies on Facebook Surveillance,” *Social Science Information* 56, no. 4 (December 1, 2017): 600.

¹⁰⁶ *Ibid.*

¹⁰⁷ Webster, “Surveillance as X-Ray,” 254.

¹⁰⁸ *Ibid.*, 255.

¹⁰⁹ “Automatic License Plate Readers,” New York Civil Liberties Union.

commercial complexes.¹¹⁰ As an organization committed to the safety and security of New Yorkers, why, then, is the police department interested in a nationwide LPR database? This question is larger than motives and intentions. If access to a database exists, the question becomes “why not?”, as the collection and storage of data points is now the default approach to information collection. The DAS’s newest collaboration is another instance of technological convergence and industry blurring.

Additionally, as seen in Figure 1, the legal realm hosts spirited debate about the use of such devices, as the interests for and against increasing surveillance technology square off. Powerful institutions such as the NYPD wield their influence in this debate, as Vigilant Solutions credits the “coordinated efforts of its law enforcement partners” in the fight to ensure that LPR collection and storage avoids legislative limits to its operation. Industry players benefit from the fact that it is “well established in the courts that there are no 4th Amendment implications in the use of LPR,”¹¹¹ and as long as the debate is centered around the public feeling secure, the argument that more surveillance equals more safety will drive support for increased implementation of LPR and similar technologies.

Collecting, coding, searching, and storing data from both CCTV systems and LPRs by police departments and their corporate sponsors also create the risk of an information monopoly or a bias of communication.¹¹² Data storage comes with risks, such as too much, too little, or inaccurate data, and policing records notoriously contain much data “just in case,” which can easily prejudice the legal process.¹¹³ Additionally, innocent “people may not be aware of records held on them or may be unable to check them.”¹¹⁴ In sum, normalized surveillance in the public policing model is the effect of a process through which commonplace technologies serve the interest of their most powerful users, which creates and perpetuates a sociocultural norm of surveillance inherent within society. In addition to the reducing the costs of owning a video camera, technical advancements in big data, primarily their ability to aggregate and query a database, add to this change. Although the traditional CCTV models were dependent on law enforcement officers monitoring screens and footage to detect danger, the current model depends on algorithmic technologies to tag and organize footage in an effort to make it instantly accessible and searchable. The changes in the police department’s surveillance apparatus is facilitated by innovate technologies, the same technologies used by average citizens to connect with one another.

¹¹⁰ “Automatic License Plate Readers,” New York Civil Liberties Union.

¹¹¹ Brian Shockley, “Protect LPR With Positive Legislation,” Vigilant Solutions, April 28, 2016, <https://www.vigilantsolutions.com/protect-lpr-with-positive-legislation/>.

¹¹² Lyon, *Electronic Eye: The Rise of Surveillance Society*, 47.

¹¹³ *Ibid.*

¹¹⁴ *Ibid.*

Chapter 6

Edward Snowden and The National Security Agency

“What we've seen over the last decade is we've seen a departure from the traditional work of the National Security Agency. They've become sort of the national hacking agency, the national surveillance agency. And they've lost sight of the fact that everything they do is supposed to make us more secure as a nation and a society.”

- Edward Snowden

The collection of “Snowden documents” reveals in detail that the NSA’s surveillance activities have transformed the use of communications networks into an environment in which the agency can monitor and intercept all activity and interactions through communications infrastructure not only in the United States but around the world. In some cases, the programs operate with the conscious cooperation of private actors, while in others, companies are unaware that the NSA redirects their data for its overreaching surveillance efforts. The omnipresent nature of the NSA’s listening apparatus impinges upon citizens’ privacy in connected and unconnected social spheres—a right we previously, and should presently, retain fully under Fourth Amendment protections from search and seizure, as personal data arguably falls under the scope of “personal effects.”

The NSA’s legacy of metadata collection has contributed to a societal change in which surveillance is the status quo, Fourth Amendment rights are compromised, and anonymity and autonomy are becoming historical remnants. The use of information technology tools to capture data and metadata in aggregate is a critical characteristic of the NSA’s modern surveillance efforts and thrives in two ways: First, the NSA leverages the sociopolitical and economic influence it maintains with private companies that own communications infrastructure.¹¹⁵ Second, due to the breadth and scope of its surveillance programs, the NSA contracts its technical intelligence efforts to private firms such as Booz Allen Hamilton.¹¹⁶ In 2013, for example, approximately one million people held top-secret security clearance to gather and work with information about citizens in the U.S. and abroad, so long as the monitoring fell under the umbrella of national security threats.¹¹⁷

Modern NSA surveillance would not be possible without the ability to allocate tens of millions of dollars¹¹⁸ to buying data directly from Internet service providers (ISPs), otherwise known as data mining.¹¹⁹ Therefore, the federal government’s failure to regulate data mining perpetuates the unfettered collection of data by corporate actors. The NSA’s engagement in contractual agreements with such actors then reinforces the asymmetric balance of power

¹¹⁵ Philip N. Howard, *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up* (New Haven: Yale University Press, 2015), 23.

¹¹⁶ *Ibid.*

¹¹⁷ *Ibid.*, 24.

¹¹⁸ In 2006, \$30 million USD had been spent by the General Accounting Office arranging contractual deals with information resellers.

¹¹⁹ Howard, *Pax Technica*, 25.

between those whose data is mined and the government,¹²⁰ a phenomenon similar to the public policing model discussed in the previous chapter. In cases where a third party does not respond to electronic surveillance record orders from the NSA, the NSA has taken upon it itself to “install a hardline tap in their server room,” as in the case of AT&T’s Room 641A.¹²¹

Snowden’s revelations incited public outcry, along with legal debate surrounding the extent to which constitutional protection against bulk metadata collection regulated those charged with regulating such activity (i.e., Congress). While we depend on the Fourth Amendment to protect the civil liberties of American citizens, and despite minor advancements¹²² in defending such protections, the onset of sophisticated surveillance technology has exposed shortcomings in its 21st-century application. Along the same lines, since its inception, the evolution of the NSA’s surveillance program has revealed a notable shift toward increased private-sector participation in expanding surveillance practices, creating a space in which the capabilities and databases of private companies can serve as resources for program’s original motivations. This chapter examines Section 215 of the Patriot Act and XKeyscore, two NSA programs built upon bulk metadata collection, underlining the technologies that make them possible as surveillance programs and how these changes simultaneously challenge and normalize this model of government surveillance.

6.1. NSA Section 215 Bulk Metadata Collection Program and XKeyscore

Under Section 215 of the 2001 PATRIOT Act,¹²³ government-sanctioned bulk surveillance programs collecting global telecommunications data required, and often received, authorization from the Foreign Intelligence Surveillance Court (FISC).¹²⁴ Declassified court orders reveal that the court mandated Verizon, among other major telecommunications providers, to hand over bulk telephony metadata to the NSA, ostensibly representing a record on every American using a mobile phone.¹²⁵ While the USA Freedom Act nominally dismantled the program in 2015,¹²⁶ under the 2008 Foreign Intelligence Surveillance Act (FISA) Amendments Act, the FISC regained the ability to permit bulk metadata collection under Section 702.¹²⁷ In other words, the data produced by any American with “links” to intelligence targets abroad, however tenuous, can be collected without a court warrant.¹²⁸ Among the technical changes that largely contribute to the success of the 215 program is the spread of mobile communications technologies, namely cell phones and, later, networked smartphones, as well as computing capacity to automatically analyze metadata. The Pew’s Mobile Fact Sheet reveals that, in 2014,

¹²⁰ Howard, *Pax Technica*, 25.

¹²¹ *Ibid.*, 26.

¹²² Specifically, USA Freedom Act which replaced the most controversial parts of the Patriot Act.

¹²³ USA PATRIOT Act: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

¹²⁴ Howard, *Pax Technica*, 24.

¹²⁵ David Gray and Danielle Keats Citron, “The Right to Quantitative Privacy,” *Minnesota Law Review*, no. 98 (November 2013): 62-144, <http://bi.galegroup.com/essentials/article/GALE%7CA379736254?u=columbiaiu>

¹²⁶ Howard, *Pax Technica*, 24.

¹²⁷ *Ibid.*, 25.

¹²⁸ *Ibid.*

92% of American adults had access to cell phones, 50% of which were smartphones.¹²⁹ Coupled with Fourth Amendment's third-party doctrine that justifies the program's widespread data collection, the program succeeds in both its wide scope and level of access.

Also revealed in Snowden's 2013 disclosures is information about the NSA's XKeyscore program. XKeyscore is the widest-reaching system for Internet-based intelligence collection, and it is similar to the telephony program in that it collects metadata as well. Training materials for XKeyscore reveal how analysts can use the program together with other systems to mine enormous agency databases. To begin a search, an analyst is required to fill in an on-screen form and enter in a generic justification for the search. The request to access databases and mine data sent in by an analyst is not reviewed by a court or anyone from the NSA before processing. Intelligence gathered from computer networks are called Digital Network Intelligence (DNI), and the XKeyscore documents further reveal that the program covers everything a typical user does on the Internet, including the content of emails, websites visited, and searches, as well as metadata. In addition to this, XKeyscore can be used to intercept and collect user data in real time.

As described in the previous chapter, the NSA's model of ubiquitous surveillance thrives because surveillance of increasingly connected technologies is cheap, and for the first time in the history of surveillance, there are innumerable ways to track, store, and analyze collected data in aggregate. For the NSA, as well as for third parties, cheap metadata surveillance is more useful than "about" content discussed earlier in this paper. "About" content requires a degree of focused and interpretive analysis to be meaningful, whereas metadata about who was called, at what time, and for how long is more revealing when analyzed by a computer and subsequently used to create patterns that reflect a person's lifestyle and interests. For example, in an experiment at Stanford University where the metadata of 500 volunteers was collected over the course of several months, the amount of information revealed shocked the study's researchers.¹³⁰ A stream of metadata was able to determine that, of the experiment participants, one had suffered a heart attack, another had had an abortion, and another was an owner of semi-automatic weapons.¹³¹

Following Snowden's revelations of the NSA's capabilities in 2014, people had a general awareness that using ICTs meant giving up some degree of privacy. In a 2014 Pew survey on government surveillance, 91% of adults agreed that consumers have lost control over how personal information is collected and used by companies.¹³² Of the respondents who used social networking sites (SNS), 80% cited concerns about third parties gaining access to their data via SNS, and another 70% expressed concern about the government's access to information shared on SNS without their knowledge or consent.¹³³ As mobile technologies become increasingly networked, accessible, and ubiquitous, so too does surveillance of these technologies. As underlined by the Pew statistics above, the societal effect of ubiquitous surveillance points to the public's sense of fear and disempowerment as we lose control over our information. However,

¹²⁹ "Demographics of Mobile Device Ownership and Adoption in the United States," accessed January 4, 2019, <http://www.pewinternet.org/fact-sheet/mobile/>.

¹³⁰ Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, 24.

¹³¹ *Ibid.*

¹³² "Public Perceptions of Privacy and Security in the Post-Snowden Era | Pew Research Center," November 12, 2014, <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>.

¹³³ *Ibid.*

mobile technologies continue to evolve in terms of size, features, and even price, and the number of Americans with mobile phones in 2018 has reached 95%, with 77% of those people owning a smartphone.¹³⁴ As theorized earlier in this paper by David Lyon, the social process through which surveillance becomes a cultural norm is a process driven by collaboration. Collaboration between economic, political, and institutional powers, as well as participants in the broader society, increases the user base of mobile technologies, and it further drives the change in expectations of privacy that accompanies the adoption of such technologies.

Society increasingly accepts, uses, depends on, and develops a symbiotic connection to the same devices and platforms that feed the metadata into the NSA's surveillance system in cooperation with the companies that produce and service those devices. This trust persists despite the fact that revelations about the telecommunications industry's role in surveillance emerged almost a decade prior to Snowden's. The Snowden revelations created public awareness of pervasive government surveillance, and to some extent, concern about how the government and social media sites are using people's data. However, there was no identifiable public action in the form of severing ties with companies working closely with the NSA following Snowden's revelations. Neither telecommunications companies nor Internet search engines, email providers, or social media platforms suffered from identifiable public backlash against their services.¹³⁵ General apathy in spite of awareness suggests that the lasting effect of learning that the federal government had collected data, with help from private companies, was a sort of learned helplessness in the face of degradation in expectations of privacy, cemented by a lack of Fourth Amendment protections.

In 2014, in the immediate wake of the Snowden disclosures, telecommunications companies were regarded as more trustworthy than the government, as about 70% of Americans surveyed by Pew stated that they trusted their cell phone company to keep their data private, a group approximately 20% larger than the group that trusted the federal government.¹³⁶ Additionally, Americans were more confident in the ability of private institutions such as telecom platforms, email service providers, and credit card companies to secure their personal data than the federal government. The survey also revealed that 49% of respondents lacked confidence in the federal government's ability to protect their data.¹³⁷ Public outrage and concern following the Snowden leaks did not amount to action, and the aforementioned statistics demonstrating increased levels of trust in private companies are evidence of the process of normalization. In other words, the sociocultural effects of pervasive surveillance demonstrate how surveillance through networked technologies is normalized through convoluted expectations of privacy. Moreover, the process of normalization demonstrates how expectations of privacy can oscillate and how cultural attitudes surrounding privacy and expectations can shift depending on what standards and norms are prevalent in society at a given moment in time.

¹³⁴ "Demographics of Mobile Device Ownership and Adoption in the United States," accessed January 4, 2019, <http://www.pewinternet.org/fact-sheet/mobile/>.

¹³⁵ Lyon, *Electronic Eye: The Rise of Surveillance Society*, 11.

¹³⁶ "How Americans Have Viewed Surveillance and Privacy since Snowden Leaks," *Pew Research Center* (blog), accessed January 5, 2019, <http://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/>.

¹³⁷ *Ibid.*

Social normalization facilitated by the NSA’s model of modern surveillance depends on society’s access to, and use of, ubiquitous technologies such as smartphones. As both access and use continue to grow across the United States, the social expectation of privacy is compromised and shifts from what those in charge of creating legally binding regulations had once sought out to promise (i.e., the federal government) to what those who are in charge of facilitating access to the tools themselves promise to their customers (i.e., private companies). In other words, Americans expect less, or have limited confidence in, the federal government’s ability to protect their data; at the same time, however, Americans have heightened levels of confidence in the service providers themselves. Hence, the Snowden scandal demonstrates an oscillation, a shift that demonstrates that society expects more privacy than what the aforementioned private companies who work alongside the federal government appear to offer.

One explanation for this shift may be that the privacy policies offered by companies are perceived to be less covert and opaque, thus making them seem less conspicuous than those of the NSA. For example, according to the Pew Center’s “Web IQ Quiz” released in December

Q40 When a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users.

True	52%
False (correct)	44%
Did not answer	3%

Figure II. Question from Pew Research Center’s “Web IQ Quiz”

2014 following the Snowden leaks, the majority of respondents answered, incorrectly, that a company’s privacy policy is meant to keep user information private.¹³⁸ Inspired by Joseph Turow, a UPenn communications professor specializing in marketing, media, and privacy, the question sought to measure deeply embedded confusions and

misinterpretations surrounding privacy policies across the web. Turow comments, “Many people don’t actually read privacy policies; they simply look at the label, and the intuitive understanding—the cultural understanding—of the label is that when something says ‘privacy policy,’ it protects your privacy.”¹³⁹ In reality, the privacy policy discloses the terms by which a company stores users’ browsing data, as well as the terms governing how the company shares this information with other entities.

In an age of technological convergence, everything—from social interactions, to shopping, to traveling—requires some level of information disclosure. Revelations about the federal government’s exploitation of networks that store data for mass surveillance has provoked a response from the implicated private-sector companies, specifically Apple, Facebook, Google, Microsoft, and Verizon, among others, as they undertake PR campaigns to portray their companies as being fundamentally concerned with user privacy. Sociological interpretations of privacy, through the process of normalization, have been adapted to accept the level of privacy dictated by private companies as confidence in the federal government and, by extension, the Fourth Amendment languishes. These statistics demonstrate that the most pressing problem of pervasive surveillance and its reach is not necessarily complacency or a lack of adequate knowledge among the greater public; rather, the problem lies in how data surveillance is

¹³⁸ Aaron Smith, “Half of Online Americans Don’t Know What a Privacy Policy Is,” *Pew Research Center* (blog), accessed January 5, 2019, <http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/>.

¹³⁹ Smith, “Half of Online Americans Don’t Know What a Privacy Policy Is.”

normalized as an impenetrable part of modern society. The process of normalization weakens sociological expectations of privacy and subjugates collective action against the federal government's surveillance apparatus as an entity with more disciplinary power than the average citizen.

Chapter 7

Facebook and Algorithmic Surveillance

“Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers.”

United Nations, Universal Declaration of Human Rights

So far, this paper has argued that surveillance has grown intensively and extensively since the early part of the 21st century as a result of emerging data-gathering technologies and the parallel integration of such technologies into institutional surveillance. It demonstrates that the proliferation of surveillance technologies creates everlasting fears with respect to how surveillance is transforming both quantitatively and qualitatively, as well as how a lack of protections rooted in the Fourth Amendment perpetuate this process.¹⁴⁰ As the sphere most responsive to the preferences of the general public, the commercial surveillance model discussed in this chapter presents an opportunity for accountability and for expectations of privacy to oscillate again.

According to Pew data published in 2016, 79% of all adult Americans online (86%) use Facebook, a 7% increase from 2015, making the social media company 47% more popular than the next leading platform, Instagram, which is also owned by Facebook.¹⁴¹ This chapter focuses on the sociological effects created by social media networks, namely Facebook, through its collection, processing, and dissemination of public and private user data. The working model of Facebook surveillance encourages its users to exhibit themselves on the platform so much so that they lose their inhibitions regarding “the type and quantity of information they have made available, as well as of the number of users accessing this information.”¹⁴² Although the platform is built on a model of user transparency that encourages information sharing and exposure, its data use policy is incoherent and paradoxical.¹⁴³ Moreover, the political economy of privacy on Facebook is such that user behavior on the platform is commodified, as Christian Fuchs thoroughly summarizes:

Facebook invests money (M) for buying capital: technologies (server space, computers, organizational infrastructure, etc.) The outcome of the production process P1 is not a commodity that is directly sold, but rather social media services (the Facebook platform) that are made available free to users The Facebook users make use of the platform for generating content when they upload their own data Their products include user-generated data, personal data, and transaction data about browsing and communication behaviors on Facebook Facebook sells the

¹⁴⁰ Augusto and Simões, “To See and Be Seen, to Know and Be Known: Perceptions and Prevention Strategies on Facebook Surveillance,” 597.

¹⁴¹ “Demographics of Social Media Users in 2016,” November 11, 2016, <http://www.pewinternet.org/2016/11/11/social-media-update-2016/>.

¹⁴² Ibid.

¹⁴³ Augusto and Simões, “To See and Be Seen, to Know and Be Known: Perceptions and Prevention Strategies on Facebook Surveillance,” 598.

users' data commodity to advertising clients at a price that is larger than the invested constant and variable capital The difference is that the users are unpaid, and therefore infinitely exploited.¹⁴⁴

Facebook's model could not have been successful without the data-generating characteristics of modern ICTs. Such characteristics enable Facebook to encode and quantify all areas of human interactions, including but not limited to "friendships, interests, casual conversations, information searches, expressions of tastes, emotional responses, and so on."¹⁴⁵ However, as Facebook users become increasingly aware of the risks inherent to Facebook with respect to privacy, freedom of thought, freedom of expression, and democratic ideals that characterize free and fair elections, the corporate model of surveillance is finally experiencing significant challenges. This chapter begins by outlining how algorithmic surveillance, one of the critical technical features of Facebook's surveillance model, normalizes a narrow expectation of privacy on the platform. The subsequent sections examine Facebook's role in the 2016 United States presidential campaign, as well as the 2017 Cambridge Analytica scandal, to arrive at the concluding discussion about how Facebook's corporate model demonstrates people's ability to oscillate expectations of privacy and challenge normalization.

7.1. Data Collection, Algorithms, and Bias

Facebook acts as a neutral facilitator of an exchange of user-generated content. Data and metadata are collected about user-generated content on the platform and later used for various purposes. For example, in 2013, a study revealed how, by studying patterns in the form of users' "Like" history can successfully predict sensitive personal attributes such as age, gender, ethnicity, sexual orientation, ethnicity, religious views, and happiness, among others.¹⁴⁶ Facebook uses these patterns to optimize user experience, but it also dumps critical data to the platforms for later use in both targeted advertising and predicting future behavior. Predicting future behavior by collecting pieces of information on an individual, or "life mining,"¹⁴⁷ is useful for a wide variety of paying public and private partners, including intelligence agencies, market researchers, and think tanks, and it is facilitated by complex algorithmic analysis.

Algorithms are computational artifacts that solve a given problem or accomplish tasks through detailed codes written in the form of rules and calculations. Algorithms have been involved in computing automation for decades but have only recently become common in popular discourse. According to Wagenknecht, Susann, et al., algorithms have transcended from technical artifacts to net infrastructure as they regulate, discern, and assert power through computation.¹⁴⁸ The invisible authority of algorithms extends their computational influence to shape human-to-human interactions, broaden general societal outlooks (especially political), and ultimately drive trending ideologies among all user groups. Algorithms have transformed from a

¹⁴⁴ Christian Fuchs, "The Political Economy of Privacy on Facebook," *Television & New Media* 13, no. 2 (March 1, 2012): 143.

¹⁴⁵ José van Dijck, "Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology," *Surveillance & Society; Kingston* 12, no. 2 (2014): 198.

¹⁴⁶ Dijck, "Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology," 200.

¹⁴⁷ Ibid.

¹⁴⁸ Susann Wagenknecht et al., "Algorithms at Work: Empirical Diversity, Analytic Vocabularies, Design Implications," in *Proceedings of the 19th ACM Conference on Computer Supported Cooperative Work and Social Computing Companion*, CSCW '16 Companion (New York, NY, USA: ACM, 2016), 536–543.

series of computational codes embedded in software into nuanced elements of infrastructure responsible for effectively controlling all areas of the platform. Beyond Facebook, other platform giants including Amazon, Google, and Twitter all rely on algorithms to operate. The scientific, quantitative, and objective characteristics that form the basic nature of algorithms are inherently deceptive qualities. Algorithms within the current digital realm primarily function based on user behavior as an input.

We can examine the “trending algorithm” as an example of one that successfully captures a user’s data and metadata to curate an individualized experience on the platform:

Trending algorithms calculate the current activity around every post, image, or hashtag by combining some measure of each item’s popularity, novelty, and timeliness. Within these measures, are a number of assumptions. In particular, trending algorithms end to be concerned with a very broad *who*, and a very narrow *when* (and a little about *what*).¹⁴⁹

One of the first identifiable instances of the trending algorithm was Facebook’s experiment on user interaction with its “News Feed” feature. The “News Feed” algorithm was successful in learning what news- and media-related information it should share to particular users based on their individual likes and preferences on Facebook and its affiliated platforms.¹⁵⁰ In addition to this, the algorithm could determine the user’s likelihood of liking, commenting, or sharing a post the algorithm pushed to the user, pertaining to news and media.¹⁵¹ Social media scholar Zeynep Tufekci defines algorithms as “computational processes that are used to make decisions of such complexity that inputs and outputs are neither transparent nor obvious to the human observer.”¹⁵² In other words, Facebook’s algorithms make decisions on the user’s behalf at every point of interaction with the platform. Everything from the colors, photos, and the arrangements of posts that appear in the “News Feed” can, and now are, controlled by algorithms.

For example, during the 2016 United States presidential campaign (USPC), the nature of information and disinformation disseminated across Facebook picked up speed through the relationship between the dubious nature of facts and the editorial nature of algorithmic processes on Facebook’s News Feed. During the USPC, the platform’s model (which depends on user data collection and algorithmic processes to create an “optimal user experience”), alongside Russian actors’ exploitation of existing algorithms, ensured that specious information surrounding wedge political issues reached targeted audiences across Facebook and a number of connected platforms.¹⁵³ While platform companies argue that their algorithms are not trained to influence political dialogue one way or the other, the experiential reality of these features suggests otherwise:

Trending algorithms measure, and they also announce. This makes them databased and calculating, and in doing so, they offer up a rich hieroglyph about some ‘us’, some public, that can itself be discussed and marveled over, or rejected

¹⁴⁹ Robert Seyfert and Johnathan Roberge, *Algorithmic Cultures* (New York: Routledge, 2016), 54.

¹⁵⁰ Zeynep Tufekci, “Algorithmic Harms beyond Facebook and Google: Emergent Challenges of Computational Agency Symposium Essays,” *Colorado Technology Law Journal* 13 (2015): 213.

¹⁵¹ Zeynep Tufekci, *Twitter and Tear Gas* (New Haven: Yale University Press, 2017), 46.

¹⁵² Zeynep Tufekci, “Algorithmic Harms beyond Facebook and Google: Emergent Challenges of Computational Agency,” 206.

¹⁵³ “Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election | Berkman Klein Center,” accessed November 20, 2017, <https://cyber.harvard.edu/publications/2017/08/mediacloud>.

...; [algorithms] can be cultural objects of meaning, not just for those producing information and looking to them for amplification, but for those who see in them a reflection of the public in which they take part.¹⁵⁴

As Gillespie argues, trending algorithms do much more than spread information based on popularity; they become a symbolic representation with cultural significance. Regardless of the topic, the fact that a certain story or idea is “trending” or “viral” is influential in and of itself.¹⁵⁵ In other words, a group of trending topics taken together can represent a pseudo-collective consciousness, a moment in time in which a certain set of ideas define the outlook of the public. While the process of content reaching this status is often spontaneous, the ability to dependably promote “trending” content has spawned an industry. Using technology such as “bots,” or zombie accounts that automatically like/retweet content, these trends can be controlled by experienced actors—usually marketing firms with relatively innocuous, commercial motives. However, this space is increasingly occupied by actors affiliated with national governments and ideological groups whose objectives generally center on manipulating public opinion.

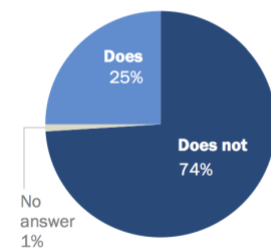
Russia, an external actor that has not traditionally been directly involved in the natural exchange of ideas within the American public sphere, nonetheless supplanted genuine social interactions and positioned its content as an authoritative source of information within these platforms. Covertly, Russia suffused coercive influence within American sociopolitical dialogue, exacerbating the tenor of conversations on digital platforms without actively participating in them. Recently revealed examples of Russian-produced social media content showcase wedge issues within American culture such as veterans, gun rights, refugees/immigration, among others.¹⁵⁶ Naturally, the incendiary nature of these posts translated into robust sharing and commenting, raising their profile under the guise of a naturally resonant post. The platform’s nature augments the ability to spread information favorable to a certain ideology or campaign independent of their truth value—the more provocative and controversial the content, the more algorithms amplify an idea’s reach.

This form of data surveillance, in which predictive analyses and the greater scope of algorithmic processes gleaned from user data inform and influence opinions and discourse, also contributes to the process of normalization. The nature of Facebook’s service is “designed to lower privacy levels and to exploit the social information users provide willingly.”¹⁵⁷ The degrading expectations of privacy facilitated by algorithmic processes in order to provide optimized user experience have increasingly identifiable effects. In this case, the effects include

Figure III. From Pew Survey “Public Attitudes Toward Computer Algorithms”

Most think social media does not accurately reflect society

% of U.S. adults who say the content on social media ____ provide an accurate picture of how society feels about important issues



Source: Survey of U.S. adults conducted May 29-June 11, 2018. “Public Attitudes Toward Computer Algorithms”

PEW RESEARCH CENTER

¹⁵⁴ Seyfert and Roberge, *Algorithmic Cultures*, 69.

¹⁵⁵ *Ibid.*, 70.

¹⁵⁶ Scott Shane, “These Are the Ads Russia Bought on Facebook in 2016,” *The New York Times*, November 2, 2018, sec. U.S., <https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html>.

¹⁵⁷ Bernhard Debatin et al., “Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences,” *Journal of Computer-Mediated Communication* 15, no. 1 (October 1, 2009): 102.

their ability to popularize fake news, spread disinformation, and individually target Americans based on their data, their likelihood to vote for a certain candidate, or their ability to be persuaded as a swing voter. As demonstrated by the USPC, these effects extend well beyond a breach of personal privacy on the platform and, as such, have alarmed users, similar to the shocked dismay generated following the Snowden disclosures.

The Pew Center’s report entitled “Public Attitudes Towards Algorithms” found that Americans expressed most concern about how algorithmic processes violate privacy. In addition to privacy, other top concerns included how algorithms can represent unfair biases and “remove the human element from important decisions.”¹⁵⁸ Moreover, the ubiquitous nature of algorithms on social media has led the majority of Americans to feel that the content misrepresents their lived experience. Algorithms and algorithmic infrastructure have become unassailable truth mechanisms. Coupled with the dissemination of untruthful and misleading information online, algorithms have such an extraordinary amount of power that “[t]he Internet has become not just a weapon in the world’s great political battles. It has become *the* weapon for ideological influence, and careful use can mean the difference between winning and losing.”¹⁵⁹ Although the 2016 USPC brought attention to how organizations exploit user data augment people’s experience on the platform, but the 2018 Cambridge Analytica scandal presented society with truths that finally resulted in action.

¹⁵⁸ “Public Attitudes Toward Computer Algorithms | Pew Research Center,” November 16, 2018, <http://www.pewinternet.org/2018/11/16/public-attitudes-toward-computer-algorithms/>.

¹⁵⁹ Howard, *Pax Tehnica*, 113.

Chapter 8

Looking Beyond: Cambridge Analytica and the Future of the “Reasonable Expectation of Privacy”

“Solitude sometimes is best society.”
- John Milton

In the spring of 2018, the data-mining voter profiling firm Cambridge Analytica came under scrutiny following revelations about their involvement in the most extensive “data breach” in the history of Facebook. In brief, the data generated by Aleksandr Kogan’s personality-quiz app downloaded by 270,000 Facebook users was stored on a private database. The extracted data was later provided to Cambridge Analytica, which later used the database containing information on 50 million users to create 30 million “psychographic” profiles about voters.¹⁶⁰ Psychographic market segmentation, or more generally, psychographic research, clusters customers by their shared personality traits, beliefs, values, attitudes, interests, lifestyles, and more.¹⁶¹ Psychographic data is extremely specific and thus can be used to accurately target customers or—in this case—voters. It was also revealed that Cambridge Analytica shares ties with some of Trump’s major supporters: One of the most infamous is Rebekah Mercer, co-owner of Breitbart News and a Republican donor whose father invested \$15 million in Cambridge Analytica. Cambridge Analytica used its “psychographic” tools to create targeted online ads for Trump’s 2016 election campaign, Ted Cruz’s campaign, and even Brexit.¹⁶² Consequently, Facebook, as the platform that facilitated the relationship between Kogan’s app and Facebook users, saw its exploitative and confusing privacy policies come under even more scrutiny by its users asking whether Facebook users were actually safe.

The Fourth Amendment has yet to be applied to social networking tracking, and debates persist with respect to its applicability. In the 2012 *U.S. v. Jones* case, the Supreme Court held that collecting and tracking GPS data of a vehicle’s movement constitutes a search under the Fourth Amendment based on the volume of data collected. Justice Samuel Alito noted that “the growing use of tracking through mobile devices [and] tracking through ‘social tools’ on phones can shape expectations of privacy.”¹⁶³ Similarly, in *Katz v. United States*, Justice John Marshall Harlan commented that “electronic as well as physical intrusion into a place may constitute a violation of the Fourth Amendment.” However, it remains unclear what defines public and private electronic information on social media platforms such as Facebook. In contrast to these more forward-thinking comments and arguments, according to Justice Hugo Black, courts may

¹⁶⁰ Robinson Meyer, “The Cambridge Analytica Scandal, in 3 Quick Paragraphs,” *The Atlantic*, March 20, 2018, <https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/>.

¹⁶¹ Michael Kranish, “Trump’s Plan for a Comeback Includes Building a ‘psychographic’ Profile of Every Voter: The Republican Presidential Nominee Is Paying Millions of Dollars to a Firm Promising a New Way to Target Supporters.,” *The Washington Post* (Online); Washington, D.C., October 27, 2016.

¹⁶² Meyer, “The Cambridge Analytica Scandal, in 3 Quick Paragraphs.”

¹⁶³ Lisa Schmidt, “Social Networking and the Fourth Amendment: Location Tracking on Facebook, Twitter, and Foursquare,” *Cornell Journal of Law and Public Policy* 22, no. 2 (January 1, 2012): 523.

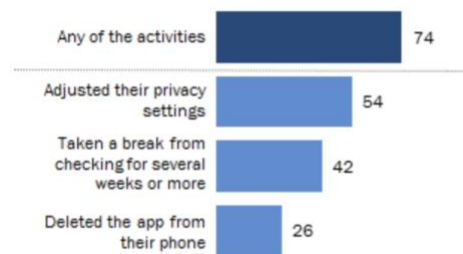
find extending the Fourth Amendment to include electronic intrusions in order to “bring the law into harmony with the times” improper and inappropriate.¹⁶⁴ The argument that the privacy policies of social media sites such as Facebook *do* sufficiently warn users against posting information that they intend to keep private is most commonly cited against the application of Fourth Amendment protections, as users both willingly give consent and expose sensitive information anyway.¹⁶⁵ However, the shaky justification that Facebook’s privacy absolves with respect to how people’s data is stored and used does not translate well to actual users, and most Americans hold misguided ideas about privacy policies as a whole, as described in the preceding chapter.

Revelations regarding how and to what extent institutions are able to surveil has agitated the general public to move beyond learned helplessness and complacency. Whereas public and government surveillance had a normalization effect enabled by and in collaboration with commercial interests, the effects of the 2016 USPC and the 2017 Cambridge Analytica scandal are identifiably different. Increasingly, it appears that Facebook’s user base views the cultural norms with respect to privacy set by the company as unacceptable, as indicated by some recent trends, such as users changing their relationship with the platform by severing ties with Facebook, taking a break, updating their privacy settings, or joining the #DeleteFacebook campaign. In a 2018 Pew survey entitled “Americans Are Changing Their Relationship with Facebook,” data reveal that, between June 2017 and 2018, 74% of Facebook users have either adjusted their privacy settings, taken a break from Facebook, or deleted the app from their phones—the first time Facebook has experienced a shift of this nature.¹⁶⁶

Figure IV. From Pew Survey “Americans Are Changing Their Relationship with Facebook”

42% of Facebook users have taken a break from the site in the past year

% of U.S. adults who use Facebook who say they have done the following in the last 12 months ...



Note: Those who did not answer or gave other responses are not shown.

Source: Survey conducted May 29-June 11, 2018.

PEW RESEARCH CENTER

In 2010, Mark Zuckerberg commented that popularity around blogging has created an environment where people have become accustomed to sharing all of their information. In an effort to prescribe the social effect, he commented, “People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that’s evolved over time.”¹⁶⁷ The evolving “social norm” Zuckerberg describes is the sum of an equation comprised of two parts: information sharing by users on the platform, and concurrent surveillance and commodification of user data and behavior. Only recently has the latter part of the equation, which facilitated the normalization of Facebook surveillance culture through algorithmic processes, targeted ads, and

¹⁶⁴ Schmidt, “Social Networking and the Fourth Amendment: Location Tracking on Facebook, Twitter, and Foursquare,” 526.

¹⁶⁵ Ibid.

¹⁶⁶ Andrew Perrin, “Americans Are Changing Their Relationship with Facebook,” *Pew Research Center* (blog), accessed January 5, 2019, <http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/>.

¹⁶⁷ Ibid., 528.

optimized experiences, caused a disturbance in the public sphere. Recent developments about the platform's operational business model, how it affects and influences its users, how it is susceptible to external manipulation, and how it approaches user data, have generated a shift in the balance of power. In a change from historical trends, American society has seen an oscillation to a more skeptical view of corporate surveillance.

Facebook as an example of corporate surveillance—one entirely set in motion by an end user, whether by social pressures, personal desire, or a habitual pattern of behavior—presents an opportunity for the strongest oscillation of the three cases presented (the NYPD, the NSA, and Facebook). The tone of press coverage and people's reactions to the USPC and the Cambridge Analytica scandal signify a change in how we approach surveillance. Facebook is one of many platforms that operate with a business model of this type, and recent revelations about Facebook with respect to user data privacy has set in motion an influential trend of modifying our relationship with it. This change could represent a pause on the socio-cultural effect of normalization that modern pervasive surveillance models have for so long perpetuated and exploited.

As emerging technologies complicate how users experience technologies built with intrinsic surveillance features, expectations of privacy are challenged, and pervasive surveillance is inevitably normalized. However, the normalization of surveillance culture may overcome its current pause, as the Facebook model continues to demonstrate. Society may organize to challenge and effectively break the process entirely by severing ties with platforms and devices perpetuating the norm, thus depriving them of the user data on which they run. Unlike the NYPD and the NSA, commercial entities are more sensitive to changes in demand based on customer preferences, and the mounting pressure on Facebook and similar platforms could portend a sea change in how these companies govern themselves. In turn, this movement could expand and motivate people to demand protections under the Fourth Amendment that accurately represent the privacy concerns of the 21st century.

There has never been a better time for acting against the infrastructure of surveillance, as public resentment towards its intrusive nature, especially the commercial model, has spurred people to act when they have never done so previously. The pendulum is reaching the end of its swing towards increased surveillance, and understanding how it was set in motion will help us dictate the next strokes of the clock. People are more informed than ever about the nature of surveillance, and are beginning to understand that although their right to privacy is encoded in the Constitution, it does not reflect actual expectations of privacy. Moreover, people can change their preferences more readily than the Supreme Court can rule to reinforce protections against 21st century privacy intrusions, and personal decisions about privacy can be taken in the absence of a silver bullet legal decision. While the right to privacy is less tangible than other fundamental needs such as food, water, and shelter, life under pervasive surveillance impinges upon the most basic characteristic of our humanity: our autonomy.

Bibliography

- Andrew Perrin. "Americans Are Changing Their Relationship with Facebook." *Pew Research Center* (blog). Accessed January 5, 2019. <http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/>.
- Augusto, Fábio Rafael, and Maria João Simões. "To See and Be Seen, to Know and Be Known: Perceptions and Prevention Strategies on Facebook Surveillance." *Social Science Information* 56, no. 4 (December 1, 2017): 596–618. <https://doi.org/10.1177/0539018417734974>.
- "Automatic License Plate Readers." New York Civil Liberties Union, July 23, 2015. <https://www.nyclu.org/en/automatic-license-plate-readers>.
- Castells, Manuel. *The Internet Galaxy [Electronic Resource] : Reflections on the Internet, Business, and Society*. New York: Oxford University Press, 2001.
- Chowdhury, Nuzhat. "I, Spy (but Only on You): Raza V. City of New York, the Civil Rights Disaster of Religious & Ethnic-Based Surveillance, and the National Security Excuse." *Columbia Human Rights Law Review* 46, no. 2 (Winter 2015): 278–331.
- Custers, Bart, Simone van der Hof, and Bart Schermer. "Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies." *Policy & Internet* 6, no. 3 (September 1, 2014): 268–95. <https://doi.org/10.1002/1944-2866.POI366>.
- Debatin, Bernhard, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes. "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences." *Journal of Computer-Mediated Communication* 15, no. 1 (October 1, 2009): 83–108. <https://doi.org/10.1111/j.1083-6101.2009.01494.x>.
- "Demographics of Mobile Device Ownership and Adoption in the United States." Accessed January 4, 2019. <http://www.pewinternet.org/fact-sheet/mobile/>.
- "Demographics of Social Media Users in 2016," November 11, 2016. <http://www.pewinternet.org/2016/11/11/social-media-update-2016/>.
- DeNardis, Laura. *The Global War for Internet Governance*. New Haven: Yale University Press, 2014.
- Dijck, José van. "Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology." *Surveillance & Society; Kingston* 12, no. 2 (2014): 197–208. <http://dx.doi.org.ezproxy.cul.columbia.edu/10.24908/ss.v12i2.4776>.

- Elmer, G. "Spaces of Surveillance: Indexicality and Solicitation on the Internet." *Critical Studies in Mass Communication* 14, no. 2 (June 1997): 182–91. <https://doi.org/10.1080/15295039709367006>.
- Fan, P. "Coping with the Big Data: Convergence of Communications, Computing and Storage." *China Communications* 13, no. 9 (September 2016): 203–7. <https://doi.org/10.1109/CC.2016.7582312>.
- Foucault, Michel. *Discipline and Punish : The Birth of the Prison*. New York: Vintage Books, 1995.
- Fuchs, Christian. *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*. New York: Routledge, 2012.
- . "The Political Economy of Privacy on Facebook." *Television & New Media* 13, no. 2 (March 1, 2012): 139–59. <https://doi.org/10.1177/1527476411415699>.
- Giddens, Anthony. *The Nation-State and Violence*. Oakland: University of California Press, 1985.
- Gray, David. "The Fourth Amendment in an Age of Surveillance," 249–94. Cambridge: Cambridge University Press, 2017. doi:10.1017/9781316459607.007.
- Gray, David, and Danielle Keats Citron. "The Right to Quantitative Privacy." *Minnesota Law Review*, *Busines Insights: Essentials*, November 2013, 62–144.
- Hilbert, Martin. "Big Data for Development: A Review of Promises and Challenges." *Development Policy Review* 34, no. 1 (January 2016): 135–74. <https://doi.org/10.1111/%28ISSN%291467-7679/issues>.
- Horten, Monica. *The Closing of the Net*. Cambridge, United Kingdom: Polity Press, 2016.
- "How Americans Have Viewed Surveillance and Privacy since Snowden Leaks." *Pew Research Center* (blog). Accessed January 5, 2019. <http://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/>.
- Howard, Philip N. *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*. New Haven: Yale University Press, 2015.
- Hu, Margaret. "Metadeath." In *In Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair*, edited by Russel A. Miller, 229–56. Cambridge: Cambridge University Press, 2017. doi:10.1017/CBO9781316658888.009.

- Jones, Matthew De Voy. "The Orwellian Consequence of Smartphone Tracking: Why a Warrant under the Fourth Amendment Is Required Prior to Collection of GPS Data from Smartphones Note." *Cleveland State Law Review* 62 (2014): 211–44.
- Joseph, George, and Kenneth Lipp. "IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color." *The Intercept* (blog), September 6, 2018. <https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/>.
- Kerr, Orin S. "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution." *Michigan Law Review* 102, no. 5 (2004): 801–88. <https://doi.org/10.2307/4141982>.
- Kranish, Michael. "Trump's Plan for a Comeback Includes Building a 'psychographic' Profile of Every Voter: The Republican Presidential Nominee Is Paying Millions of Dollars to a Firm Promising a New Way to Target Supporters." *The Washington Post* (Online); Washington, D.C., October 27, 2016. <http://search.proquest.com/docview/1832993126/abstract/D264016CD7204EB5PQ/1>.
- Levine, E. S., Jessica Tisch, Anthony Tasso, and Michael Joy. "The New York City Police Department's Domain Awareness System." *Interfaces* 47, no. 1 (February 2017): 70–84. <https://doi.org/10.1287/inte.2016.0860>.
- Lyon, David. "Digital Citizenship and Surveillance| Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity." *International Journal of Communication* 11, no. 0 (February 14, 2017): 19.
- . *Electronic Eye: The Rise of Surveillance Society*. Minneapolis, UNITED STATES: University of Minnesota Press, 1994. <http://ebookcentral.proquest.com/lib/columbia/detail.action?docID=310274>.
- . *Surveillance after September 11*. Malden, MA: Distributed in the USA by Blackwell Pub, 2003.
- Marx, Gary T. "Surveillance Studies." In *International Encyclopedia of the Social & Behavioral Sciences*, 733–41. Elsevier, 2015. <https://doi.org/10.1016/B978-0-08-097086-8.64025-4>.
- Meyer, Robinson. "The Cambridge Analytica Scandal, in 3 Quick Paragraphs." *The Atlantic*, March 20, 2018. <https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/>.
- Misa, Thomas J, Philip Brey, and Andrew Feenberg. *Modernity and Technology*. Cambridge: MIT Press, 2014.

- Monica Anderson. “6 Facts about Americans and Their Smartphones.” *Pew Research Center* (blog). Accessed January 4, 2019. <http://www.pewresearch.org/fact-tank/2015/04/01/6-facts-about-americans-and-their-smartphones/>.
- “Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election | Berkman Klein Center.” Accessed November 20, 2017. <https://cyber.harvard.edu/publications/2017/08/mediacloud>.
- Philip Chen, C.L., and Chun-Yang Zhang. “Data-Intensive Applications, Challenges, Techniques and Technologies: A Survey on Big Data.” *Information Sciences* 275 (August 2014): 314–47. <https://doi.org/10.1016/j.ins.2014.01.015>.
- “Public Attitudes Toward Computer Algorithms | Pew Research Center,” November 16, 2018. <http://www.pewinternet.org/2018/11/16/public-attitudes-toward-computer-algorithms/>.
- “Public Perceptions of Privacy and Security in the Post-Snowden Era | Pew Research Center,” November 12, 2014. <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>.
- Schmidt, Lisa. “Social Networking and the Fourth Amendment: Location Tracking on Facebook, Twitter, and Foursquare.” *Cornell Journal of Law and Public Policy* 22, no. 2 (January 1, 2012): 515-[ii].
- Schneier, Bruce. *Data and Goliath : The Hidden Battles to Collect Your Data and Control Your World*. New York, N.Y.: W.W. Norton & Company, 2015.
- Seyfert, Robert, and Jonathan Roberge. *Algorithmic Cultures*. New York: Routledge, 2016.
- Shane, Scott. “These Are the Ads Russia Bought on Facebook in 2016.” *The New York Times*, November 2, 2018, sec. U.S. <https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html>.
- Shockley, Brian. “Protect LPR With Positive Legislation.” Vigilant Solutions, April 28, 2016. <https://www.vigilantsolutions.com/protect-lpr-with-positive-legislation/>.
- Smith, Aaron. “Half of Online Americans Don’t Know What a Privacy Policy Is.” *Pew Research Center* (blog). Accessed January 5, 2019. <http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/>.
- Strandburg, Katherine J. “HOME, HOME ON THE WEB AND OTHER FOURTH AMENDMENT IMPLICATIONS OF TECHNOSOCIAL CHANGE” 70 (n.d.): 67.

“#trendingistrending: When Algorithms Become Culture – Culture Digitally.” Accessed January 5, 2019. <http://culturedigitally.org/2016/02/trendingistrending/>.

Tufekci, Zeynep. “Algorithmic Harms beyond Facebook and Google: Emergent Challenges of Computational Agency Symposium Essays.” *Colorado Technology Law Journal* 13 (2015): 203–18.

Wagenknecht, Susann, Min Lee, Caitlin Lustig, Jacki O’Neill, and Himanshu Zade. “Algorithms at Work: Empirical Diversity, Analytic Vocabularies, Design Implications.” In *Proceedings of the 19th ACM Conference on Computer Supported Cooperative Work and Social Computing Companion*, 536–543. CSCW ’16 Companion. New York, NY, USA: ACM, 2016. <https://doi.org/10.1145/2818052.2855519>.

Wang, C., Q. Wang, K. Ren, and W. Lou. “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing.” In *2010 Proceedings IEEE INFOCOM*, 1–9, 2010. <https://doi.org/10.1109/INFCOM.2010.5462173>.

Webster, C. William R. “Surveillance as X-Ray.” *Information Polity: The International Journal of Government & Democracy in the Information Age* 17, no. 3/4 (September 2012): 251–65.

Williams, Raymond. *Keywords : A Vocabulary of Culture and Society*. New York: Oxford University Press, 1985.

Wood, David Murakami, and C. William R. Webster. “Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of Britain’s Bad Example.” *Journal of Contemporary European Research* 5, no. 2 (August 1, 2009): 259–73.