CATÓLICA
INSTITUTO DE ESTUDOS POLÍTICOS
LISBOA

The Political Philosophy of Surveillance: from Historical Roots to COVID-19

Student: Ana Sofia Baguinho, 104519007

Advisor: Professor William Hasselberger

Portuguese Catholic University

MA in Governance, Leadership, and Democracy 2021

Word Count: 25326

Table of Contents

Acknowledgements

The development of this thesis was a long and difficult process, but nevertheless a gratifying endeavor that I’m extremely proud of having undertaken. In the production of this thesis, there were many lessons learned, many drawbacks, but just as many treasurable accomplishments.

First and foremost, I’d like to thank my advisor, Professor William Hasselberger, without whom I would have never been able to write about this subject. Surveillance and digital technologies were not exactly comprised in my in-depth studies during my MA in Governance, Leadership, and Democracy. My long, hard-fought drive to secure this topic as my main research was only realized thanks to Professor William, who, being highly proficient in the area, accepted this risky but worthwhile idea, and provided me with much needed guidance on its formulation.

I’d also like to show my deep appreciation for my family, including my mother, father, brother, and sister, and my friends Maria, Rodrigo, Nika, Varaidzo, and João for showing me what I was capable of achieving in every moment I doubted it couldn’t be achieved, for their patience in this prolonged period that ended up requiring more study and research than was first anticipated, and most of all, for their imperishable belief in and support for my ambitions.

Abstract

Many theorists have argued that surveillance has become the dominant organizing method of social activities in late modernity. Given the increased prevalence and employment of surveillance systems around the world, this thesis seeks to trace and contextualize the developments in surveillance, both theoretically and practically, that have led to its current extent and nature. We begin by analyzing the philosophical theories that provide the normative frameworks which condone, recommend, limit and make it meaningful. This comprises Jeremy Bentham's "Panopticon," Michel Foucault's "Disciplinary Societies" and "Panopticism," Fredrick Winslow Taylor's "Scientific Management," and Gilles Deleuze's "Societies of Control."

Next, we describe the difference that digital technologies make to surveillance systems, namely that the former greatly enhance the latter's ubiquity. As we shall see, COVID-19 is an important subject of analysis regarding surveillance since it has triggered an acceleration of technological development and influence. This second chapter will hence examine surveillance on three levels, describing the contexts in which surveillance has developed in each level, and how it is developing as a response to the COVID-19 pandemic. The first concerns surveillance on a National Level, with a focus on government surveillance. The second involves surveillance on a City Level, including smart city operations and workplace surveillance, and the third assesses surveillance on a Personal Level, covering social media surveillance and smart home technology.

In the final chapter, we underscore certain aspects of modern surveillance practices where either Bentham, Foucault, Taylor, or Deleuze's principles are implicit. For social media surveillance, we

also draw from Shoshana Zuboff's concept of "surveillance capitalism". Lastly, the inherent differences and impact of surveillance operations for the current geopolitical and social order are highlighted, drawing from accounts that shed light on Autocracy's empowerment with such technology, on Democracy's increased potential for misuse, and on the likely repercussions of politically and socially employing surveillance systems. The conclusion then argues that surveillance, as it stands, has major potential to inherently and permanently alter the global political and social landscape.

Introduction

Introduction

Surveillance is a process that has always existed to some degree, and many theorists argue that it has become the dominant organizing method of social activity in late modernity.[1] The reason offered is that the increased prevalence and employment of surveillance techniques around the world gives great leeway for ubiquitous information systems to progressively regulate many, if not all, facets of social life. Whether it involves security agencies scrutinizing people's telecommunications activities, workplaces surveilling employees and their performance, social media platforms tracking uploads and clicks, or advertisers collecting substantial data on customers, surveillance practices – though usually hidden – have come to characterize the way present institutions operate.

The focus of this research will thus be on surveillance systems and the specific ways actors are harnessing a variety of monitoring tools to advance their sector's goals with the objective of making these practices more known and visible, and ultimately support comprehension and debate regarding surveillance in its various forms. This topic of interest carries wide-ranging relevance because society is now at a critical juncture where the technologies involved in the analyzed surveillance apparatuses are set to "transform all realms of human experience."[2] To support this

[1] Kirstie Ball, Kevin Haggerty, and David Lyon, ed., *Routledge Handbook of Surveillance Studies* (Oxford: Routledge, 2012), PDF version, 1.

[2] Henry Kissinger, Eric Schmidt, and Daniel Huttenlocher, *The Age of AI: And Our Human Future* (Little, Brown and Company, 2021) Kindle edition, 18 out of 205.

research, we aim to describe how, to what extent, which, and for what purposes[3] actors are employing surveillance systems, and what kinds of technologies are involved, analyzing these in three distinct levels – National level, City level, and Personal Level.

To truly understand the scope and magnitude of current surveillance practices, it is important to look firstly at the philosophical theories that provide the normative frameworks which condone, recommend, limit, and make it meaningful. For this we selected the four most influential thinkers in shaping the transdisciplinary field of surveillance studies. Next, when analyzing present-day surveillance, we begin by describing the contexts in which surveillance has developed in each level, and how they are developing in response to the COVID-19 pandemic.

After describing the preferred Methodology, we delineate all the concepts and objects relevant to the thesis that invoke further clarification in a subsection termed Key Concepts and Definitions. The first chapter, titled The Historical and Philosophical Background of Surveillance Tools for Social Purposes, will analyze theories on the social purpose of surveillance practices, starting with the Enlightenment philosopher Jeremy Bentham who devised an architectural design of institutional surveillance – the Panopticon – and extoled its utilitarian efficiencies. To follow, the 20th century French thinker Michel Foucault, who looks at the history of ideas and society to illustrate how surveillance became a central method for governance and the construction of modern subjects, launching the idea of surveillance as a technology of *power* that paved the way for what

[3] Not all surveillance purposes and actors are publicly known or available. When the purpose is not mentioned throughout the thesis, it should be assumed that which actors involved in and the reasons for employing surveillance in a specific sphere were not found.

Foucault calls the “disciplinary society,” of which the Panopticon is the architectural figure. Frederick Winslow Taylor and his advocacy of Scientific Management continues the section, analyzed in this research to illustrate how one core feature of Taylorism, namely “the constant help and watchfulness of the management,” incites the advancement of workplace surveillance. Finally, we analyze Gilles Deleuze’s theory of “Societies of Control,” according to which surveillance operations deterritorialize subjectivity and disperse control mechanisms, making surveillance more numerical and abstract.

With the advent of digital computer-based programs, sensors, and cameras, the remarkable technological progress – of Big Data and Artificial Intelligence especially – in the last decade has made more forms of surveillance possible, which not only augment the capacity for better operational performance and associated advantages, but the potential for misuse and related disadvantages. Chapter 2, titled Surveillance in its Present-day Capacity, entails a broad overview of the empirical data on surveillance, beginning with an outline of the significant developments in digital technologies and how they enable further and more powerful surveillance techniques. Additionally, when considering present-day surveillance, it is important to look at how the global COVID-19 crisis is accelerating processes conducive to surveillance utilization and normalization. Historically, plagues have “fast-tracked” underlying historical processes – today we are witnessing this with technological evolution. This second chapter will then deal with analyzing surveillance on three levels, with insights into how the COVID-19 pandemic has affected each level.

The first category relates to Surveillance on a National level, with a focus on government-enacted surveillance for national and state security. This contains a contextual description of how the terrorist attacks of 9/11 engendered a convergence of techno-security and state-corporate agendas and transformed the concept of security to encompass the full policy range of the coercive state apparatus as well as non-coercive aspects of public policy (like food, transport, and energy security, for example). Then we turn to a collection of quantitative data that reveal the increased salience given by governments in developing AI capabilities and describe a few national AI strategies that states have developed. This is followed by an extensive illustration of the *Global Expansion of AI Surveillance*, with a presentation of the comprehensive data on which national governments are employing AI Surveillance techniques and what types are involved (smart/safe cities, smart policing, and facial recognition) based on the AI Global Surveillance (AIGS) Index, drawing some correlations and conclusions. Lastly, a description of how COVID-19 is transforming the government-surveillance nexus in three countries: Australia, China, and the Netherlands.

The second category deals with describing the current extent and nature of Surveillance on a City Level, which considers surveillance in so-called “smart city” projects and in the workplace – and as a result of COVID-19, in a work-from-home setting. A general definition of “smart cities” is defined, following with an illustration of some countries’ smart city agendas, highlighting the phase they’re in and the attention given to them before and during COVID-19. Then, a reflection on how AI and other “smart” technologies have significantly transformed daily workplace surveillance, and how COVID-19 is also greatly impacting employee surveillance, with concrete examples of some corporations' surveillance conduct in such settings.

The third category concerns Surveillance on a Personal Level: spaces of surveillance that center on the capture of personal information, which includes social media and the "smart home". This includes a listing of the technologies and social media platforms people use that possess monitoring and data collection capabilities and likewise augment their own monitoring capabilities. COVID-19 is a significant consideration on this account as the pandemic not only rendered the one form of social contact as safe was online, but also compelled people to spend more time at home due to lockdowns and restrictions, which manifestly increased the volume of data about individuals that circulate in these networks. All surveillance schemes analyzed in these three spheres demonstrate that the COVID-19 pandemic has supercharged the application of surveillance techniques.

To end, the third chapter, titled Bridging Surveillance Theory and Practice – Debating the Potential Implications, links the theory delineated in chapter 1 to the surveillance practices described in chapter 2. This section will underscore certain aspects of present surveillance operations where either Bentham, Foucault, Taylor or Deleuze's principles are implicit. Accordingly, Bentham's Panopticon ends up fitting more accurately within the current workplace surveillance apparatus than the traditional workplace surveillance methods. Foucault's idea of "disciplinary power" and Deleuze's "modulation power" overlap in the smart home, and underline the expanded scope of external discipline and control into domestic spaces, which were heretofore exempt of such.

Taylorism appears to have been revived in some workplaces, which, coupled with significantly advanced monitoring technologies, portends an advanced form of Scientific Management – “Digital Taylorism” or “Neo-Taylorism”. Foucault’s portrayal of how the plague in Vincennes sanctioned increased social regimentation and control is utilized to argue that with COVID-19, we are witnessing a comparable systematic, underlying process. Additionally, the pandemic-driven proliferation of technologies and practices for health monitoring of citizens has implications for what Foucault terms “biopower,” as well as Bentham’s advocacy of permanently visible identities as a way to shape particular kinds of behaviors. Shoshana Zuboff’s recent and influential conceptualization of “surveillance capitalism” elucidates how companies may be establishing new kinds of power and behavior modification methods online and in social media that operate outside of human knowledge and public responsibility.

To close, an analysis of the inherent differences and impact of surveillance practices for the current political and social order. We draw from empirical studies that shed light on Autocracy’s empowerment with such technology (the majority-exportation of surveillance technology coming from China and no longer the US), Democracy’s increased risk for misuse and subsequent backsliding, and on the likely repercussions of politically and socially employing surveillance systems. The chapter concludes that surveillance and its concomitant asymmetric relations of power have a *high potential* for permanently and irreversibly altering the global landscape.

Methodology

In aiming to produce a concise account of the aforementioned points, the chosen approach is a mixed methods research design involving a content analysis of both qualitative and quantitative data, which will be achieved through an internet-based research. The methodology of this research is a combination of qualitative and quantitative explorations, drawing initially on the history of philosophical ideas concerning social surveillance and control and subsequently on empirical studies of current digital surveillance practices and trends. Given how recent the trans-disciplinary field of surveillance studies is, the objective is to seek both theoretical and factual resources, including books, both academic and non-academic articles, reports, and indexes.

Key Concepts and Definitions

Surveillance: entails the monitoring of behavior or activities with the aim of gathering information, and then directing, managing, or influencing activity and behavior. As sociologist David Lyon describes, surveillance "is the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction."[4] In this thesis the terms "surveillance" and "monitoring" are used interchangeably.

Data: units of quantifiable information, or, in Rob Kitchin's definition, "material produced by abstracting the world into categories, measures and other representational forms – numbers,

[4] Torin Monahan and David Murakami Wood, ed., *Surveillance Studies: A Reader* (New York: Oxford University Press, 2018), PDF version, 19.

characters, symbols, images, sounds, electromagnetic waves, bits – that constitute the building blocks from which information and knowledge are created."[5]

Smart Technologies: the term SMART is derived from the acronym which describes "self-monitoring, analysis and reporting technology."[6] These include Artificial Intelligence, Big Data, Internet of Things, and cloud computing.

Artificial Intelligence (AI): refers to the ability of a computer-controlled robot or digital computer to perform tasks that traditionally performed by intelligent beings[7] (such as humans). AI is a multipurpose technology, enabling and supporting the application of various other technologies.

Machine Learning (ML): a subset of AI which refers to flexible, non-specialized intelligence with the ability to learn new tasks without enforced human-coded instructions. ML algorithms analyze huge assortments of data, apply statistical methods and learn from previous errors to then complete a particular task effectively.[8]

Deep Learning: a subset of ML, deep learning uses "deep neural networks" or multi-layered ML programs, which provide its system with a heightened ability to detect even the smallest patterns.[9]

[5] Rob Kitchin, *The Data Revolution* (London: Sage, 2018), PDF version, 11.
[6] Netlingo, "Smart Tech," https://www.netlingo.com/word/smart-tech.php
[7] Encyclopedia Britannica, "Artificial Intelligence," https://www.britannica.com/technology/artificial-intelligence
[8] MIT Technology Review, "What is Machine Learning?" https://www.technologyreview.com/2018/11/17/103781/what-is-machine-learning-we-drew-you-another-flowchart/
[9] Ibid.

Algorithms: correspond to numerical formal instructions. In the words of mathematician Hannah Fry, algorithms are "invisible pieces of code that form the gears and cogs of the modern machine age."[10]

Digital Twin: "A digital twin is a virtual representation of an object or system that spans its lifecycle, is updated from real-time data, and uses simulation, machine learning and reasoning to help decision-making."[11]

Big Data: there is not an agreed upon definition of big data, either academic or industry defining. However, the most cited definitions tend to reference Big Data as data sets that are large in volume (usually consisting of petabytes/terabytes of data), high in velocity (generated in or near real-time), and diverse in variety of type (meaning it can be naturally structured or unstructured, as well as spatially and temporally referenced).[12] Beyond this, other key characteristics include Big Data ideally being exhaustive in scope (capturing entire systems or populations), fine-grained in resolution (strives to be rigorously detailed), relational in nature (allows the conjoining of differing data sets as it contains common fields), flexible (can easily add new fields), and scalable (can quickly expand its size).[13]

[10] Hannah Fry, *Hello World: Being Human in the Age of Algorithms* (NewYork: W. W. Norton & Company), PDF version, 2.

[11] IBM, "What is a Digital Twin?" https://www.ibm.com/topics/what-is-a-digital-twin

[12] Doug Laney, "3D Data Management: Controlling Data Volume, Velocity, and Variety," *Meta Group*, February 2001, https://toaz.info/doc-viewer See also Paul Zikopoulos et al., *Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data* (New York: McGraw Hill, 2012), PDF version.

[13] Danah Boyd and Kate Crawford, "Six Provocations for Big Data," A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 2011, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431 ; Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (London: John Murray, 2013), PDF version;

Datafication: "to datafy a phenomenon is to put it in quantified form so that it can be tabulated and analyzed."[14] Thus, datafication is about selecting an activity or process that was hitherto unanalyzed or tacit and transforming it into data, making it trackable, monitorable, and optimizable. Through this process, various domains of human life became exposed to being digitally processed via methods of analysis that can, on a large-scale, be computerized and automated.

Internet of Things (IoT): "the networking capability that allows information to be sent to and received from and devices (such as fixtures and kitchen appliances) using the Internet."[15] This is done by embedding sensors, chips, and communications modules into commonplace objects, such as refrigerators and lights, turning them into internet-connected refrigerators and sensorized lighting systems that are able to correspond with each other.

Cloud Computing: "the practice of storing regularly used computer data on multiple servers that can be accessed through the Internet."[16]

Biometrics: "biometric technologies refer to all processes used to recognize, authenticate and identify persons based on physical and/or behavioral characteristics."[17] Thanks to modern biometric technology, analogue-to-digital conversion along with automated handling of biometric

[14] *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, 78.

[15] Merriam-Webster, "Definition of Internet of Things," https://www.merriam-webster.com/dictionary/Internet%20of%20Things

[16] Merriam-Webster, "Cloud Computing," https://www.merriam-webster.com/dictionary/cloud%20computing

[17] European Commission, "Biometrics Technologies," https://ati.ec.europa.eu/reports/technology-watch/biometrics-technologies-key-enabler-future-digital-services

identifiers are now possible. Examples include facial, emotion, and voice recognition systems, among others.

Function Creep: the expansion or use of a technology or system beyond its original purposes. David Lyon defines it as “the addition of new features beyond the scope of the original project.”[18]

Sousveillance: is the management and self-monitoring of one’s personal life and health by way of intimate digital technologies that record data about an individual.[19] Different from surveillance, sousveillance is deliberately employed and controlled by a person for personal fulfillment. This process is also referred to as the “**quantified self**” which entails the voluntary act of self-tracking with technology.

Lateral Surveillance/peer-to-peer monitoring: “not the top-down monitoring of employees by employers, citizens by the state, but rather the peer-to-peer surveillance of spouses, friends, and relatives.”[20] Social media platforms, for example, have made lateral surveillance quite effortless and costless, as users can choose to listen to, research, watch and record anyone.

[18] David Lyon, *Surveillance Studies: An Overview* (Cambridge: Polity Press, 2007), PDF version, 201.

[19] Rob Kitchin, *The Data Revolution*, 131.

[20] Mark Andrejevic, “The Work of Watching One Another: Lateral Surveillance, Risk, and Governance,” *Surveillance and Society* 2, no.4 (2005): 481, https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3359/3322

Chapter 1: The Historical and Philosophical Background of Surveillance Tools for Social Purposes

While surveillance has become a permissible aspect of modern life, it exists, in consensus, to protect property and citizens while promoting a more productive society. Computer-based programs, sensors, and cameras are only a few devices used to surveil people, and despite the obvious advantages, there are also drawbacks – the threat to privacy is increasingly evident and disturbing given the raised risk of paternalism and manipulation.

With the proliferation of technological progress in the Digital Age – making more forms of surveillance possible and accessible – it is crucial to look at the philosophical theories that provide the normative frameworks which condone, recommend, limit, and make it meaningful. Therefore, this chapter will focus on the most cited figures[21] in surveillance studies, namely the English enlightenment philosopher Jeremy Bentham, French philosopher and historian Michel Foucault, American mechanical engineer Frederick Winslow Taylor, and the French philosopher Gilles Deleuze.

1.1. Jeremy Bentham → Panopticon

Jeremy Bentham, recognized as the father of utilitarianism, was an English philosopher from the 18th century with notable contributions in many fields. Bentham, like many Enlightenment

[21] See *Routledge Handbook of Surveillance Studies*; *Surveillance Studies: A Reader*; and David Lyon, ed., *Theorizing Surveillance: The Panopticon and Beyond* (Exitor: William Publishing, 2006), for numerous references of these four figures.

thinkers, hoped to formulate an exact quantitative science of morality and politics. To better understand the thinker's reasoning behind the Panopticon and his ethics of surveillance, it is important to clarify how it ties to Bentham's utilitarian attitude.

Bentham theorized that actions are right or wrong inasmuch as they create pleasure or pain. If utility describes the ability to generate happiness, the rightness of an action is hence determined by its utility: by its tendency to advance happiness over unhappiness. This is the **principle of utility** – "that which disapproves or approves of every action whatsoever, according to the tendency which it appears to augment or diminish the happiness of the party whose interest is in question."[22]

He asserts that human beings derive pain and pleasure from the moral, political, religious, and physical dimensions of our lives. Contending that to base moral behavior on impressions of pain and pleasure is not a subjective choice, the philosopher believed humans were actually compelled to do so.[23] According to Bentham our particular tendencies toward pain avoidance and our desire for pleasure, in addition to being what we in fact motivates us, are reasonable as well. However, actions that seek individual pleasure without regard for the effect it has on others is not in line with the principle of utility. Rather, an action conforms to said principle when there's an overall tendency to increase the total level of happiness of all persons affected.[24]

[22] John Bowring, ed., *The Works of Jeremy Bentham*, 11 Vols., (Edinburgh: William Tait, 1838-1843), PDF version, Vol. I, chapter I. 2.
[23] The Works of Jeremy Bentham, Vol. I, chapter I.1.
[24] *Works*, Vol. I, chapter I. 6.

Following this reasoning, to secure such moral behavior and check undesirable actions, governments might acknowledge this theory by enforcing highly stringent punishments and laws. This, however, is not in conformity to Bentham. Legislation, according to the philosopher, should aim to assure "the greatest happiness of the greatest number of people."

Thus, at a time when the tradition of imprisonment for purposes of criminal reform was non-existent in England,[25] Bentham made the case for a Panopticon prison, a penitentiary that offered clear and absolute supervision of prisoners by the person overseeing the controls, an arrangement devised to develop moral character and improve labor productivity. As part of his vision of reforming law and advancing "rational social control," Bentham "concentrated on the panopticon, a scheme which was 'practicable', instead of parliamentary reform, which was 'visionary'."[26]

According to Gary Browning, Bentham, albeit seemingly a "very English theorist", was nevertheless representative of the European Enlightenment tradition given his assurance to establishing rational thinking about public policy and morality, and being a "radical who critiqued custom, the common law, and reliance upon tradition."[27] This meant a view of reshaping society according to science and instrumental reason.

The Panopticon is a multifaceted case that accurately expresses a utilitarian attitude vis-à-vis pain avoidance and pleasure maximization. Its utility resides in minimizing public expenditure and

[25] The first state prison in England was only inaugurated in 1816.

[26] Philip Schofield, *Utility and Democracy: The Political Thought of Jeremy Bentham* (New York: Oxford University Press, 2006), PDF version, 81.

[27] Gary Browning, *A History of Modern Political Thought: The Question of Interpretation* (New York: Oxford University Press), PDF version, 297.

progressing the operation and application of punishment in order to maximize the public good. Likewise, the diffusion of Enlightenment ideas considerably guided the philosopher's deliberations. With Bentham, individuals were framed as being responsible for their own actions and presumed not to be subject to any divine laws, and thus were conceivably rational. So, as Janet Semple points out,[28] measuring improvements in a man's work was the only way, for Bentham, to judge said man's "moral improvement."

The idea of hard labor translating into reformation of moral character has its origin in the inspection house, in 1787. Two years prior, Bentham had visited his brother Samuel in Russia, who was a naval engineer for the prince in Krichev. Samuel's circular inspection house, aimed at supervision of Russian peasants, is said to have inspired Bentham's *Panopticon Writings*. In these, Bentham argues for how the Panoptic model can be applied to schools, hospitals and other institutions:

> No matter how different, or even the opposite the purpose: whether it be that of punishing the incorrigible, guarding the insane, reforming the vicious, confining the suspected, employing the idle, maintaining the helpless, curing the sick, instructing the willing in any branch of industry, or training the rising race in the path of education: in a word, whether it be applied to the purposes of perpetual prisons in the room of death, or prisons for confinement before trial, or

[28] Janet Semple, *Bentham's Prison* (Oxford: Clarendon Press, 2003), PDF version, 93.

> penitentiary houses, or house of correction, or work-houses, or manufactories, or mad-houses, or hospitals, or schools.[29]

Accordingly, Bentham notes the extent to which his project can be applicable, revealing how the Panopticon could serve as a template for whichever institution that demanded it, where more surveillance equals more progressive reform.

Bentham's Panopticon describes a circular prison with someone placed in the central tower overseeing the prisoners' activities in their cells. Albeit an architectural idea, it is one that results in a "new mode of obtaining power of mind over mind in a quantity hitherto without example."[30] The Panopticon, via its distinct architectural design, creates an illusion of uninterrupted surveillance wherein inmates are not constantly watched but believe they are. In the *Panopticon Letters*, its format was intended as circular, arranged with cells that would extend throughout the circumference and toward the center. The height wasn't fixed, as it depended on the number of inmates. The inspection area would be at the penitentiary's core, separate from the main structure and associated with the outer perimeter solely by stairways, and having none of the floors and ceilings coincide. A vacant space designated as an annular area would've been between the inspector's cabin and cells.[31] A key feature of the prison-Panopticon was to construct an extension of perception beyond visible spaces along with reducing temporal relations to spatial relations, hence reinforcing the panoptic power's potential to discipline prisoners.

[29] Jeremy Bentham and Miran Božovič, *The Panopticon Writings* (London: Verso Books, 1995), PDF version, 34.
[30] Miran Božovič, Introduction: 'An utterly dark spot' in *The Panopticon Writings* (London: Verso Books, 1995), 1.
[31] Bentham and Božovič, *The Panopticon Writings*, 35.

In this sense, surveillance is achieved from one single point, the central tower in which the inspector possesses such extended power, leading prisoners to be seen but unable to see the one who sees them. The inspector is grasped as an invisible presence, "an utterly dark spot"[32] in the prison's all-transparent space. It is exactly the inspector's seeming omnipresence which sustains perfect discipline within the Panopticon. According to Bentham, even a brief exposure to the inmates would destroy the inspector's perceived omnipresence. Indeed, for the prisoners the inspector is all-seeing, all-knowing, and all-powerful. Moreover, a large window facing the outward circumference would be in each cell so as to illuminate the structure, while the inward circumference would be formed by an iron grating in order to prevent inmates from being in view of each other.

This characterization of the Panopticon is in keeping with Michel Foucault's – a 20th century French historian who looked at the past to illustrate how surveillance became a central method for governance and the construction of modern subjects – definition of Panopticism, which hypothesizes surveillance as comprising an omniscient inspector. According to Foucault, Panopticism is "a type of power that is applied to individuals in the form of continuous individual supervision, in the form of control, punishment, and compensation, and in the form of correction, that is, the modelling and transforming of individuals in terms of certain norms"[33] in which

[32] *The Panopticon Writings*, 18.

[33] Michel Foucault, ed., *Power: essential works of Foucault 1954-1984* (London: Penguin Books, 2002), PDF version, Vol. 3, p 70.

“panoptic” represents “seeing everything, everyone, all the time.”[34] However, Bentham's goal wasn’t to conceive a society where people would be constantly observed. The idea was, rather, to internalize discipline and hence eventually exhaust the need for the inspector, and as such the watching itself. In other words, once discipline is internalized the self becomes its own watcher and discipliner. Consequently, all-seeing and actually continuous inspection is not desired. In fact, Bentham’s Panopticon was already not truly all-seeing given that the purpose of such a surveillance system was to obviate the demand for punishment, watching, along with the Panopticon itself.

Bentham envisioned the Panopticon as a liberal political project: a proposed answer to his home country’s increasing economic and social problems of the period. Pursuant to the greatest happiness principle, Bentham regarded punishment as evil, allowed solely for the purpose of precluding greater evil. The structure of the Panopticon itself was a considered architecture that would serve the goal of liberating convicts from evidently more coercive modes of institutional violence that were prevalent at the time:

> the key point was not the fact that the inmate of Panopticon would be watched all the time, but (…) that they would be aware that they might be being watched. The inspector saw an infraction. He did not punish immediately, but waited. He saw a second infraction. At some point thereafter, he would confront the perpetrator

[34] Michel Foucault, ed., *Psychiatric Power: Lectures at the Collège de France 1973-1974* (New York: Palgrave Macmillan, 2006), PDF version, 52.

> with his record book. "See here, your infractions, with the date and time. This is your punishment." Once a punishment had been administered, and the prisoners saw that, should they misbehave, punishment was certain, they would no longer misbehave. There would no longer be any need for them to be watched. They would be reformed.[35]

Altogether, Bentham's Panopticon draws on three central assumptions. First, the inspector's omnipresence, which is ensured by his absolute invisibility. Second, the ubiquitous visibility of subjects under surveillance, and finally, the suspicion of constant inspection by those watched. It is relevant to underscore that for Bentham, there were two sides of power involved in the Panopticon. One side mentions the "power over" which entails the capability to spatially organize distinct types of prisoners, to observe them, and to discipline and punish those who violate the predetermined rules for conduct and behavior. The other suggests the power exerted over oneself, in other words, prisoners end up exercising self-discipline and self-restraint as a result of the recognition that they are constantly being monitored, rendering any form of coercion altogether unnecessary save for rare occasions of disobedience. As noted by Regan and Johnson, "this effect is precisely what Bentham believed the panoptic prison would produce. Seeing the guard tower or believing the guards were watching, inmates would adjust their behavior to conform to norms they expected the guards to enforce."[36]

[35] Philip Schofield, *Bentham: A Guide for the Perplexed*, (London: Continuum, 2009), PDF version, 92.

[36] Deborah Johnson and Priscilla Regan, "Introduction," in *Transparency and Surveillance as Sociotechnical Accountability: A House of Mirrors*, (Abingdon: Routledge, 2014), PDF version, 16.

Having previously highlighted Bentham's clarification on the Panopticon's applicability to any establishment where its purposes are desired,[37] it is worth noting that Bentham, on one hand, as pointed out by Foucault,[38] construes the early phases of what was already taking place – particularly in military institutions and hospitals – and, on the other, forecasts the panoptic system's adoption in other circles of social life. What's more, it may be added that Bentham's vision had actually gone beyond the establishment of a panoptic setting as, in *Principles of Penal Law*, he submits that every person should be recognizable at any specific place and time they should find themselves, meaning not just within a Panopticon. In recalling how English sailors printed their family names on their wrists in order to identify their bodies in case of falling victim to a shipwreck, he asserts:

> If it were possible that this practice should become universal, it would be a new spring for morality, a new source of power for the laws, an almost infallible precaution against a multitude of offences, especially against every kind of fraud in which confidence is requisite for success… imprisonment, having for its only object the detection of individuals, might become rare, when they were held, as it were, by an invisible chain.[39]

Here there is a clear extension of Panopticism, wherein the steady visibility of all persons – in regards to making their identity permanently visible – would deter them from particular forms of

[37] *Panopticon Writings*, 34.
[38] Michel Foucault, "The Eye of Power," in *Power/Knowledge: Selected Interviews and Other Writings (1972-1977)*, ed. Colin Gordon, (New York: Pantheon Books, 1980), PDF version, 147.
[39] *Works of Jeremy Bentham*, Vol. 1, 1006.

behavior. Chapter 3 reiterates this point, in the context of the rise of biometrics and facial recognition which enable precisely what Bentham envisioned.

1.2. Michel Foucault → Disciplinary Societies & Panopticism

Michael Foucault's publication, *Discipline and Punish* (1977), was a fundamental milestone in surveillance studies. It prompted an increased interest in the area, which was then incited by the evolution of searchable databases and computers and more recently by all the information and communication technologies that we currently employ on a daily basis. For the study and analysis of surveillance in society, Foucault was a "foundational thinker"[40] whose writings on the rise of the contemporary disciplinary society led scholars to "take surveillance seriously in its own right."[41]

In *Discipline and Punish*, Foucault sets Bentham's Panopticon as the focal point of his appraisal of Enlightenment disciplinary practice and thought. Bentham sought to extensively reform society, outlining its irrationality, and particularly disputing and reforming the schemes of law and punishment. As Gary Browning points out, Bentham's critique was egalitarian and radical to the extent that he suggested overturning the order of an elite[42] along with rendering society contingent on rational examination and determination. Foucault acknowledges this side of the Enlightenment

[40] David Murakami Wood, "Editorial: Foucault and Panopticism Revisited," *Surveillance and Society*, 1, no. 3 (2003): 235 [234-239]

[41] David Lyon, *The Electronic Eye: The Rise of Surveillance Society*, (Minneapolis: University of Minnesota Press, 1994), PDF version, 7.

[42] The utilitarian produces its own elite, like the inspector in the watch tower. A new technocratic elite arises. The political elite that uses it for state surveillance. Bentham might not have intended for his model to be elitist, but the rise of surveillance systems around the world say otherwise.

expressed in Bentham’s social theory. However, it is “the transition from the infliction of gross, physical forms of punishment to modern forms where punishment is determined by scientific, calculating procedures so as to deter crime and reform criminals through less draconian techniques" that Foucault does not believe to "constitute an unqualified amelioration in the treatment of human beings.”[43]

For Foucault, the Enlightenment, despite discovering the liberties, likewise produced the disciplines.[44] Popularizing the conception of the Panopticon as the embodiment of social control in present times, Foucault turned Bentham’s innovative approach to confinement architecture in the 18th century into the seed of biopolitics.[45] According to Foucault, the Panopticon was not recognized for its original utility and structure seeing that the principles of observation, correction of behavior and surveillance did not end with the prison scheme. Rather, discipline runs throughout society into the organization of hospitals, schools, and other institutions, making for a “carceral” society under a “permanent gaze.”[46]

Anne Brunon-Ernst, in quoting Schofield, notes that "[Foucault's interpretation of the Panopticon] would have seemed very odd to Bentham, who regarded his Panopticon prison as humane, and an enormous improvement on the practices of the criminal justice system of the time.”[47] Brunon-

[43] Gary Browning, *A History of Modern Political Thought: The Question of Interpretation*, (Oxford: Oxford University Press, 2016), PDF version, 304.

[44] Michel Foucault, *Discipline and Punish*, (New York: Vintage Books, 1995), PDF version, 222.

[45] Biopolitics refers to the regulation of populations through the exercise of biopower, which is the classifying of citizens based on biological features.

[46] Foucault, *Discipline and Punish*, 248, 250.

[47] Anne Brunon-Ernst, ed., *Beyond Foucault: New Perspectives on Bentham’s Panopticon* (Surrey: Ashgate Publishing, 2012), PDF version, 2.

Ernst goes on to assert that scholars working on Bentham's Panopticon have always been aware of the inherent contradiction in the philosopher's writings, as Janet Semple expresses when she addresses that "the panopticon writings are (...) disturbing and create problems for Bentham's admirers." The variation between a progressively attractive Bentham, which is mostly by virtue of the new edition of *The Collected Works of Jeremy Bentham* as well as scholars' monographs at the Bentham Project, and a still objectionable Panopticon is broadly ascribed[48] to Foucault's depiction of the Panopticon in *Discipline and Punish*. Provided that Foucault's analysis of the Panopticon has driven Bentham's work to become more known to a wider audience, it has also conversely spun Bentham into a precursor of Big Brother.[49]

As such, it is worth noting that, at present, the Panopticon is mainly comprehended through Foucault's use and analysis of the notion. Nevertheless, it seems appropriate to summarize Foucault's analysis of the Panopticon so as to ascertain why it resonated in many fields of study, especially since his reasoning is not only rehabilitating certain elements of Bentham's work, but likewise developing and expanding it into a broader context of networks and power relations in modern societies.

Foucault fundamentally argues that from the eighteenth and nineteenth centuries Western societies are marked by a recent form of power which is "capillary" and influences "the grain of individuals, touches their bodies and inserts itself into their actions and attitudes, their discourses, learning

[48] Anne Brunon-Ernst, ed., *Beyond Foucault: New Perspectives on Bentham's Panopticon*, 3.

[49] Janet Semple, "Bentham's Haunted House," In *The Bentham Newsletter*, 1987, PDF version, 36, https://www.ucl.ac.uk/bentham-project/sites/bentham-project/files/newsletter_11.pdf

processes and everyday lives."[50] Put simply, the Panopticon prison system of organization has become active and present in many, if not most, features of Western societies. What's more, Foucault endeavors to reveal through compelling examples that these schemes often remain unnoticed or hidden, precisely because they are identified in the fibers of everyday life, and that is what makes them so ubiquitous and powerful.

Initially, Foucault began investigating panoptic settings prior to even coining them as such.[51] From his works on clinics and asylums there's a frequent emphasis on the emergence, pointing to the eighteenth century's end, of a different architectural arrangement of medical institutions that allowed constant observation of patients wherein the key feature was the "power of the gaze." Moreover, Foucault mostly considered the "power of the gaze," the "power over," or even power as repression – a power which was exercised by the watchers. In these institutions, Foucault sought, in his own words, "to find out how the medical gaze was institutionalized, how it was effectively inscribed in social space, how the new form of the hospital was at once the effect and the support of a new type of gaze."[52] He therefore wrote of a gaze which was "penetrating," "inquisitorial," and "illuminating." Foucault asserted, for example, that "the proximity that comes into being in the asylum … is simply that of a piercing gaze, observing, scrutinizing, moving pitilessly close."[53]

[50] *Discipline and Punish*, 209-210.

[51] Marcelo Hoffman, "Disciplinary Power," in *Michel Foucault: Key Concepts*, ed. Dianna Taylor (London: Routledge, 2014), PDF version, 27.

[52] Foucault, "The Eye of Power," 146.

[53] Michel Foucault, *History of Madness*, (Abingdon: Routledge, 2006), PDF version, 488.

Still, even in these accounts Foucault does refer to the other side of power – implicit in the panoptic *dispositifs* – which is the power that those who are being monitored exercise over themselves, identified as "technologies of the self" seeing that the watched, cognizant of being under continual observation, eventually internalize the existent rules and norms, and hence start to behave in the required fashion sans coercion. For example, Foucault contends that the elimination of physical restraints in the asylum "was part of a whole, of which the essential element was the constitution of '*self-restraint*', where the freedom of the mad" was continuously examined by the gaze.[54] This self-objectification is a dimension likewise present in his observation of the incessant feeling of guilt that was instilled in the madmen as a component of their treatment: "the asylum organized [guilt] for the madman as self-consciousness (...) Through this guilt, the madman became an object of punishment always offered to himself and the other; and from that recognition of his status as object, and his consciousness of his own guilt, the madman was to return to his consciousness as a free, responsible subject (...) This movement (...) was a process to be found in work as well as in the gaze."[55]

Also worth mentioning is scholars like Norris and Elden's emphasis on the importance of the plague[56] in Foucault's accounts since the control of a town named Vincennes which was facing an epidemic at the end of the 17th century is precisely where he begins clarifying Panopticism.

[54] Foucault, *History of Madness*, 487.
[55] Ibid., 485.
[56] Clive Norris, "From personal to digital" in *Surveillance as Social Sorting: Privacy, risk, and digital discrimination*, ed. David Lyon, (London: Routledge, 2003), 250-251; Stuart Elden, "Plague, Panopticon, Police," in *Surveillance and Society* 1, 3 (2003): 240-253. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3339/3301

Foucault highlights as one of the changes of the late 18th century the emergence of intervention mechanisms that were not medical or therapeutic. Rather, he outlined increased concerns with food, environment, and modes of life. It is also during this period that medicine solidifies as a crucial aspect to the maintenance and development of society. Foucault then asserts that the importance given to biopolitics in a capitalist society, and thus the move toward prevention and regulation make the development of profiles, surveillance, statistics, and monitoring essential.[57] As he puts it, governments no longer dealt only with territory and individuals, but also with an "economic and political problem" – their population.[58]

Noting two modes of dealing with disease in the West, Foucault distinguished between an older form, the treatment of lepers which involved branding and exile, and the regulation of the plague which involved identification and discipline:

> This enclosed, segmented space, observed at every point, in which the individuals are inserted in a fixed place, in which the slightest movements are supervised, in which all events are recorded, in which an uninterrupted work of writing links the centre and periphery, in which power is exercised without division, according to a continuous hierarchical figure, in which each individual is constantly located,

[57] Michel Foucault, ed., *Essential Works of Foucault 1954-1988,* (New York: The New Press, 2001), Volume 3, PDF version, 137.
[58] Michel Foucault, "Society Must Be Defended" in *Lectures at the Collège de France 1975-76* (New York: Picador, 2003), PDF version, 243, 245.

> examined and distributed among the living beings, the sick and the dead - all this constitutes a compact model of the disciplinary mechanism.[59]

Foucault suggests that if "the leper gave rise to rituals of exclusion, (...) the plague gave rise to disciplinary projects."[60] He argues then that the development of social control consists of the interplay of these two exercises of power and that the "panopticon is the architectural figure of this composition."[61] Thus, as pointed out by Norris:

> the Panopticon is far more than an architectural form of visualization in that it is also the social, political, and technical infrastructure that renders visualization meaningful for the basis of disciplinary social control. At the heart of the panoptic project is the collection of individualized codified information, and this provides the rationale for classification and subsequent authoritative intervention.[62]

The plague was used to depict how, according to Foucault, any type of confusion and disorder[63] was managed or resolved from the 19th century onward. The Panopticon represents a transformation from the plague because it is a permanent structure, becoming normal and no longer exceptional. Taking from Bentham's prison Panopticon, Foucault employed the underlying concept as a symbol of the disciplinary regime that abounds in modern society, wherein the key method of social control has shifted from "spectacle" to "surveillance."[64] In essence, Foucault

[59] *Discipline and Punish*, 197.
[60] Ibid., 198.
[61] Ibid., 200.
[62] Norris, "From Personal to Digital," 250.
[63] *Discipline and Punish*, 232.
[64] Ibid., 10, 49, 97.

portrayed the power mechanism in the Panopticon – Panopticism – as being a generalizable power design of the governing technique that fostered “docile bodies,” and deemed it as a model of disciplinary control in the modern world.

Power as discipline and dominance receives a lot of attention in *Discipline and Punish*:

> the human body was entering a machinery of power [the prison] that explores it, breaks it down and rearranges it. A ‘political anatomy’ …. defined how one may have a hold over others’ bodies… so that they may … operate as one wishes, with the techniques, the speed and the efficiency that one determines.[65]

He further notes that “the perpetual penalty that traverses all points and supervises every instant in the disciplinary institutions compares, differentiates, hierarchizes, homogenizes, excludes.”[66] These methods which aim to create “docile bodies” make for predictive societies wherein such bodies are not just units of communication, but of information.

In his discussion of Panopticism’s growth in modern society, Foucault emphasizes the role of “experts” who emerge alongside various panoptic institutions and generate “truths” regarding “normalcy” and “deviance”:

[65] *Discipline and Punish*, 138.
[66] Ibid., 183.

> We are in the society of the teacher-judge, the doctor-judge, the educator-judge, the social worker-judge; it is on them that the universal reign of the normative is based.[67]

These knowledge/power arrangements, as well as the "power of the gaze," create a system in which individuals exercise self-restraint and self-discipline without being forced to do so in order to comply to the "norm" and the perceived anticipations of the "watchers." In the words of Foucault:

> [s]o it is not necessary to use force to constrain the convict to good behavior, the madman to calm, the worker to work, the schoolboy to application, the patient to the observation of the regulations (...) He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection.[68]

Following the discussion of Bentham's Panopticon project and how Foucault used it as a metaphor in his understanding of the formation of the disciplinary society, a few observations can be made. To begin with, Bentham emphasized the Panopticon's cost-effectiveness in order to maximize the utility of punishment. Because of the total invisibility of the inspector, as well as the universal visibility of inmates aware that they may be watched by the inspector at any time, the lack of any

[67] *Discipline and Punish*, 304.
[68] Ibid., 202-203.

need to maintain large and costly coercive personnel created a setting in which inmates would behave in ways expected of them "willingly." They would, in other words, practice self-control and self-discipline. He even claimed that this would cause them to change their personalities and lose their drive to commit wrong. In this sense, rather than power as coercion or repression, the component of power that he emphasizes in his texts is power over oneself. Foucault primarily concentrated on the Panopticon as a *dispositif* that involves the exercise of power as repression, but he likewise recognized that the Panopticon also involved the exercise of power over oneself – "technologies of the self" –, as he openly acknowledged on multiple occasions, both in his early and notably in his later works. Both Bentham and Foucault discussed the Panoptic model's application to the rest of society. Both thinkers mentioned other institutions where this model could be used (hospitals, factories, schools, asylums, etc.), but Bentham went even farther when he addressed the importance of everyone having an instantly recognizable identity, even outside of such institutions. As Browning writes:

> While Bentham may have imagined the Panopticon to represent a less severe regime of punishment than what had gone before,[69] the project aims to control individuals by machinery and surveillance so that they perform in required ways. It is an exercise in behavior modification, which assumes that rational ends justify the objectification of individuals.[70]

[69] The goal of the project is to establish the most cost-effective model of punishment, with the goal of both reforming convicted criminals and preventing others from committing crimes.

[70] Browning, *A History of Modern Political Thought*, 312.

This concept of behavior modification in Shoshana's Zuboff account of 21st century "surveillance capitalism" will be revisited in Chapter 3.

1.3. Frederick Winslow Taylor → Taylorism/Scientific Management

As a result of the second industrial revolution in the early twentieth century, "business became big business, and the number and kinds of positions in the office ballooned,"[71] so management faced a dilemma – how to conduct these employees. Having worked for years in heavy manufacturing, and after witnessing a great diversity in the way jobs were executed – some proficient and others not – Frederick Winslow Taylor, an American mechanical engineer, set out to resolve inefficiencies in systematic ways. Accordingly, he articulated a new management theory known as *scientific management*, or Taylorism.

Before the 1900s management theory was not understood nor consolidated as it is currently: the idea of scientifically studying and improving the work process did not properly exist prior to Taylor's publication of the *Principles of Scientific Management*. According to Taylor, ensuring "maximum prosperity" is "the principle object of management."[72] This meant higher wages for employees and lower costs for employers and businesses, for which such achievement implied the elimination of inefficiencies.

[71] Nikil Saval, *Cubed: A Secret History of the Workplace*, (New York: Doubleday, 2014), PDF version, 33.

[72] Frederick Winslow Taylor, *The Principles of Scientific Management*, (New York: Harper & Brothers, 1919), PDF version, 9.

Thus, Taylor analyzed the labor process so as to maximize laborer productivity and asserted that it could be accomplished in two ways. Firstly, by narrowing the time wasted throughout the production process, particularly by inhibiting “worker soldiering” which meant slowing task completion deliberately.[73] Secondly, by dividing the work process into a series of basic operations, each of which can be precisely measured and monitored. For Taylor, employers would thrive in “obtaining the maximum output of each man and each machine” solely “through the adoption of modern scientific management.”[74]

Seeking to delineate the knowledge of the “one best method” to accomplish a task by regimenting, identifying, and fragmenting workflows and to set up methods of employee surveillance to achieve production targets, Taylor outlines four principles of management. The first is to replace the ‘rule of thumb’ approach, or old individual opinion or judgement, with precise scientific knowledge and investigation to boost production standards. Second, “scientifically” select the most suitable person to tackle a job, based on motivation and capability, as well as train them to perform at maximum efficiency, which means to execute the job in the one specific way devised. Third, monitor work performance, providing guidance and supervision when necessary in order to ensure maximum productivity. Lastly, “an almost equal” allocation of labor between workers and managers so that the latter utilize their time to plan and train, allowing the former to carry out what they've been

[73] Taylor, *The Principles of Scientific Management*, 13-14.
[74] Taylor, *Principles*, 27.

instructed to do efficiently.[75] What this implies is a hierarchical and strict division of management – intellectual work – from production – manual work.

Taylor's scientific management techniques were considered, at the beginning of the twentieth century, the ultimate achievement in workplace effectiveness.[76] Prior to becoming a U.S. Supreme Court Justice Louis Brandeis channeled Taylorism to support his argument for opposing a rate increase demanded by railroads. The publicity and attention given to Brandeis' application of Taylorism to foil the request for rate increase led, according to Robert Kanigel, to scientific management's endorsement and promotion worldwide,[77] influencing both European and American industrialists – Henry Ford especially –, along with philosopher Antonio Gramsci, and Vladimir Lenin.

"The constant help and watchfulness of the management"[78] comprised one essence of scientific management, which, for Kanigel, produced the "unholy obsession with time, order, productivity, and efficiency that marks our age."[79] Moreover, Marcelo Hoffman, whilst providing a synopsis on Foucault's conception of disciplinary power, also utilizes Taylor's *Principles* to exemplify the operation of this power.[80] Effectively, Taylorism involved the advancement of progressively sophisticated techniques of employee surveillance and monitoring. "The rule of the Taylorist

[75] Taylor, *Principles*, 36-37.
[76] Robert Kanigel, "Taylor-Made: How the World's First Efficiency Expert Refashioned Modern Life in His Own Image," *The Sciences* 37, no. 3 (1997) http://www.ams.sunysb.edu/~weinig/Taylor-made.pdf
[77] Robert Kanigel, *The One Best Way: Frederick Winslow Taylor and the Enigma of Efficiency*, (New York: Viking, 1997), 429-443.
[78] Taylor, *Principles*, 85.
[79] Kanigel, *The One Best Way*, 7.
[80] Marcelo Hoffman, "Disciplinary Power," in *Michel Foucault: Key Concepts*, 27.

system is that the unobserved worker is an inefficient one."[81] Thus, in this respect, Taylor's philosophy contributed to the expansion of disciplinary power in the workplace originating a time-and-motion-involved scheme of behavior reinforced by the supervisor's gaze.

According to Hoffman, "individualization, observation and the constitution of an administrative identity on the basis of knowledge through observation all figure centrally in Taylor's account of the selection of the appropriate worker to load 47 tons of pig iron per day."[82] Schmidt, the worker selected by Taylor in this example, was communicated the following:

> Well, if you are a high-priced man, you will do exactly as this man tells you tomorrow, from morning 'til night. When he tells you to pick up a pig and walk, you pick it up and you walk, and when he tells you to sit down and rest, you sit down. You do that right straight through the day. And what's more, no back talk. Now a high-priced man does just what he's told to do, and no back talk. Do you understand that? When this man tells you to walk, you walk; when he tells you to sit down, you sit down, and you don't talk back at him.[83]

In this excerpt, Hoffman highlights various disciplinary practices. There's the exhaustive uniformity regarding Schmidt's movements in that his supervisor, besides directing the work, also has command over when and how he rests to maximize efficiency. Furthermore, not allowing

[81] Alex Rosenblat, Tamara Kneese, and Danah Boyd, "Workplace Surveillance," *Open Society Foundations Future of Work Commissioned Research Papers*, (New York: Data & Society Research Institute, 2014) https://datasociety.net/wp-content/uploads/2014/10/WorkplaceSurveillance.pdf
[82] Hoffman, "Disciplinary Power," 37.
[83] Taylor, *Principles*, 45-46. Note that Schmidt's average daily load was 12.5 tons of pig iron a day.

“back talk” illustrates “the disciplinary relationship between increased utility and increased obedience.”[84] As Taylor asserts that Schmidt accepted the aforementioned conditions and managed to realize the loading of 47 tons per day, he adds that under constant observation Schmidt hardly ever failed to do the task at the desired pace, with the desired skill, for three years.[85] Hoffman then points out that Taylor “leaves us with the distinct impression that the application of scientific management succeeded in yielding Schmidt as a docile as well as useful individual.”[86]

While disciplinary practices are manifestly present in Taylor's examples for advocating scientific management, Hoffman argues that Taylorism also “de-naturalizes” disciplinary power given that disciplinary action through scientific management is widely contested.[87] In fact, Taylor advises against any hurried application of Taylorism, asserting that only a lengthened period of adaptation and habituation will ensue its successful application.[88] Nevertheless, Taylorism did gain traction, underscored in a biography of Taylor which reports that, by 1918, his “system was taking on the trappings of an international movement... [and Taylorism’s] ideas have had an enormous influence on the industrial life of almost all countries.”[89] As a result, administrative surveillance are now commonplace in modern West.

[84] Hoffman, "Disciplinary Power," 37.
[85] Taylor, *Principles*, 47.
[86] Hoffman, "Disciplinary Power," 38.
[87] Taylor, *Principles*, 49-52; Taylor writes about employees who intimidate managers, damage machinery, and threaten to strike.
[88] Ibid., 128-35.
[89] Sudhir Kakar, *Frederick Taylor: A Study in Personality and Innovation* (Livonics Infotech, 2018), PDF version, 11-12.

1.4. Gilles Deleuze → Societies of Control

In the modern age, surveillance functioned as a mechanism of self-correction by processes of normalization and individualization, for which the diagrammatic form was the Panopticon. In postmodern civilization, however, power and control are seemingly more flexible and dispersed, and the globalization and subsequent prevalence of capitalism also shifted organization from hierarchical observation to a distributed and digital capture, decoding, and recoding of information. In other words, the emergent data-centric information economy has changed the kinds of surveillance involved, now comprising digital and lateral surveillance for example. As such, the adequacy of Foucault's conception of Panopticism for describing modern surveillance has been increasingly challenged.[90]

Foucault cautions a clear distinction between "confinement" and "enclosure".[91] As William Bogard points out, enclosure does not demand material constraint, so while "the physical interior of the panopticon may be a gentler enclosure than the dungeon, (...) confinement remains its technology."[92] In moving from the architectural or institutional to the governing of a multiplicity of subjects, and substituting industrial production for the information network as the dominant

[90] See Oscar H. Gandy, *The Panoptic Sort: Towards a Political Economy of Personal Information* (Oxford: Westview 1993); David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Cambridge: Polity, 1994); Kevin D. Haggerty and Richard V. Ericson, "The Surveillant Assemblage." *British Journal of Sociology* 51, no. 4 (2000): 605-22; Roy Boyne, "Post-Panopticism," *Economy and Society* 29, no. 2 (2000): 285-307; and Shoshana Zuboff, *In the Age of the Smart Machine: the Future of Work and Power* (New York: Basic Books, 1988).

[91] Gilles Deleuze, "Postscript on the Societies of Control," *October* 59 (1992): 4. https://www.blogs.hss.ed.ac.uk/crag/files/2015/09/deleuze_control.pdf?fbclid=IwAR1chxk3wkw78GY1CWDUw__BzsmR8oIAs528XO-sVnLcVK_b52HMU_Rad4I

[92] Kirstie Ball, Kevin Haggerty, and David Lyon, ed., *Routledge Handbook of Surveillance Studies*, 31.

model for arranging society, Foucault's version of Panopticism, which relies on a restrictive spatiality, somewhat loses its applicability for analyses of contemporary surveillance, given its inability to satisfy the expanding needs of capital for better communication speeds, mobility of labor, and risk management. Surveillance theories have hence witnessed a rise in the range of concepts and positions that attempt to debate new surveillance-enabling technologies, with or without employing the panoptic paradigm.

A perceptive and noteworthy[93] philosopher that moves beyond the Panopticon metaphor is Gilles Deleuze, a French Philosopher who, in 1992 – before the internet's hegemony –, argued that "everywhere *surfing* has already replaced the older *sports*."[94] In *The Postscript on the Societies of Control*, Deleuze provides analyses of control and power in the new media environment, observing that today's surveillance has developed beyond that of Foucault's disciplinary society, where individuals are "normalized" through their explicit locations, to what he terms "society of control," where differences and similarities are scaled down to code. Just as Foucault notes the transience of disciplinary societies, that they emerged after the "societies of sovereignty," Deleuze notes how the former were to be followed by the societies of control. Foucault turns to history so as to exemplify how surveillance developed into a central method for the structuring of contemporary subjects and for governance. Likewise, Deleuze then argues that the simultaneous technological revolutions and sociopolitical upheavals of the 1960s and 1970s signaled the end of Foucault's

[93] David Lyon, ed., *Theorizing Surveillance: The Panopticon and Beyond*, 13, 73, 103, 142, 300; Ball, Haggerty, and Lyon, ed. *Routledge Handbook of Surveillance Studies*, 15, 21, 28, 30; David Lyon, *Surveillance as Social Sorting*, 90.
[94] Deleuze, "Postscript," 6.

modern surveillance regime, leading to today's more automated, mechanical, and, according to some, brutal late-capitalist regime.[95]

Before delving into *Postscript*, it is important to highlight some of Deleuze's prior arguments regarding his reading of Foucault in 1988. In Deleuze's analysis of *Discipline and Punish*, he believes Foucault moves beyond the dualism of his earlier works,[96] for which the Panopticon's duality are forms of matter – the prison – and forms of function – punishment.[97] Deleuze asserts that these forms are in flux, whose productive capacity dwells continually in an 'informal' space, and hence deliberates:

> What can we call such a new informal dimension? On one occasion Foucault gives it its most precise name: it is a 'diagram', that is to say a 'functioning, abstracted from any obstacle [...] or friction [and which] must be detached from any specific use'. The diagram is no longer an auditory or visual archive but a map, a cartography that is coextensive with the whole social field.[98]

In *Postscript*, Deleuze, building on Foucault, attempts to further define the diagram of social control. In the first section, the philosopher portrays the control society as budding, historically tracing it against the earlier disciplinary forces. The second section involves an outline of the logic of the control society as a set of concepts, premises, and behaviors. The final section depicts a

[95] Torin Monahan and David Murakami Wood, ed., *Surveillance Studies: A Reader* (New York: Oxford University Press, 2018), PDF version, xxii.
[96] Gilles Deleuze, *Foucault* (Minneapolis: University of Minnesota Press, 1988), PDF version, 39.
[97] Deleuze, *Foucault*, 33.
[98] Ibid., 34.

program for residing in a society of control. Essentially, in light of the swift "exteriorization of productive forces in the twentieth century and its acceleration after the Second World War" through developments in methods of statistical modeling, computerization, and networks, Deleuze describes how the disciplines are in a "generalized crisis."[99] This is so because these disciplinary "interiors," as Deleuze puts it, are no longer compatible with a mode of production that currently demands dispersed, decentralized, as well as mobile administration. Therefore, a new model of enclosure arises from the "shift from architectural and optical modes of surveillance towards the integration of dispersed sites of information solicitation within simulational feedback loops."[100]

Deleuze addresses how the forces of globalization and capitalism are transforming societies along with how institutions like the factory, the hospital and the school have increasingly turned into a *corporation,*[101] of which the difference between the two societies lies in the method and process. While discipline focuses on attaining a docile, stable and long-term society that intends the most efficient resource management in order to realize the goals of government, corporations fixate on short-term outcomes, which demand constant control and therefore monitorization and assessment of markets, strategies, etc. The fundamental difference between the corporation and the nation-state is that the former does not aim for the flourishing of society altogether, but instead focuses on controlling specific parts of progressively globalized markets.

[99] Deleuze, "Postscript," 3. Deleuze asserts that this crisis relates to "all the environments of enclosure," comprising the hospital, prison, family, school, factory.
[100] Greg Elmer, "A diagram of panoptic surveillance," *New Media & Society* 5, no. 2 (2003): 240. https://www.dhi.ac.uk/san/waysofbeing/data/data-crone-elmer-2003.pdf
[101] Deleuze, "Postscript on the Societies of Control," 4.

To clarify, the objective is no longer to, for example, spawn a good and consistent worker, but to know where and how to complete the worker's task as efficiently as possible. Thus, as the global system of control and capital calls for subjects who are heterogeneous, fluid, and flexible instead of subjects who are molded into a final and fixed form, society transitions from systems based on *molds* into *modulations*[102] which, being both flexible and short-term, are alterations according to circumstances, “like a self-deforming cast that will continuously change from one moment to the other.”[103] Here it's important to underscore that Deleuze's attention was on linked databases and continuity of institutions generating and sharing information not just between themselves but with third parties as well. Thus, the technical logic that regulates societies of control, for Deleuze, is “modulation.” Considering the transfer from industrial to network management in contemporary society, *modulation* control, as opposed to the unalterable mold, adapts to the consequent deterritorialization of productive forces,[104] making surveillance more numerical and abstract.

In a disciplinary society, the transitions from one institution to another are linear and chronological, meaning persons are always starting over again as life is almost like a constant reset as we turn from the bedroom, to the school, to the workplace and so on. In a society of control, Deleuze argues, nothing ever truly ends, as “the man of control is undulatory, in orbit, in a continuous network.”[105] Deleuze recalls not only the constant postponements as well as the

[102] Deleuze, "Postscript," 4.
[103] Ibid.
[104] Kirstie Ball, Kevin Haggerty, and David Lyon, ed., *Routledge Handbook of Surveillance Studies*, 33. The modulated control is expressed "by models, codes and new methods of social sorting."
[105] Deleuze, "Postscript." 6.

ambiguous start of Kafka's *Trial*, and refers to the interminability of ongoing education. Deleuze, in describing how disciplinary societies have a signature and number for placing individuals while in societies of control individuals are reduced to code or a password,[106] emphasizes the subsequent loss of individual's relevance as subjects to be surveilled. Rather than attempting to subject and discipline actual individuals or bodies, it is now their *representations* in data, and so the individual is captured as a collection of distinct pieces of information. This is what Deleuze terms the *dividual*, which is essentially the individual cut up into a variety of data points, divided and fed into algorithms, marking another transition in society – to data-bodies. Furthermore, whereas the economy of the disciplinary society is anchored by production, and its stimulus is consumer need, Deleuze claims[107] that advertising – “the joys of marketing” – is what drives the economy of control, for which the stimulus is consumer desire.

The concept of control, articulated by Deleuze, derived by way of a modulating set of relations and practices between social forces has, in the words of Greg Elmer, “tended to lend more weight to networked and immanent forms of surveillance, perspectives that highlight and otherwise question the ever-changing and ever-expanding surveillance systems, mechanisms, protocols, policies, techniques, and technologies.”[108] Deleuze conceptualized a different mode of power which he witnessed unfolding in the developing economic, technological, and organizational activities of the era post-Ford. As the information network replaced industrial production as the

[106] Ibid., 5.
[107] Deleuze, “Postscript,” 6, 7.
[108] *Routledge Handbook of Surveillance Studies*, 22.

dominant model for the organization of society, Deleuze’s theory of modulatory power has become a significant frame for academic understandings of the effects of pervasive data gathering enabled by ever-growing networked surveillance technologies.

In this chapter we looked at four theorists of surveillance – Jeremy Bentham, Michel Foucault, Frederick Winslow Taylor, and Gilles Deleuze – in light of their significant influence in shaping the trans-disciplinary field of surveillance studies. It should be noted, though, that while all four describe the logic of certain surveillance operations, it may be said that Bentham and Taylor were actual proponents of surveillance, influencing some practices as we will see in Chapter 3. Conversely, Foucault and Deleuze were simply analysts, with reservations about whether surveillance is actually good or not for society.

Chapter 2: Surveillance in its Present-day Capacity

This chapter consists of a broad overview of the empirical data on surveillance in three different levels – National, City, and Personal. As the scope of the study of surveillance practices in these levels is particularly vast (including a survey of COVID-19's impact in each – a development which is still unfolding as of this writing), the main objective of tis chapter is to outline the *general* trends. For all levels, the countries/governments, cities/corporations, and social networks cited were selected with the objective of featuring a wide range of societies, including countries with different regimes, cities with differing levels of development, and so on. Before delving into each level, however, this chapter begins with the developments in technology which have significantly changed the overall surveillance apparatus, and secondly at why the COVID-19 pandemic is a key consideration with respect to the development and employment of such systems.

The Difference Technology Makes

Surveillance practices have always been involved in social life, and with the advancement of modernity along with that of a centralized bureaucratic state their scope has especially widened. The British social theorist Anthony Giddens argues that surveillance is an essential feature of modernity, constituting one of its four "institutional clusterings," together with industrial production, centralized control of the modes of violence, and capitalist enterprise.[109] It may even be said that surveillance spans all aforementioned aspects of modernity in the sense that it has been

[109] Anthony Giddens, *The Nation State and Violence* (Cambridge: Polity Press, 1985), PDF version, 4.

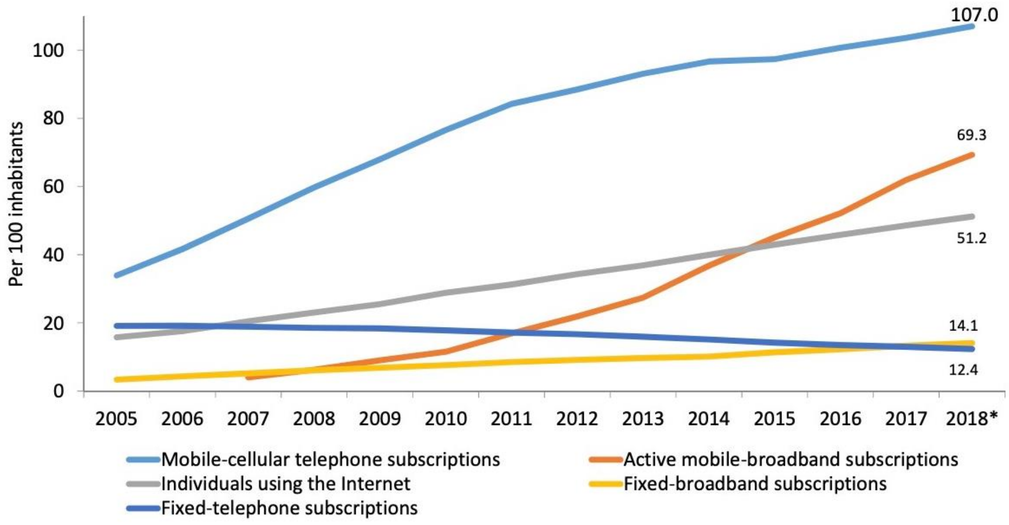
fundamental to the use of the modes of violence, to the operation of industries, and to the functioning of capitalism. In fact, even the most primitive societies engaged in different forms of surveillance practices, according to a few ethnographic studies,[110] albeit essentially executed face-to-face. As Alan Westin points out in *Privacy and Freedom*, social systems which create norms – and this is the case for all human societies – always involve mechanisms that can enforce them. Thus, in efforts to identify those who do and do not conform to such norms, all societies employ some form of watching conduct.[111]

Haggerty and Ericson observed that surveillance technology has, in the intervening decades, outperformed even George Orwell's dystopic vision[112] considering that the digital evolutions of the late 20th century and onwards illustrate a definite upsurge in the extent and nature of surveillance operations. During the latter half of the 20th century, personal information took on an unparalleled political, economic, and cultural significance, of which the move to computerized record-keeping was the single most important determinant.[113] The advent of widespread Information and Communication Technologies (ICT) – like the computer, the internet as it grew from web 1.0 to 4.0,[114] and the mobile phone – have expanded the capacities for record gathering

[110] Alan Westin, *Privacy and Freedom* (New York: Ig Publishing, 1967), PDF version, 7.
[111] Ibid., 13.
[112] Haggerty & Ericson, "The Surveillant Assemblage," *British Journal of Sociology* 51, no. 4 (2000): 606. https://www.uio.no/studier/emner/matnat/ifi/INF3700/v17/bakgrunnsnotat/the_surveillant_assemblage.pdf
[113] *Routledge Handbook of Surveillance Studies*, 22.
[114] Web 1.0 refers to the "read-only" web, wherein users' access to the internet was limited to viewing material from static web pages linked together by hyperlinks. Online 2.0 is the "interactive" web, in which users are able to read and create information as well as communicate with others on social media platforms. Web 3.0 is considered by many as the contextual web seeing that it provides information and services suited to the user. Web 3.0 is able to determine what content is valuable and relevant and what is not using algorithmic decision-making (such as fake news or spam). Web 4.0 is Web 3.0's mobile and embedded version.

as well as dissemination seeing that they enable the maintenance, storage, linking and searching of databases, thus resulting in a great expansion of surveillance capacities in multiple ways. According to data gathered by the International Telecommunication Union (ITU), the trends in the access to and use of ICTs are mostly positive.[115] As of 2018 more than half of the world's population is online. The usage of such technology has had an increasing trend except in regards to non-digital fixed-telephone subscriptions, home internet connectivity is getting more traction, and subscriptions to mobile telephones continue to rise (there are already more mobile-phone subscriptions than the global population), as shown in the figure below:

Chart 1.1: Global ICT developments, 2005–2018*



Note: * ITU estimate.
Source: ITU.

Source: Measuring the Information Society Report 2018 Volume 1, 50. https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf

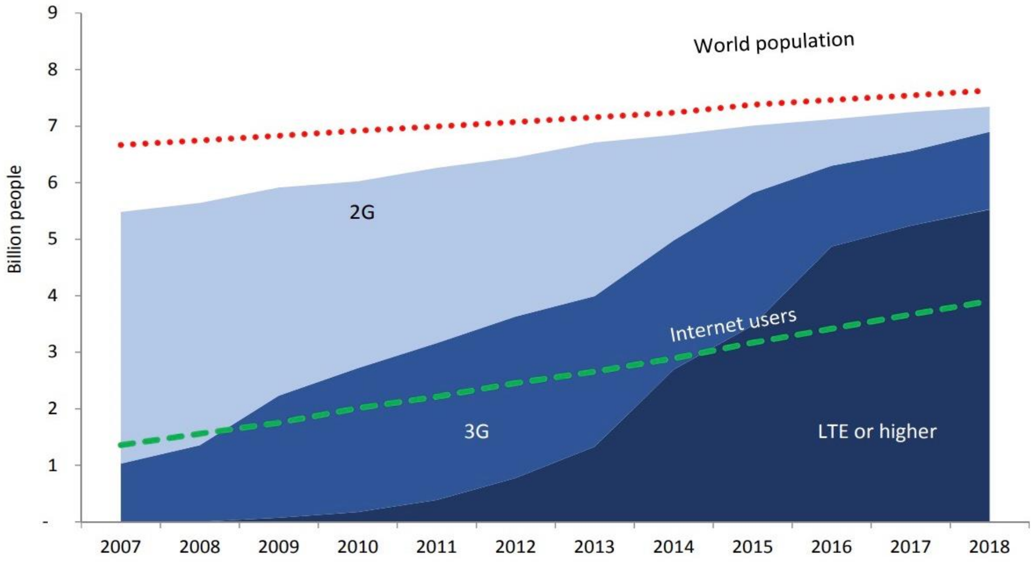
[115] Measuring the Information Society Report 2018, volume 1, 3. https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf

Broadband technologies, which allow wide bandwidth data to be transmitted over a high-speed internet connection, have brought noticeable economic impacts. Between 2010 and 2017, on average, a 1% increase in fixed-broadband coverage is related with a 0.08% increase in gross domestic product (GDP), and a 1% rise in mobile broadband adoption is connected with a 0.15% boost in GDP.[116] So, it seems reasonable to assume that countries have aimed to provide their citizens with access to such technologies in order to expand the world's interconnectivity and further expedite administrative and economic endeavors. Depicted in the next figure, almost everyone on the planet (until 2018) has access to a mobile-cellular network signal. Moreover, the majority of people can connect to the Internet via a 3G or higher-quality network,[117] which hints at the amount of data capture that is achievable in a world almost fully covered by access to the internet:

[116] Measuring the Information Society Report 2018, volume 1, 6, 8.

[117] [117] Measuring the Information Society Report 2018, 8-9.

Chart 1.14: Mobile coverage by type of network, 2007–2018*



Note: * ITU estimate.
Source: ITU.

Accordingly, the emergence and utility of networks, databases, and algorithms of the information society have revamped data from being difficult to access and costly, to now being widely, regularly, remotely, and automatically collected. As surveillance practices become progressively accessible, practicable, and compelling, the aims and methods of monitoring persons likewise increase, underscoring the distributed nature of surveillance operations which cover management, publicity, political and security strategies. In this fashion, "computer algorithms are becoming interwoven with every manner of human activity and practice,"[118] driving the monitorization of persons to be all the more fruitful and ubiquitous.

[118] William Hasselberger, "Ethics beyond Computation: Why We Can't (and Shouldn't) Replace Human Moral Judgement with Algorithms," *Social Research: An International Quarterly* 86, no. 4 (2019): 977.

The Scottish sociologist and surveillance theorist David Lyon argues that[119] any understanding of modern forms of surveillance requires an analysis of emerging technologies, and outlines in four points the consequences of electronic surveillance, which he believes to have provoked major changes in the political, economic, and cultural spheres. First, the availability of more precise and larger data files. Second, an increased dispersion of monitorization, extending surveillance to nearly every space. Third, a boost in the tempo of data-flows.[120] Fourth, the amplification of consumers, workers, and citizens' visibility and transparency.[121]

A more recent development which has become increasingly applied to surveillance tasks is Artificial Intelligence (AI). Generally speaking, AI is defined by MIT Technology Review as the "quest to build machines that can reason, learn, and act intelligently,"[122] but it does not correspond to one particular technology. Rather, as the Carnegie Endowment for International Peace suggests, it is more accurate to consider AI "as an integrated system that incorporates information acquisition objectives, logical reasoning principles, and self-correction capacities."[123]

Following the Industrial Revolution, the technological developments that mushroomed from the Digital Revolution facilitated advances with the aim of supplanting native human capabilities with

[119] David Lyon, *The Electronic Eye: The Rise of Surveillance Society*, 40-53.
[120] Data-flows essentially refer to the transfer of information from one part of the system to another.
[121] Lyon, *The Electronic Eye*, 55-56.
[122] MIT Technology Review, "Artificial Intelligence," https://www.technologyreview.com/topic/artificial-intelligence/
[123] Steven Feldstein, *The Global Expansion of AI Surveillance*, Washington: Carnegie Endowment for International Peace, 2019, PDF version, 5 https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf .

machine power as it bolstered the belief in boundless technological progress.[124] In the beginning, automated machines could only replace physical capabilities, whereas now AI also supplies cognitive abilities which is what allows algorithms to perform routine, specialized, and predictable tasks.[125] New performances in Artificial Intelligence are now feasible given the many technological breakthroughs of the last decade, namely online data collection and cloud computing; Machine Learning (ML) advancements and the emergence of Deep Learning (DL); enhanced performance of complicated algorithms; a new generation of computer hardware and smart microchips; and market-driven incentives for new AI applications.[126]

It may be argued that contemporary Machine-learning AI is just not viable without surveillance. To train algorithms to spot patterns and make judgments, AI applications rely on massive amounts of data – data which provides the training set to generate and adjust the AI algorithms. Without data to learn from, AI cannot autonomously complete the tasks it is required to, and without scouring given sources for information, in other words, practicing surveillance, it cannot gather such data. Much of it is taken from customers or users (e.g. internet users) without their knowledge. Internet corporations watch our clicks to figure out what news articles, products, and advertisements we like. Facebook, for example, recently stated that it will begin utilizing user's

[124] Josh Lauer, "Surveillance history and the history of new media: An evidential paradigm," *New Media Society* 4, no. 14 (2012): 578.
[125] Martin Ford, *Rise of the Robots: Technology and the Threat of a Jobless Future* (New York: Basic Books, 2015), PDF version, 73.
[126] Feldstein, *The Global Expansion of AI Surveillance*, 5; see also, WhiteHouse.gov, "Preparing for the Future of Artificial Intelligence," https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

posted videos to train AI algorithms.[127] Nevertheless, surveillance is not just a source of power for algorithms, it is also a service for which they are being deployed.

The application of AI to cameras has taken surveillance a step further as it allows AI to perform deep learning and visual analysis without the need for human intervention. AI-powered facial recognition technology (FRT), for instance, has already begun to change the access control business. A camera that includes FRT backed by AI can be used in conjunction with an access control device to detect faces and, as a result, provide a frictionless manner for people to get access to a secure location. Whereas analogue and traditional video surveillance may have turned out inefficient and costly considering issues related to, for instance, too many screens for a single monitoring operator to keep track of, the recent creation of smart cameras – powered by big data, internet of things, AI, and cloud services – assures a solution to these issues with algorithmic layers adept in automatically and autonomously identifying and detecting license plates, faces, behaviors, suspicious objects, and even attitudes in video footage. What's more, rather than the preceding in-your-face surveillance which allows recognition from the watched, the data-driven methods that technological progress enable adds to the conundrum of visibility – "human subjects become more transparent to surveillance systems that become less transparent."[128]

Given the present pervasiveness of technology in all aspects of human life, the never-ceasing generation and capture of data produces an economy of personal information unlike anything

[127] Facebook AI, "Learning from videos to understand the world," https://ai.facebook.com/blog/learning-from-videos-to-understand-the-world/

[128] Sun-Ha Hong, *Technologies of Speculation: The Limits of Knowledge in a Data-drive Society* (New York: New York University Press, 2020), PDF version, 61.

witnessed heretofore.[129] Such an economy is propelled by surveillance systems that gather data and then analyze it for patterns and associations considered relevant, and as they become increasingly automated their ubiquity and activity are also raised, markedly transforming basic patterns of institutional, governmental, and commercial conduct. The developments in corporate, material, and administrative infrastructures alongside data-handling, data-manipulation and technologies have, as Lyon, Haggerty, and Ball assert, conquered historical limitations to vision. These developments in surveillance have "produced downstream social changes in the dynamics of power, identity, institutional practice, and interpersonal relations on a scale comparable to the changes brought by industrialization, globalization, or the historical rise of urbanization."[130]

By virtue of society's "datafication," surveillance combines the monitorization of both physical and digital spaces. In addition to government and corporate surveillance, these hybrid surveillance settings also contain self-surveillance as well as intricate forms of watching and being watched via social media and the associated paradigm of voluntary data distribution. Hence, it is relevant to analyze the current extent and nature of surveillance on three distinct levels. But first, a note on the relevance of the global COVID-19 crisis for these questions.

COVID-19: An Accelerator of Technological Influence

Following the global COVID-19 pandemic of 2020, governments and corporations all around the world are implementing extraordinary data-gathering tactics in order to both stem the spread of

[129] Ball, Haggerty, and Lyon, ed., *Routledge Handbook of Surveillance Studies*, 321.
[130] *Routledge Handbook of Surveillance Studies*, 1.

COVID-19 and transition to a safer and more economically secure future. During a time of lockdowns and physical distancing, digital technologies are helping to communicate real-time life-saving information, ensure the continuance of crucial public services (such as online education, for instance), and bridge social isolation.

Governments have used a number of strategies to “flatten the curve,” to lower infection, hospitalization, and, ultimately, death rates. These include instructions to stay at home, mask requirements, and social isolation. Essentially, the solutions focus on measurement and monitorization, which place a greater emphasis on modifying individual behavior than in changing workplace settings to make them safer. A new, nearly universal adoption of contagion and disease surveillance has numerous ramifications. Surveillance becomes a trade-off for normalcy as the accepted narrative implies that comprehensive testing, screening, and tracking of persons is vital to safeguard them and will allow a return to some sense of normalcy.

Emergencies, such as the current pandemic, tend to accelerate historical processes. In the race to comprehend and control the virus, new uses of data and resulting technologies are being developed at breakneck speed. As historian Yuval Noah Harari asserts,[131] decisions that would normally take years to make are now made in a few hours, often without democratic debate. Because the risks of doing nothing are greater, dangerous and inexperienced technologies are rushed into service. In large-scale social exercises, entire countries become experimental subjects. In this sense, the future

[131] Yuval Noah Harari, "The World After Coronavirus," *Financial Times*, March 20, 2020, 1-15, 1. https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

landscape of the world may be one very different from the one we lived in prior to COVID-19 since it “will influence global politics and society as other diseases have in the past.”[132]

The global spread of COVID-19 adds a new wrinkle to the debate over surveillance and privacy. Face masks used to avoid infection have the unintended consequence of impeding facial recognition technology, while mobile phone apps used to trace and track an individual’s interaction with the virus have the ability to capture personal data not necessarily relevant to health. The Coronavirus outbreak — and the resulting demand for timely public health data — has paved the way for data collecting and tracking on a scale that would have been unthinkable before. Therefore, it is important to look at how and to what extent COVID-19 is influencing surveillance practices and the implementation of technology in each level of analysis of the subsequent sections.

2.1. Surveillance: National level (Government Surveillance)

According to Kevin D. Haggerty and Minas Samatas,[133] surveillance has become essential to human epistemological and organizational undertakings and is a linchpin of governmental operations in a variety of institutional realms. The attacks of 9/11 engendered a decisive uptake in surveillance systems, marking what Shoshana Zuboff labels “surveillance exceptionalism”[134] seeing that existing surveillance practices were beefed up and earlier limits rescinded as a pretext

[132] Jeffrey D. Sachs, *The Ages of Globalization* (New York: Columbia University Press, 2020), PDF version, X.

[133] Kevin D. Haggerty and Minas Samatas, eds., *Surveillance and Democracy* (Abingdon: Routledge, 2010), PDF version.

[134] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (New York: PublicAffairs, 2019), PDF version, 101-104.

for the “war on terror.” Subsequently, the terrorist attacks spurred a momentous restructuring of the surveillance field, incorporating legislation to expedite state surveillance, political and financial commitments to advanced surveillance technologies and programs, rearrangement of government activities to prioritize national security, and search of assorted public-private partnerships for security’s provision.[135]

From counter-terrorism and policing to crisis management and critical infrastructure protections, the concept of security has since then been expanded to encompass the full policy range of the coercive state apparatus. Moreover, non-coercive aspects of public policy are likewise being “securitized” and reorganized into new paradigms of, for example, transport security, food security, energy security, cyber-security, and so forth, consequently reshaping how these issues are framed and approached by policy makers – a reconfiguration of public policy and state practice of which surveillance is at the heart.[136] The amped security-focused landscape post-9/11, coupled with globalization of the economy which prompted major advancement and globalization of industrial and technology sectors has amounted to what Ben Hayes terms the “surveillance-industrial complex” – government outsourcing of security activities to private entities. A former European Commissioner for Justice and Home Affairs explains:

[135] *Routledge Handbook of Surveillance Studies*, 285.
[136] *Routledge Handbook of Surveillance Studies*, 168-169.

> Security is no longer a monopoly that belongs to public administrations, but a common good, for which responsibility and implementation should be shared by public and private bodies.[137]

The convergence of techno-security and state-corporate agendas foments a potentially problematic dynamic wherein political decisions are conditioned not only by democratic consideration for the public good, but also by profitable procedures for private corporations, hence inciting surveillance's present multifaceted nature.

From a geopolitical standpoint, countries are engaging in a sort of arms race to be at the vanguard of innovation in relation to automated and algorithmic decision-making based on Big Data. Considering that "great power competition has always been defined by technological edge,"[138] AI is sure to influence global competitiveness in the next few years, promising to give early adopters a considerable strategic and economic advantage. National governments have begun to put AI-targeted regulations in place in order to maximize the technologys promise while also addressing its social and ethical ramifications.[139] The progressive salience given by governments in developing AI capabilities is demonstrated by the sheer number of times Artificial Intelligence (AI) and Machine Learning (ML) were mentioned in congressional and parliamentary records. The

[137] Ibid., 169.

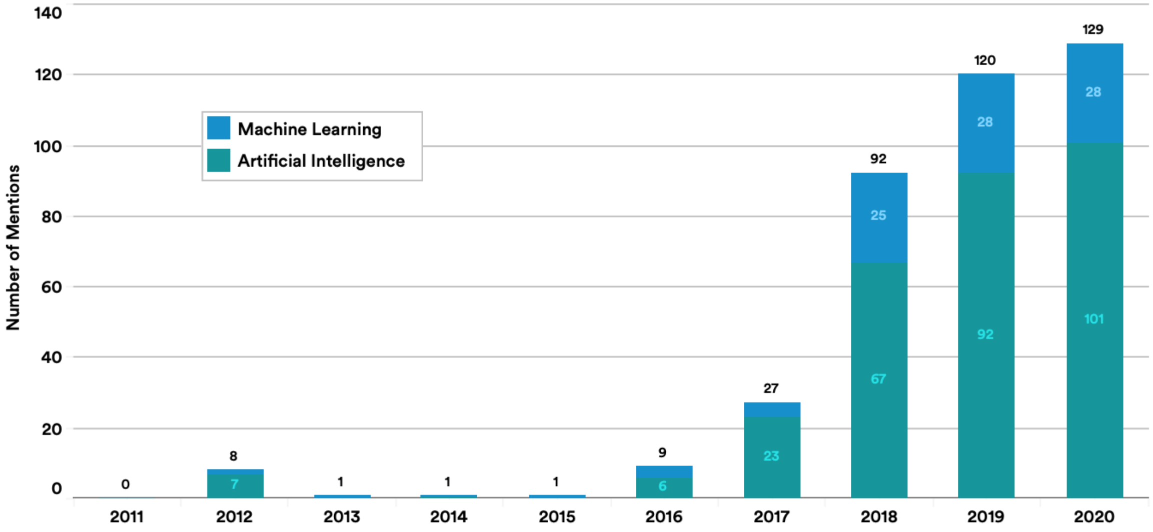
[138] Anja Manuel, "US, Europe and UK must unite to keep Chinese tech at bay: Great Powers always triumph thanks to their technological edge. Today is no different," *Financial Times*, October 2020. https://www.ft.com/content/bc7abf86-f13e-4025-a120-004361aef21a

[139] Daniel Zhang et al., "The AI Index 2021 Annual Report," *AI Index Steering Committee, Human-Centered AI Institute, Stanford University*, March 2021, 153, https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report_Master.pdf

next two figures outline the number of AI and ML mentions in the proceedings of U.S. Congress and U.K. Parliament from 2011 to 2020, respectively:

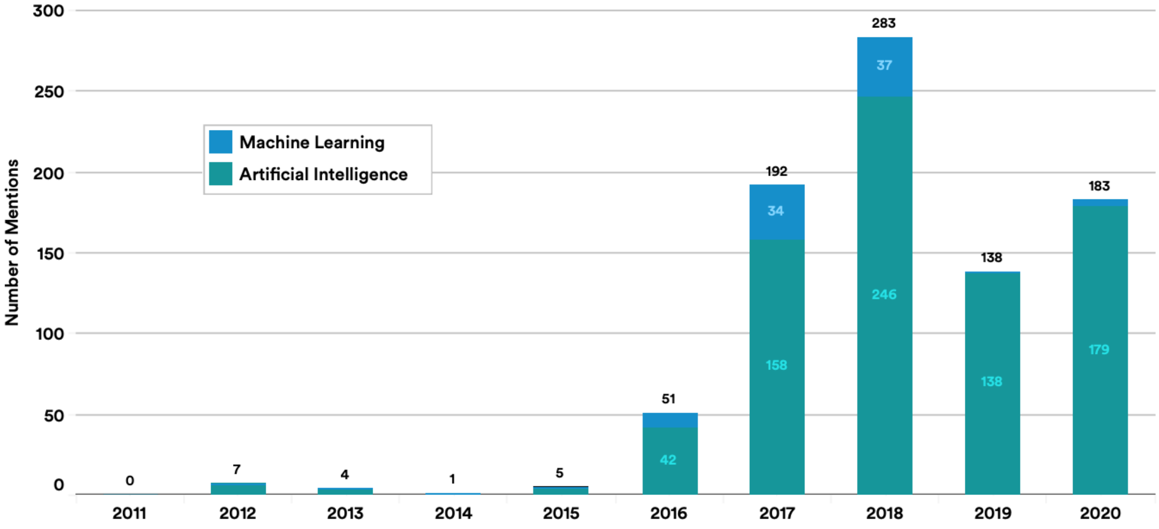
MENTIONS of AI and ML in the PROCEEDINGS of U.S. CONGRESS, 2011-20

Sources: U.S. Congressional Record website, the McKinsey Global Institute, 2020 | Chart: 2021 AI Index Report



MENTIONS of AI and ML in the PROCEEDINGS of U.K. PARLIAMENT, 2011-20

Sources: Parliament of U.K. website, the McKinsey Global Institute, 2020 | Chart: 2021 AI Index Report



In just five years, Artificial Intelligence went from barely mentioned to over a hundred mentions, of which the 116th U.S. Congress was "the most AI-focused congressional session in history."[140] Given governments' clear concern with AI, it isn't surprising then that countries throughout the world are developing policies and initiatives to integrate governmental and intergovernmental efforts in order to guide and support AI development. There are 32 countries that have announced AI strategies and 22 that are producing AI strategies at the moment.[141]

The *Pan Canadian AI Strategy*, published by the Canadian Institute for Advanced Research in 2017, was the first National AI strategy paper published. The Canadian approach focuses on training the country's future AI workforce, supporting significant AI innovation hubs and scientific research, and establishing Canada as a thought leader on the economic, ethical, policy, and legal consequences of AI.[142] CIFAR's annual report,[143] released in November 2020, highlighted significant expansion in Canada's AI ecosystem, as well as activities and research connected to healthcare and AI's influence on society, among other strategy outcomes.

In the same year, China released *A Next Generation Artificial Intelligence Plan*, published by the State Council for the People's Republic of China (PRC). China has one of the most comprehensive AI strategies in the world. It covers research and development, along with talent development through skill training and education, as well as ethical principles and national security concerns,

[140] Daniel Zhang et al., "The AI Index 2021 Annual Report," 172, https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report_Master.pdf
[141] Ibid., 155.
[142] CIFAR, "Pan-Canadian AI Strategy," https://cifar.ca/ai/
[143] CIFAR, "Pan-Canadian AI Strategy Impact Report (AICAN 2020)," https://cifar.ca/wp-content/uploads/2020/11/AICan-2020-CIFAR-Pan-Canadian-AI-Strategy-Impact-Report.pdf

including control and security for the Chinese Communist Party (CCP). It sets specific goals, such as putting AI in line with competitors by 2020, becoming the global leader in domains like voice and image recognition, and others by 2025, and becoming the principal center for AI innovation by 2030.[144] In February 2019, China established a New Generation AI Innovation and Development Zone,[145] and in May 2019, a multi-stakeholder coalition comprised of academic institutions and private-sector entities such as Tencent and Baidu announced the "Beijing AI Principles."[146]

The French AI Strategy entails creating an aggressive big data policy, focusing on four strategic sectors: health care, the environment, transportation, and defense; increasing French research and development efforts; preparing for the impact of AI on the labor force; and ensuring diversity and inclusivity in the field.[147]

The National Strategy for the Development of Artificial Intelligence, published by the Government of the Russian Federation, emphasizes the country's national interests and establishes recommendations for the development of an "information society" until 2030. A national technology effort, departmental projects for federal executive bodies, and programs like the Russian Federation's Digital Economy are all aimed at implementing the AI framework across

[144] China's State Council, "A Next Generation Artificial Intelligence Development Plan," https://na-production.s3.amazonaws.com/documents/translation-fulltext-8.1.17.pdf
[145] China.org.cn, "National New-Generation AI Innovation & Development Pilot Zone established in Beijing," http://www.china.org.cn/china/2019-02/22/content_74493744.htm
[146] BAAI, "Beijing AI Principles," https://www.baai.ac.cn/news/beijing-ai-principles-en.html
[147] AI for Humanity, "French Strategy for Artificial Intelligence," https://www.aiforhumanity.fr/en/

sectors.[148] Russian President Vladimir Putin attended the Artificial Intelligence Journey Conference in December 2020, where he proposed four AI policy ideas: developing experimental legal frameworks aimed at the use of AI, providing neural network creators with competitive access to big data, evolving practical measures to present AI algorithms, and improving private investment in domestic AI.[149]

Without getting into further details on the aforementioned and other countries' national strategies for AI, it is clear that AI's impact extends beyond individual consumer decisions as it is beginning to alter basic governance patterns. Not only does AI provide governments with unmatched capabilities to track and shape citizens' choices, but also offers them new capabilities to promote false information and disrupt elections, to name a few examples. To develop AI and extend its application to all spheres of life, while leaving governments better equipped to further their political goals for the flourishing of society, also leaves them better able to perpetuate illiberal schemes, processes which become increasingly opaque where these technologies are concerned.

According to *The Global Expansion of AI Surveillance*, a Carnegie Endowment for International Peace report, an increasing number of nations are using powerful AI surveillance technologies to track and monitor individuals in order to achieve a variety of policy goals – "some lawful, others that violate human rights, and many of which fall into a murky middle ground."[150] The goal of the research is to find out which nations are taking up AI surveillance technology, what forms of AI

[148] Kremlin, "On the development of artificial intelligence in the Russian Federation," http://www.kremlin.ru/acts/bank/44731/page/1
[149] Kremlin, "Artificial Intelligence Conference," http://en.kremlin.ru/events/president/news/64545
[150] *The Global Expansion of AI Surveillance*, 1.

surveillance are being employed by governments, and which companies and countries are providing such technology, for which the answers culminate in the creation of the AI Global Surveillance (AIGS) Index.

Distinguishing the use of AI surveillance tools between three subcategories, namely smart/safe city, facial recognition systems, and smart policing, the AIGS Index documents that, up to 2019, at least 75 out of 176 nations are actively deploying AI technology for surveillance, of which 56 are engaged in smart/safe city platforms, 64 in facial recognition systems, and 52 in smart policing.[151] *Smart/safe cities* have sensors that communicate real-time data to help with public safety, city management, and service delivery. Facial recognition cameras, sensors, and police body cameras are all connected to intelligent command centers in "safe cities" to respond to emergencies, ensure public safety, and prevent crime. *Facial recognition systems* involve biometric technologies[152] that match live or recorded footage of individuals with photos from databases using cameras (video or still images). Some systems go further and examine aggregate demographic trends or undertake broader sentiment analysis through facial recognition crowd scanning, so not all systems focus solely on database matching. *Smart Policing* involves data-driven analytic technology that is utilized to aid police response and investigations. Some systems feature algorithmic analysis to make forecasts regarding future crimes.[153]

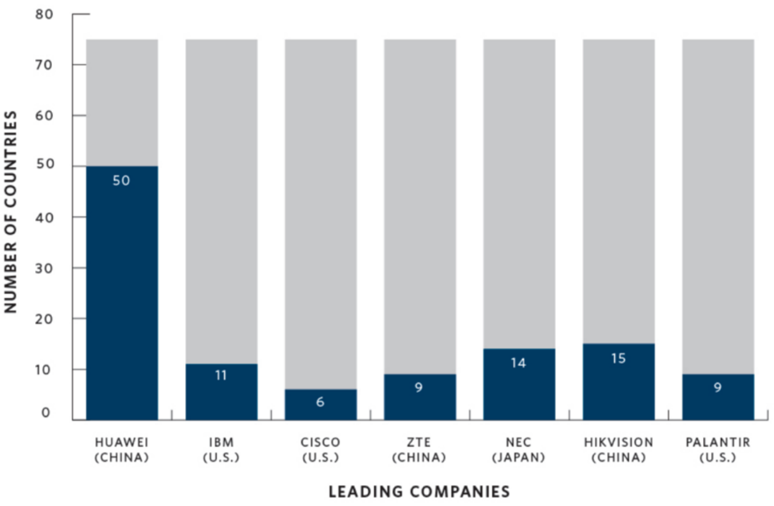
[151] *The Global Expansion of AI Surveillance*,, 7.

[152] Curiously, from 2014 to 2018 the failure rate of facial recognition went from 4.0% to 0.2%. NIST, "NIST Evaluation Shows Advance in Face Recognition Software's Capabilities," https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities

[153] *The Global Expansion of AI Surveillance*, 16-21.

The adoption of AI surveillance is rapidly gaining traction. According to the report "Freedom on the Net 2018," 18 of the 65 countries analyzed were adopting AI surveillance tools developed by Chinese corporations.[154] After just one year, the AIGS Index reveals that 47 of the 65[155] are now taking up Chinese-produced AI surveillance technologies. The next figure shows how many countries each tech company is supplying AI surveillance technology to. Evidently, China is the biggest supplier of AI surveillance at the moment, with Chinese technology present in at least 63 countries. Nevertheless, other countries are also delivering sophisticated surveillance technology, namely Japan, Germany, France, and the U.S., with the latter having a surveillance-technological presence in 26 countries.

Leading Companies Contributing to AI Surveillance



NOTE: The AIGS Index tracks seventy-five countries that employ AI surveillance. The numbers here reflect how many of those countries each company is present in.

[154] Freedom House, *Freedom on the Net* 2018, 9. https://freedomhouse.org/sites/default/files/FOTN_2018_Final.pdf

[155] *The Global Expansion of AI Surveillance*, 8.

When it comes to finding an association between regime type and procurement of AI surveillance technology, it would seem reasonable to expect that authoritarian countries would lead in such acquisitions given these regimes' disregard for privacy and human rights, as well as the convenience and cost-effectiveness such technologies bring to enforcing and perpetuating repressive forces.[156] However, while autocratic governments are securing advanced monitoring capabilities, so are democratic governments. According to the AIGS Index, AI surveillance systems are being deployed by 51% of liberal democracies, whereas only 37% of closed autocracies, 41% of electoral autocracies, and 41% of electoral democracies are employing such systems.[157] Therefore, since many democracies and autocracies are embracing this technology, it becomes clear that regime type is not a reliable predictor for ascertaining which governments will power their monitoring apparatuses with AI. Though it should be noted that regime type may influence whether such technology is used in ways that violate human rights.

However, the AIGS Index does demonstrate a substantial link between military spending and the usage of AI surveillance technology by governments. Of the top 50 military spending nations, 40 are applying AI surveillance systems, which includes both affluent and poorer states, and contains the full range of regime types.[158] India, Japan, Saudi Arabia, Spain, Singapore, Israel and the United Kingdom represent some of the countries with high military spending using AI surveillance

[156] Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright, "The Digital Dictators: How Technology Strengthens Autocracy," *Foreign Affairs* 99, no. 2 (2020): 111 – 112, https://www.foreignaffairs.com/system/files/pdf/articles/2020/99210.pdf
[157] *The Global Expansion of AI Surveillance*, 8.
[158] Ibid., 11.

technology.[159] This observation is not unexpected when one considers that countries that invest widely in their military usually have stronger technological and economic capabilities, as well as specific threats to be concerned about. It should then come as no surprise that a state that takes its security seriously and is keen to allocate significant resources towards maintaining formidable military-security capabilities will seek out the latest AI and surveillance techniques.

Of the 75 countries employing AI surveillance, there are 35 using all forms of AI surveillance – safe/smart city, smart policing, and facial recognition technology. Of those 35, 12 are liberal democracies,[160] 13 electoral democracies,[161] 4 closed autocracies,[162] 6 electoral autocracies,[163] and from those, 17 are countries that are part of the Chinese government's Belt and Road Initiative (BRI). It should be noted, however, that there is a caveat when dealing with empirical data on the employment of AI surveillance around the world, which is that both governments and corporations deliberately disguise their surveillance capabilities, making it quite challenging to accurately determine what governments are attempting in the surveillance sector as well as what are the associated effects.[164]

Of course, the pursuit of sustained technological progress, including in AI and surveillance, already existed prior to the COVID-19 pandemic, and we've already seen that many countries are,

[159] SIPRI, "Military Expenditure Database," https://www.sipri.org/databases/milex

[160] Australia, Denmark, France, Germany, Japan, Malta, Netherlands, South Korea, Spain, United Kingdom, United States, Uruguay.

[161] Bolivia, Brazil, Colombia, Ecuador, India, Indonesia, Israel, Malaysia, Mexico, Panama, Philippines, Singapore, South Africa.

[162] China, Qatar, Saudi Arabia, United Arab Emirates.

[163] Bangladesh, Kazakhstan, Kenya, Kyrgyzstan, Pakistan, Russia.

[164] *The Global Expansion of AI Surveillance*, 8.

indeed, adopting systems of omnipresent surveillance. This trend has, however, been supercharged by the outbreak of COVID-19 as governments are undertaking experimental systems that they allege will upgrade operational efficiency.[165] Since then, authorities have accelerated efforts to introduce further automated forms of decision-making, and, hence, Big Data collection and surveillance.

While traditional public health surveillance actions, such as contact tracing and quarantines, were used in the fight to stem COVID-19, these responses were distinctively enhanced with the use of various technologies, such as data networks, smartphone location data, big data analysis, ankle bracelets, and drones. Not only are existing technologies being employed to track and monitor citizens, they are also undergoing major developments for improved utility, accuracy and adaptability in applications toward managing the COVID-19 health response. Facial Recognition Technology, for example, hit a bump in the road when its sudden inability to detect faces came to the forefront due to global mask-wearing. As a result, it has already been improved and adapted to present circumstances.[166]

To help with symptom tracking and contact tracing, a slew of smart phone apps have been developed. Police, military, and government surveillance activities to ensure people are complying with COVID-19 regulations have also been considerably expanded.

[165] Siddharth Venkataramakrishnan, "Algorithms and the coronavirus pandemic," *Financial Times*, January 2021, 6. https://www.ft.com/content/16f4ded0-e86b-4f77-8b05-67d555838941

[166] Martin Pollard, "Even mask-wearers can be IDd, China facial recognition firm says," *Reuters*, March 2020, https://www.reuters.com/article/us-health-coronavirus-facial-recognition-idUSKBN20W0WL; James Clayton, "Facial recognition beats the Covid-mask challenge," *BBC*, March 2021, https://www.bbc.com/news/technology-56517033

In **Australia**, the use of digital technology by government to mediate relations with citizens is becoming more common. In April 2020, COVIDSafe,[167] an automated mobile contact-tracing app, was launched. The program is voluntary and was created to aid the government manual contact-tracing efforts. When a person with the app downloaded tests positive for COVID-19, their state of residence's health department is notified, and the infected user's consent is sought to download the previous 14 days of the relevant phone's contact data from a storage of centralized national data. It is worth noting that the Federal Minister for Government Services has officially stated that,[168] once the pandemic has ended, the national data store will be removed, and that users should delete the tracing app. For COVID-19-related policy-making, the government has mostly relied on the Biosecurity Act 2015[169] to issue regulations and determinations, some of which have resulted in the introduction of additional police powers to enforce social distance and other specifications. At least one Australian state's police have announced plans to use drones to aid their implementation of restrictions.[170] Curiously, some Australian news programs have used CCTV footage of citizens breaching quarantine, exposing these individuals to "name and shame" them.[171]

[167] Australian Government Department of Health, "COVIDSafe App," https://www.health.gov.au/resources/apps-and-tools/covidsafe-app
[168] Ry Crozier, "Govt to release source code of forthcoming 'COVID trace' app," *itnews*, April 2020, https://www.itnews.com.au/%20news/govt-to-release-sourcecode-of-forthcoming-covid-traceapp-546884
[169] Federal Register of Legislation, "Biosecurity Act 2015," https://www.legislation.gov.au/Details/C2020C00127
[170] Michael Richardson, "'Pandemic drones': useful for enforcing social distancing, or for creating a police state?" *The Conversation*, March 2020, https://theconversation.com/pandemic-drones-useful-for-enforcing-social-distancing-or-for-creating-a-police-state-134667
[171] 9 News Australia, "Woman caught breaching home isolation," *Youtube*, Video File, August 18, 2021, https://www.youtube.com/watch?v=3yuTrgR30eg

Argued by Francis Fukuyama, a country's resilience to the coronavirus has less to do with the dichotomy between democracies and autocracies, and more with "the state's capacity and, above all, trust in government."[172] In this respect, **China** has taken a strategy to gain trust in and public acceptance of the government's use of digital technologies by emphasizing nationalism and patriotism. The so-called "Great Firewall of China," or system of state internet censorship, discerns between individuals who can and cannot penetrate the wall to access restricted content, resulting in varying levels of information freedom and so conditioning the Chinese ideological spectrum.[173] Social media sites which algorithmically highlighted posts favorable to the Chinese Communist Party (CCP) showed citizens their effective role in halting the pandemic and fomented a nationalist climate as the population internalized the state's interests as their own good.[174] While the country was already adopting patterns of technological social governance, with online censorship, facial recognition, social media, and the social credit system – all of which AI and surveillance are fundamental components – these technologies represent significant measures in the battle against COVID-19 by assisting the prediction of outbreaks, assuring prompt food and medicine supplies, identifying quarantine violators, and providing online medical consultations.[175] China's practice

[172] Francis Fukuyama, "The Thing That Determines a Country's Resistance to the Coronavirus," *The Atlantic*, March 2020, https://www.theatlantic.com/ideas/archive/2020/03/thing-determines-how-well-countries-respond-coronavirus/609025/

[173] Kristin Shi-Kupfer, Mareike Ohlberg, Simon Lang, and Bertram Lang, "Ideas and Ideologies Competing for China's Political Future," *Mercator Institute for China Studies* 5, October 2017, PDF version, 10, https://merics.org/sites/default/files/2020-04/171004_MPOC_05_Ideologies_0_web_1.pdf

[174] Zifeng Chen and Clyde Yichen Wang, "The Discipline of Happiness: The Foucauldian Use of the "Positive Energy" Discourse in China's Ideological Works," *Journal of Current Chinese Affairs* 48, no. 2 (2020): 201 https://journals.sagepub.com/doi/pdf/10.1177/1868102619899409

[175] Olivia Shen, "Coronavirus and Techno-Authoritarianism," *The China Story*, May 2020. https://www.thechinastory.org/coronavirus-and-techno-authoritarianism/

of mass datafication has strengthened the effectiveness of these programs. In addition to China's well-known ambition of reaching global supremacy in AI by 2030, it is worth underscoring that ensuring health tracking on mobile phones was said to be on the CCP's policy agenda.[176]

In the **Netherlands**, technology was already an essential part of government, both internally and in citizen-facing agencies. However, existing technologies are currently being repurposed and public-private associations are racing to produce an app aiding the pandemic response. Such partnerships are observed, for example, in the digital healthcare sector, with boosted efforts in data collection as well as sharing. Philips, Welfare and Sport, two Dutch Universities, and the Ministry of Health developed a virtual COVID-19 portal aimed at hospitals sharing patient data,[177] propelling the Dutch state to allow the distribution of patient data *without preceding consent*. Moreover, the development of COVID-19 treatments has involved active collaboration between medical universities and laboratories, which includes the application of AI-centered techniques.[178] In regards to policing, it should first be noted that Dutch law enforcement already possessed a strong tradition of tech-use for policing endeavors, including an extensive facial recognition system[179] (over 2.2 million images). As containment measures were comparably relaxed around

[176] Liza Lin, China's Plan to Make Permanent Health Tracking on Smartphones Stirs Concern," *The Wall Street Journal*, May 2020, https://www.wsj.com/articles/chinas-plan-to-make-permanent-health-tracking-on-smartphones-stirs-concern-11590422497

[177] Joost Maltha, "Philips launches national portal for digital exchange of COVID-19 patient data in the Netherlands," *Philips*, April 2020, https://www.philips.com/a-w/about/news/archive/standard/news/articles/2020/20200415-philips-launches-national-portal-for-digital-exchange-of-covid-19-patient-data-in-the-netherlands.html

[178] Weng Shen Cheung, "Amsterdam institutions leading AI collaboration to fight COVID-19," April 2020, https://www.iamsterdam.com/en/business/news-and-insights/news/2020/amsterdam-institutions-ai-collaboration-coronavirus

[179] DutchNews, "Dutch police facial recognition database includes 1.3 million people," https://www.dutchnews.nl/news/2019/07/dutch-police-facial-recognition-database-includes-1-3-million-people/

May 2020, the nature of such measures entail that police efforts focus on monitoring public spaces, with scan-vehicles,[180] drones,[181] and cameras.[182] As for contact tracing, seven apps were rolled out, but in light of data concerns and security flaws none were deemed appropriate for official use. Nonetheless, the State is decisive on producing an app, having since chosen to team up with technology giants like Google and Apple,[183] demonstrating the potential for taking advantage of their dominant market statuses when reaching a balance between their strategic interests as commercial businesses and public health objectives.

2.2. Surveillance: City level (Smart Cities and Workplace Surveillance)

In order to assess the world's most surveilled cities, Comparitech conducted a quantitative analysis based on how many public CCTV cameras exist in 150 cities around the world.[184] Globally, 770 million cameras are distributed throughout the world, with 54% of these residing in China alone. On a number-of-cameras-per-1,000-people basis, out of the 20 most surveilled cities in the world, London, Indore, Hyderabad, and Delhi are the only non-Chinese cities to top the list – meaning 11 of the 20 most surveilled cities are from China –, correspondingly placing third, fourth, twelfth,

[180] Woody Mcconaughey, "Unjustified parking fines by scan cars," *Netherlandsnewslive*, May 2021, https://netherlandsnewslive.com/unjustified-parking-fines-by-scan-cars-dailyauto-nl/164745/

[181] Kristel Vaan Teeffelen, "Drones check whether you comply with the corona rules, but is that actually allowed?" *Trouw*, April 2020, https://www.trouw.nl/nieuws/drones-controleren-of-u-zich-aan-de-coronaregels-houdt-maar-mag-dat-eigenlijk-wel~b3e551a4/

[182] Beveiliging News, "Rotterdam deploys camera trucks against 'corona offenders'," https://beveiligingnieuws.nl/nieuws/rotterdam-zet-camerawagens-in-tegen-corona-overtreders

[183] Rtl News, "'Dutch corona app will be tested in June,'" https://www.rtlnieuws.nl/tech/artikel/5135056/ontwerp-corona-app-nederland-design-github

[184] Comparitech, "The world's most surveilled cities," https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

and sixteenth. However, on a number-of-cameras-per-square-mile basis, only 11 Chinese cities make the top 20, joined by Delhi, London, Chennai, Singapore, Seoul, Moscow, New York, Mumbai, and Mexico City. Notably, Chennai, Delhi, and London have more cameras per square mile than any city in China, reflecting urban density against sprawling, spread-out cities.

At the National Level, several states are employing AI surveillance for what are called **"smart/safe city" programs**. According to the AIGS Index, out of the 75 countries using AI surveillance, 56 are directing it toward smart city endeavors. Although the smart city concept remains in flux and is interpreted and defined in different ways,[185] it can be said that its definitions generally involve the application of ICTs to improve urban service delivery, rationalizing cities and enhancing collective services through digital innovation.[186]

In the past decade, new and developing forms of surveillance have been adopted, or experimented with, in smart cities. These include drones with cameras, body-worn cameras, dash cams, along with forms of smart video surveillance like mobile phone tracking, behavioral detection software, cameras with facial recognition technology, predictive policing, automatic number plate recognition (ANPR) and so forth. As Germaine Halegoua puts it, "current smart city developments

[185] Vito Albino, Uberto Berardi, and Rosa Maria Delgado, "Smart cities: definitions, dimensions, and performance," *Journal of Urban Technology* 22, no. 1 (2015): 1726, see Table 1 for a summary of existing smart city definitions, http://cl.uw.edu.pl/dok/smart_cities.pdf

[186] Andrew Karvonen, Fredrico Cugurullo, Frederico Caprotti, ed., *Inside Smart Cities: Place, Politics and Urban Innovation* (London: Routledge, 2019), PDF version, 4.

are meant to address problems quickly based on huge amounts of data gathered through sensors and antennae that constantly monitor urban activities and environments."[187]

This thesis will only analyze smart city projects that involve the enhancement of monitoring capabilities across all sectors. **Kuala Lumpur** currently deploys ET City Brain, a fully integrated AI-enabled system operating Chinese Company Alibaba's Apsara[188] – a cloud computing platform – which manages real-time collection of data and integration of emergency and traffic response data from scores of traffic cameras, among other sources.[189] Its aim is to increase traffic flow efficiency and even modulates traffic signal timing to carry emergency vehicle passage.

Rio de Janeiro's local government, with the aim of monitoring the city on a 24/7 basis, opened the Centro de Operações do Rio (Rio Operations Center), known as COR in 2010, a data warehouse that stores data on weather, traffic, security, and energy, focusing on providing information about situations and submitting quick solutions. COR is a physical and technologically connected and interactive space, with the city's video surveillance system serving as one of its primary purposes for the monitorization of weather conditions, situation and risk management, incident management, and planning of big events.[190] To observe urban spaces and promote public safety

[187] Germain Halegoua, "An Introduction to Smart Cities," in *Smart Cities* (Cambridge: The MIT Press, 2020), EPUB version, 23.

[188] Alibaba Cloud, "Apsara Stack," https://www.alibabacloud.com/product/apsarastack

[189] Barbara Szewcow and Jonathan Andrews, "Kuala Lumpur to build 'City Brain' with Alibaba Cloud," *ITU*, February 2018, https://www.itu.int/en/myitu/News/2020/04/07/13/14/Kuala-Lumpur-to-build-City-Brain-with-Alibaba-Cloud

[190] Clara Schreiner, "International Case Studies of Smart Cities – Rio de Janeiro, Brazil," *Inter-American Development Bank*, 2016, 16, https://publications.iadb.org/publications/english/document/International-Case-Studies-of-Smart-Cities-Rio-de-Janeiro-Brazil.pdf

and order, COR utilizes two systems for the operation of cameras: UBICUS and DIGIFORT,[191] which allow real-time images to be displayed in sequential, fixed or programmed forms by presenting them simultaneously in accordance with operational need. It is worth noting that while full access is not granted, both Rio's military police and civilian police can gain access for security and criminal investigations.[192]

In **Phuket**, the city uses mobile services, data analytics, and IoT to inform the local police as well as tourists of the city's happenings to make the city a safer environment for tourists.[193] Operated by public and private agencies, Phuket has over 2,000 surveillance cameras that cover most public areas, including street checkpoints and shorelines.[194] These cameras can automatically tag and identify tourists' facial features, capturing individual's faces and comparing it to a police database. The surveillance network is centralized and integrated with its big data analytics platform so as to enable police reception of timely signals in emergency circumstances.[195] Phuket is also harnessing technologies to create more business opportunities. In providing over 1,000 free Wi-Fi hotspots, the city collects tourists' demographic data. An operations center combines all data gathered by

[191] Ibid., 59.

[192] Rio Prefeitura, "Centro de Controle Operacional (CCO)," https://www.rio.rj.gov.br/web/gmrio/centro-de-controle-operacional

[193] Ernest Ho, "Smart City Phuket: Leveraging the IoT for Tourism," *AIBP*, April 2017 http://iotbusiness-platform.com/blog/smart-city-phuket-leveraging-iot-tourism/

[194] "Phuket governor says island needs 1,500 additional CCTV cameras," *The Phuket News*, June 2017, https://www.thephuketnews.com/phuket-governor-says-island-needs-1-500-additional-cctv-cameras-62769.php

[195] Ibid.

See also Pracha Asawateera, "Phuket Smart City Road Map," https://phuketrealestateassociation.files.wordpress.com/2016/10/pkt-smartcity-ws-update.pdf these hotspots in order to produce useful consumer insights which enable local businesses to come up with more targeted marketing strategies.[196]

Given **Nairobi**'s high crime rate and lack of security,[197] Kenya Safaricom (country's dominant telecommunications firm) and the Kenyan Government signed an agreement in 2014 to construct a surveillance network in their capital. With the aid of Huawei, 116 LTE base stations, 200 traffic surveillance systems, 1,800 cameras, and 2 data centers were installed in Nairobi.[198] What's more, they developed an Emergency Contact Center in Nairobi fostering voice-based first responder dispatching, video surveillance, call center interoperability, as well as face and license plate recognition capacities.[199]

Lisbon's Smart City strategy is conducted by the Centro de Gestão e Inteligência Urbana (Urban Intelligence and Management Centre) of which the main focus is a data-based management culture that hopes to provide more transparent, efficient, and innovative services for the city's residents. The city council involved NEC Corporation in an effort to tackle the challenge of disparate data and information across inflexible, complex, and isolated public and private sources, by building an intelligent management platform along with sensors which allowed the integration, aggregation,

[196] Medha Basu, "Exclusive: Phuket's smart city vision," *GovInsider*, December 2017, https://govinsider.asia/smart-gov/phuket-smart-city-digital-economy-pracha-asawathira/

[197] Samuel L. Aronson, "Crime and Development in Kenya: Emerging Trends and the Transnational Implications of Political, Economic, and Social Instability," *Inquiries Journal/Student Pulse* 2 no. 9 (2010) http://www.inquiriesjournal.com/a?id=278

[198] Huawei, "Video Surveillance as the Foundation of 'Safe City' in Kenya," https://www.huawei.com/en/industry-insights/technology/digital-transformation/video/videosurveillance-as-the-foundation-of-safe-city-in-kenya

[199] Huawei, "Kenyan Safe City Can Now Sleep Better," https://archive.li/pBsxf#selection-4471.1-4471.38

management and display of a variety of pertinent data sources.[200] With this platform, the city is capably monitoring and managing 30 external systems and 10 internal systems that were once separate. Furthermore, the Municipal Service Operation Center is responsible for monitoring waste management systems, transportation and traffic systems, and public safety providers, delivering helpful insights to users.[201]

Cities have been put to the test as a consequence of COVID-19, with services and businesses shut down and medical facilities pushed to their limits. Accordingly, the pandemic has fueled smart city enterprises as evidenced by the amplified reliance on telemedicine, teleworking, online education and commerce, and surveillance systems, and several cities have harnessed smart technologies to stem the Coronavirus's spread.[202]

We find an example of a successful and democratic harnessing of smart city technologies in combating the pandemic in **Seoul**. Rather than enforce total lockdown, which brings inevitable socioeconomic ramifications, Seoul opted for extensive surveillance that rested on an anonymized spatial-temporal mapping, employing mobile phone data, CCTV data, and credit and debit card transaction data, to monitor and track patients' mobility.[203] The outcomes of such mapping were

[200] Lisboa Inteligente, "Plataforma de Gestão Inteligente de Lisboa," https://lisboainteligente.cm-lisboa.pt/lxi-iniciativas/plataforma-de-gestao-inteligente-de-lisboa/

[201] NEC Corporation, "NEC's intelligent management platform makes Lisbon smarter," *Asmag*, October 2019, https://www.asmag.com/showpost/30622.aspx

[202] Klaus R. Kunzmann, "Smart Cities After COVID-19: Ten Narratives," *disP – The Planning Review* 56, no. 2 (2020): 22 https://www.tandfonline.com/doi/full/10.1080/02513625.2020.1794120

[203] Jung Won Sonn and Jae Kwang Lee, "The smart city as time-space cartographer in COVID-19 control: the South Korean strategy and democratic control of surveillance technology," *Eurasian Geography and Economics* 61, no. 4-5 (2020): 1-11, https://www.tandfonline.com/doi/full/10.1080/15387216.2020.1768423

published on mobile apps along with government websites, allowing for information to be anonymously, adequately and transparently communicated to citizens while helping circumvent public panic and the propagation of fake news.

In **New York City**, the smart city programs guided by the OneNYC 2050 strategy were substantially instrumental in aiding the city's response to the COVID-19 crisis. When supplies of Personal Protective Equipment were running short, the city put out a digital request for donations and employed digital technologies to monitor them.[204] Following the disease outbreak, it correspondingly began to monitor anti-Asian sentiment as well as hate crimes.

Singapore, which places first in multiple Smart City index and ranking reports,[205] produced two systems that played noteworthy roles in the digital surveillance prospect during the COVID-19 crisis – TraceTogether and SafeEntry. The former is an app that relies on Bluetooth signals to enable authorities to detect individuals who have been exposed to those who are infected. The app is able to make a record of the time and encounter through the exchange of Bluetooth signals in smartphones when they are within a two-meter range. Subsequently, the information is used to determine close contacts based on the duration and proximity between users. SafeEntry is an automated check-in plus check-out system which logs visitors' and people's entry into shopping malls, schools and universities, offices, among other sites, allowing the documentation of

[204] Eden Strategy Institute, "Top 50 Smart City Governments," 2021, 20, https://www.smartcitygovt.com/202021-publication

[205] Institute for Management and Development and Singapore University for Technology and Design, "2020 Smart City Index," https://www.imd.org/globalassets/wcc/docs/smart_city/smartcityindex_2020.pdf; see also Eden Strategy Institute, "Top 50 Smart City Governments," 2021 https://www.smartcitygovt.com/202021-publicationold

individuals' arrival and departure times at a specific venue through a QR code scan using mobile devices so as to aid data verification and contact tracing and efforts.[206] While the TraceTogether app is a voluntary surveillance scheme, SafeEntry is obligatory.

A report conducted by the ESI ThoughtLab has explored how 167 cities with ranging populations and economies are using smart innovation to drive results in a post-COVID world. According to the report – when asked about the pandemic's lasting impacts – more than two-thirds of cities will rethink urban design and space utilization, while 54% will rethink mobility. What's more, over half of top city officials consider that the crisis will change how people work, live, travel, and interact in cities for the rest of their lives.[207]

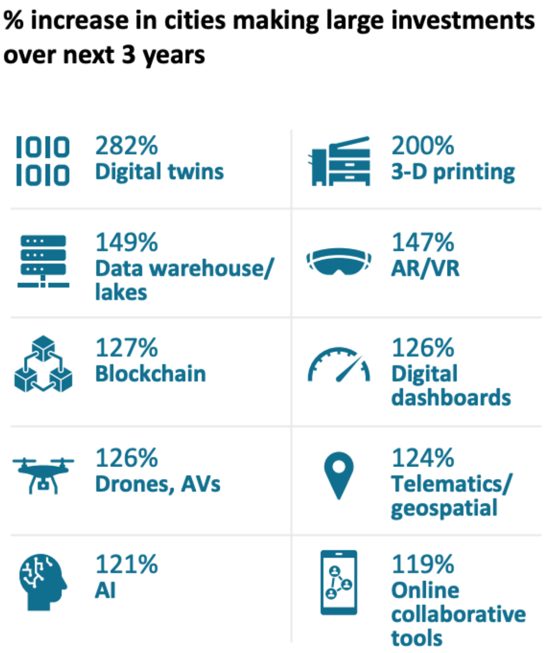
The major lesson during the pandemic, for 65% of cities, according to ESI ThoughtLab, was just how essential smart city projects are for their future. For 68% of cities in Europe and 80% in the Middle East it was a particularly critical admission. In addition, about 43% acknowledged the value of operational agility and continuity, and a similar number grasped the value of timely data and analytics. COVID-19 likewise persuaded cities on the importance of investing more on improving core infrastructure (37%) as well as in inexpensive and reliable connectivity (25%).[208]

[206] GOVTECH Singapore, "Responding to COVID-19 With Tech," https://www.tech.gov.sg/products-and-services/responding-to-covid-19-with-tech/; see also Smart Nation Singapore, "Singapore's Technology Driven Response To The Pandemic," https://www.smartnation.gov.sg/whats-new/combating-covid-19-with-technology#suite3

[207] ESI ThoughtLab, "Smart City Solutions for a Riskier World," 19. https://econsultsolutions.com/wp-content/uploads/2021/03/ESITL-Smart-City-Solutions-eBook-Final.pdf

[208] ESI ThoughtLab, "Smart City Solutions for a Riskier World," 21.

In the illustrations of the aforementioned Smart City projects, cities are already adopting a broad assortment of smart technologies, particularly AI, biometrics, cloud and mobile. As real-time and predictive information become ever more decisive to effective urban service delivery in the time of COVID-19, *Smart City Solutions for a Riskier World* has found that in the coming years, cities plan to significantly increase investments in these technologies, with investment in cloud platforms being highlighted by 88% of city leaders as the most urgent necessity for the fruitful delivery of citizen services.[209] The figure below reveals the percentage increase in cities making hefty investments over the next three years.



% increase in cities making large investments over next 3 years

282% Digital twins	200% 3-D printing
149% Data warehouse/ lakes	147% AR/VR
127% Blockchain	126% Digital dashboards
126% Drones, AVs	124% Telematics/ geospatial
121% AI	119% Online collaborative tools

[209] ESI ThoughtLab, "Smart City Solutions for a Riskier World,", 29.

Accordingly, it is imperative that Policymakers address widespread fears regarding public surveillance as data collection processes continue to grow. A smart city's cameras, sensors, and audio solutions collect huge amounts of information, but just a small extent can be revealing and misused by governments. Therefore, smart cities require robust security policies, not just to protect against function creep but also against cyber criminals and terrorists that could capitalize on the IoT backbone that underpins smart cities. Data management is thus critical to successful urban service delivery. However, according to *Smart City Solutions for a Riskier World*, just 35% of surveyed cities (167) have "a written policy that ensures the responsible management of data" and only 39% "ensure there is an appropriate budget for data management."[210]

It is worth mentioning Hungarian-Canadian sociologist Frank Furedi's theory on the "culture of fear". Furedi has written broadly about the emergence and consolidation of a precaution-oriented, fearful culture. The sociologist uses important examples such as terrorism, child abuse, and crime to demonstrate that Western populations are residing in a decidedly risk-averse and anxious era wherein public fears exist out of proportion to the magnitude of harm. The language surrounding "risk", according to Furedi, has become culturally ubiquitous, with the pervasive reinforcement of a variety of security risks being symptomatic of an inclination to focus on everyday life's negative aspects. As a result, he contends that modern Western citizens are affected and moved by a "culture

[210] ESI ThoughtLab, "Smart City Solutions for a Riskier World," 33.

of fear" that is vigorously promoted by state institutions as well as those working with security industries and media.[211]

What this makes clear is that technology companies and analysts – like ESI ThoughtLab – are encouraging cities to focus on risk, or risk-prevention, rather than other important public goods such as free-will, privacy, and self-government. If tech companies can convince cities to focus mainly on risk, they can sell more of these costly systems. Taking the COVID-19 crisis into account, it may be argued that it has also amplified the importance given to risk-prevention by technological and political elites, making it the most critical public good.

In what regards **workplace surveillance**, employee monitoring is not new. In fact, it may be argued that workplace surveillance has always existed under capitalism:

> The fact that human labor power is traded as a commodity that employers purchase and then seek to maximize surplus out of, requires some form of monitoring and evaluation, which necessarily involves a certain degree of interference with workers' privacy.[212]

Prior to the rise of electronic surveillance, advancements in workplace surveillance largely occurred within the Taylorist model.[213] Taylor's central contribution was a strong case in favor of a well-educated managerial class to supervise organizations' low-level workers. In the following

[211] Frank Furedi, *Culture of Fear: Risk-Taking and the Morality of Low Expectation* (London: Bloomsbury Continuum, 2018), EPUB version.
[212] Ivan Manokha, "New Means of Workplace Surveillance," *Monthly Review*, February 2019, https://monthlyreview.org/2019/02/01/new-means-of-workplace-surveillance/
[213] Ibid.; See also Chapter 1, section 1.3 of this thesis.

periods, management became grasped as a basic organizational component, associated with employee monitoring.[214] Moreover, given the growth of complex corporations with enhanced levels of geographic dispersion and task differentiation, conviction in managerial oversight has been intensified. Taylorism thus entailed, as has been generally noted, the development of progressively more sophisticated worker monitoring systems.[215] Nevertheless, this form of surveillance was based solely on abstract time and visual observation – commonly referred to as "traditional" monitoring procedures.

More recently, as work transitioned from the industrial to the digital age, employee tracking techniques evolved with new technologies. Now, managerial oversight has become noticeably easier given that new technologies have facilitated more diversified, ubiquitous, and extensive surveillance practices. Furthermore, the lines between what constitutes a workplace are increasingly being blurred as technologies and digital devices mediate work productivity and communications, both on-site and remotely. According to a 2019 study[216] assessing 239 big corporations, it was revealed that 50% were employing "nontraditional" surveillance methods, incorporating analyzing and logging phone calls, tracking meeting attendance, and scrutinizing social media posts and emails, representing a 20% increase since 2015 and estimating such practices to reach 80% in 2020.

[214] Monahan and Wood, ed., *Surveillance Studies: A Reader*, 261.

[215] Martha Crowley et al., "Neo-Taylorism at Work: Occupational Change in the Post-Fordist Era," *Social Problems* 57, no. 3 (2010): 421-47. https://swab.zlibcdn.com/dtoken/9bfec8f5254eabe869aac01c9f58b061

[216] Rick Wartzman, "Workplace tracking is growing fast: most worker don't seem very concerned," *Fast Company*, March 2019, https://www.fastcompany.com/90318167/workplace-tracking-is-growing-fast-most-workers-dont-seem-very-concerned

With recent advancements and several discoveries in AI, the area now provides significant benefits and potential for businesses, ranging from increased productivity gains through automation to data analysis at scale, and more. In the *Atlas of AI*, Kate Crawford argues that today, surveillance technologies have largely taken over the duty of oversight in the workplace. The managerial class uses a variety of technologies to monitor employees, such as tracking their movements with apps, comparing patterns of responding to emails and scheduling meetings, investigating their social media feeds, and nudging them with suggestions to help them work faster and more efficiently. Employee data is used to anticipate who is most likely to succeed – based on a set of narrow, quantitative criteria – who may be deviating from business goals, and who may be organizing other employees. Some involve machine learning approaches, while others are more straightforward algorithmic systems. As AI becomes more widely used in the workplace, some of the more basic monitoring and tracking technologies are being enhanced with additional predictive capabilities to become more intrusive tools for asset control, value extraction, and worker management.[217]

With the COVID-19 pandemic, workplace surveillance trends have expanded, reflected in the increased sales of monitoring tools[218] during the transition to remote work. Albeit not a new concept, the pandemic has, for many employers, rendered teleworking, or working from home, the "new normal." As many people are relocated to work from home, and those that keep commuting

[217] Kate Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence* (New Haven: Yale University Press, 2021), PDF version, 62-63.
[218] Polly Mosendz and Anders Melin, "Bosses Panic-Buy Spy Software to Keep Tabs on Remote Workers," *Bloomberg*, March 2020, https://www.bloomberg.com/news/features/2020-03-27/bosses-panic-buy-spy-software-to-keep-tabs-on-remote-workers

require workplace safeguards against contracting the virus, new surveillance tools have been developed for supervision of remote workers and collection of worker health and safety data. Pointed out in a Washington Post article, many employee-monitoring and time-tracking companies, comprising Hubstaff, Teramind, ActivTrak, and Time Doctor, saw their revenue and customer base escalate since the COVID-19 outbreak.[219] To be sure, two software companies witnessed their surveillance programs spike 500% and 600% in the spring of 2020.[220]

Hubstaff snaps screenshots of browsed websites, documents being written and social media sites being visited, every few minutes. It is essentially an activity monitor that totals the percentage of time a worker has spent moving the computer mouse or typing, which then acts as a productivity score.[221] Time Doctor takes regular screenshots of employee's screens, tracks their breaks, and sends nudges when they stray or move to non-work linked sites. Supervisors are then provided with dashboards that disclose an employee's work output.[222] Teramind's remote employee monitoring tracks the entirety of user activity, scrutinizing online activity and enforcing admin rules and policies even when an employee is offline. Teramind utilizes 20 tools[223] for employee

[219] Drew Harwell, "Managers turn to surveillance software, always-on webcams to ensure employees are (really) working from home," *Washington Post*, April 2020, https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance/

[220] Adam Isaak, "Employee tracking is increasingly widespread, and it could be doing more harm than good," *CNBC*, June 2020, https://www.cnbc.com/2020/06/17/employee-surveillance-software-is-seeing-a-spike-as-workers-stay-home.html;

[221] Adam Satariano, "How My Boss Monitors Me While I Work From Home," *The New York Times*, May 2020, https://www.nytimes.com/2020/05/06/technology/employee-monitoring-work-from-home-virus.html; for an in-depth description of Hubstaff features, see https://hubstaff.com/features/employee_monitoring

[222] Sarah O'Connor, "Workplace surveillance may hurt us more than it helps," *Financial Times*, January 2021, https://www.ft.com/content/27faa953-1723-4597-a5a0-2ff9e617feab

[223] Teramind, "Remote Employee Monitoring," https://www.teramind.co/solutions/remote-employee-monitoring

surveillance, including Live View and History Playback; User Behavior Analytics; Remote Desktop Control; Website, Email, Social Media and Keyboard monitoring, to name a few. ActivTrak focuses on team and individual workforce analytics, featuring granular data reporting, and detection of mouse and keyboard movements.[224] Notably, ActivTrak forgoes more intrusive capabilities like live video recording.

Recently, Amazon capitalized on the COVID-19 crisis and rolled out a new workplace monitoring tool[225] – AWS Panorama – which analyzes security camera footage in workplaces through computer vision technology, allowing the detection of compliance or lack thereof with social distancing rules. What's more, Amazon says the tool can also monitor employees to evaluate whether people are where they shouldn't be, or if there's an oil spill, among other things that point to decreased productivity. Walmart had a patent filed for a sound sensors system placed near cashiers that could, based on audio data, determine an employee's performance metric.[226] The US retailer has also purchased facial recognition technology to identify both customers and workers in its stores and surveil their productivity, purchases, and location.[227]

IBV's "Digital acceleration" report demonstrates a correlation between digital maturity and financial performance. The research discovered that during COVID-19, across 12 industries and by an average of 6%, tech-savvy corporations outperformed the lesser tech-savvy ones on revenue

[224] ActivTrak, "How ActivTrak Works," https://www.activtrak.com/how-it-works/
[225] Dave Lee, "Amazon to roll out tools to monitor factory workers and machines," *Financial Times*, December 2020, https://www.ft.com/content/58bdc9cd-18cc-44f6-bc9b-8ca4ac598fc8
[226] O'Connor, "Workplace surveillance may hurt us more than it helps," *Financial Times*.
[227] Esperanza Fonseca, "Worker Surveillance Is on the Rise, and Has Its Roots in Centuries of Racism," *Truthout*, June 2020, https://truthout.org/articles/worker-surveillance-is-on-the-rise-and-has-its-roots-in-centuries-of-racism/

growth.[228] What's more, 60% of executives expressed the acceleration of their businesses' digital transformations during the COVID-19 pandemic, and 64% conceded a move to more cloud-based firm activities.[229] Accordingly, these findings make clear that, in the course of COVID-19, digital technologies have become a significant source of competitive advantage, therefore expediting the procurement of such tools, thus increasing the potential for their misuse as regulations have not caught up to these fast-tracked developments in times of emergency.

COVID-19 upended work in several ways and pressed companies and employers to reconsider best methods for getting work done, of which the consequent blurring of the private and public spheres through heightened surveillance is alarming, as is the prospective for such surveillance operations to continue post-COVID-19.

2.3. Surveillance: Personal Level (Social Media and Smart home technology)

This subsection traces surveillance operations in settings where some monitoring practices are visible, meaning that some kinds of data capture are manifest. In this sense, individuals who partake in the use of the social platforms and technologies examined here are cast as voluntary subjects of surveillance. Additionally, the surveillance systems analyzed here concern the capture of personal information.

[228] IBM Institute for Business Value, "Digital Acceleration," 2, https://www.ibm.com/downloads/cas/MBV83XAY

[229] IBM Institute for Business Value, "COVID-19 and the Future of Business," 3, https://www.ibm.com/downloads/cas/1APBEJWB

After 1945, the rise of Fordist mass production and consumption intensified corporate interest in gathering information on people's consumption patterns. This, as Fuchs et al. argue,[230] not only engendered the growth of the advertising sector, but the increase in consumer research and monitoring as well. With the convergence of telecommunications and information technology, distributed communications networks like the internet have extended significantly the opportunities for collecting, monitoring, and classifying personal data. Indeed, the rise of the Internet has enabled a globally networked arrangement of surveillance, as the former adds two dimensions to the latter: global networking and interaction.[231]

However, what propelled the appeal for information extraction through online surveillance practices was not the internet in itself, but the consolidation of what is known as "Web 2.0."[232] Evolving from Web 1.0, instead of web content being mostly provided by web designers and specialists, Web 2.0 allows anyone to create content which can be dynamically updated. Furthermore, such content can be accessed and engaged with on a range of platforms like tablets and smartphones. Rather than merely browsing information or being limited to somewhat narrow discussions, internet users can now actively and easily participate in the construction of the online world. This represents the emergence of social media and networking.

[230] Christian Fuchs, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval, eds., *Internet Surveillance: The Challenges of Web 2.0 and Social Media* (New York: Routledge, 2012), PDF version, 8.

[231] Ibid., 3.

[232] Web 2.0 is highlighted here as it represents the internet platforms and services whose content is generated or made available owing to user participation, meaning social networks and blogs like Twitter and Facebook, sharing platforms such as YouTube, etc.

Web 2.0. sites and services all rely on the active participation of persons willing to share information relating to their lives and take up work such as posting, writing, sharing, tagging, communication, among others.[233] In this manner, they not only volunteer labor, but also a wealth of data, comprising user profiles, locations, photos, opinions, tastes and beliefs, as well as their social network. As such, the introduction of Web 2.0 and thusly social media has allowed corporations to capitalize on time spent engaging in information exchange and communicative activity. Given the expansion in information production, and in consumption thereof, "every content-creating platform is also potentially a content-capturing platform."[234] In sum, user-generated content and behavior is also surveilled and collected at mass scale.

In Web 2.0 participatory platforms, many scholars classify users as *prosumers*[235] given that they generate valuable data and content as both producers and consumers, signifying a partial collapse onto one another of the modes of consumption and production. Through collective efforts, prosumers generate, extract value from, and add value to the services or products they engage with, regardless of whether users are aware of this or not. As prosumers, users become "productive laborers who produce surplus value and are exploited by capital."[236] Therefore, the capitalist production's emergent property of surplus value generating labor means that accumulation and production break down should such labor be withdrawn. To corroborate this, Fuchs sets up a

[233] Rob Kitchin, *The Data Revolution*, 130.
[234] *Routledge Handbook of Surveillance Studies*, 348.
[235]*Surveillance Studies: A Reader*, 277, 298. *Routledge Handbook of Surveillance Studies*, 323; *Internet Surveillance: The Challenges of Web 2.0 and Social Media*, 74, 150; *The Data Revolution*, 129.
[236] *Surveillance Studies: A Reader*, 277.

thought experiment wherein users would cease their use of social media platforms. The results would be a drop in the number of users, halting investments by advertisers seeing that no prospective customers for their products might be found, dropping profits for new media corporations, and their eventual bankruptcy. Therefore, users are fundamental to creating profit in the media economy,[237] empowering digital platforms to act as means of production, of which surveillance is an intrinsic operation as it supports data collection and hence value extraction.

More than ever before, information is being privatized as it is collected and aggregated for resale as a commodity or integrated into the production of customized commodities. Corporations are becoming increasingly reliant on data collection and analysis of consumer wants, requirements, and desires. This has evolved into a critical resource whereupon marketing and business decisions are predicated[238], covering the services companies choose to offer, the locations wherein they operate, the "investments" made in certain "relationships" with consumers and so on. Although the gathering and handling of consumer data is enclosed by data protection laws as well as privacy regulations, it's already been established in previous sections that the means for enacting surveillance are progressively innovative and enticing:

> Corporations are able to use the tools, processes and possibilities of new information and communication technologies, and employ rewards, discounts, entertainment, collaboration, special access, networking, recognition, better

[237] Ibid., 278.

[238] *Routledge Handbook of Surveillance Studies*, 321.

> service and products, and coercion (...) to produce detailed consumer-specific data. In addition, algorithmic processes can be used to extensively analyze this information, revealing associations and propensities between various sets of consumers that may be obvious or ‘non-obvious’.[239]

Additionally, corporations utilize social media to recruit or find out about employees. A number of sites, such as Abika,[240] fyiscreening,[241] and Sterling Backcheck,[242] offer tracking services of personal data on social and other comparable networks, as well as extensive reports on a person’s web trail. Indeed, the practice has become so widespread that, in Germany, legal action has already been taken[243] to check the use of social media-derived personal information as a recruiting factor.

Consumer surveillance is not as opaque as other surveillance operations. Most website policies and privacy settings do summarize the extent to which user information is gathered and shared. Facebook’s terms of service, for example, detail the kind of information that is collected, ranging from “things that you and other do and provide,” “device information,” “information from partners,” which are used to “provide, personalize and improve [its] Products,” for “providing measurement, analytics and other business services,” “promoting safety, integrity and security,” and “researching and innovating for social good,” which they identify as “topics of general social welfare, technological advancement, public interest, health and well-being.” Additionally, besides

[239] Ibid.
[240] Abika, “Abika Consulting,” https://www.abikaconsulting.com/
[241] Fyiscreening, “Employment Screening and Background Checks,” https://fyiscreening.com/
[242] SterlingBackcheck, https://www.sterlingbackcheck.ca/
[243] David Jolly, “Germany Plans Limits on Facebook Use in Hiring,” *New York Times*, August 2010, https://www.nytimes.com/2010/08/26/business/global/26fbook.html

sharing this information on Facebook Products, it is also shared with third-party partners, including "partners who use [its] analytics services," "advertisers," "measurement partners," "partners offering goods and services in [its] Products," "vendors and service providers," "researchers and academics," and "lar enforcement or legal requests."[244] Notably, Facebook does allow its users to adjust their privacy settings to limit who views their content, but this approach, as Nicole S. Cohen points out, "places the onus on individuals to seek out and activate their privacy settings, which does not address larger issues of privacy and surveillance, nor does it acknowledge the fact that most people are unaware of website privacy settings and policies in the first place."[245]

Beyond corporate surveillance of consumer-generated traffic, which is publicly disclosed, Daniel Trottier argues that social media enables formerly discrete surveillance operations to feed off one another, comprising four types of surveillance:

> Individuals watching over one another, institutions watching over a key population, businesses watching over their market and investigators watching over populations (...) Individual, institutional, market and investigative scrutiny all rely on the same interface. Thus, familiarity with the site as an interpersonal user facilitates other uses. In addition to relying on the same interface, these practices also rely on the same body of information. This means that personal

[244] Facebook, "Data Policy," https://www.facebook.com/about/privacy/update
[245] *Surveillance Studies: A Reader*, 301.

> information that has been uploaded for any particular purpose will potentially be used for several kinds of surveillance.[246]

According to records acquired by the Electronic Frontier Foundations from the Freedom of Information Act, the CIA and the FBI are progressively scanning social networking sites, Web forums, chat rooms, and blogs to aid security investigations and law enforcement.[247] There are also websites that promote peer-to-peer monitoring. PeoplePublicRecords[248] and Abika, for instance, provide checks on a person's background. Spokeo[249] is a search engine that specializes in assembling personal information on the web. Moreover, Sentry Parental Controls[250] and Catchacheat[251] offer monitoring services of children and partners' activities.

In a research conducted by AT&T Labs and the Worcester Polytechnic Institute reports that in 2009, user-monitoring technologies were detected in 80% of 1,000 investigated popular websites, a significant escalation from 40% in 2005.[252] On another note, Freedom House's 2019 *Freedom on The Net* report has identified 40 countries that have introduced social media surveillance programs, inferring that 89% of internet users are being monitored,[253] accounting for roughly 38%

[246] Daniel Trottier, *Social Media as Surveillance: Rethinking Visibility in a Converging World* (Farnham: Ashgate, 2012), EPUB version, 193 out of 287.
[247] Jennifer Lynch, "Government Uses Social Networking Sites for More than Investigations," *Electronic Frontier Foundation*, August 2010, https://www.eff.org/deeplinks/2010/08/government-monitors-much-more-social-networks
[248] PeoplePublicRecords, http://www.peoplepublicrecords.org/
[249] Spokeo, "Know More," https://www.spokeo.com/
[250] Sentry, "More than parental control," https://sntry.io/
[251] Catchacheat, "How to Catch Your Cheating Lover," https://www.catchacheat.com/
[252] Julia Angwin, "The Web's New Gold Mine: Your Secrets," *The Wall Street Journal*, July 2010, https://www.wsj.com/articles/SB10001424052748703940904575395073512989404
[253] Adrian Shahbaz and Allie Funk, "Freedom on the Net 2019 Key Finding: Governments harness big data for social media surveillance," *Freedom House*, 2019, https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance

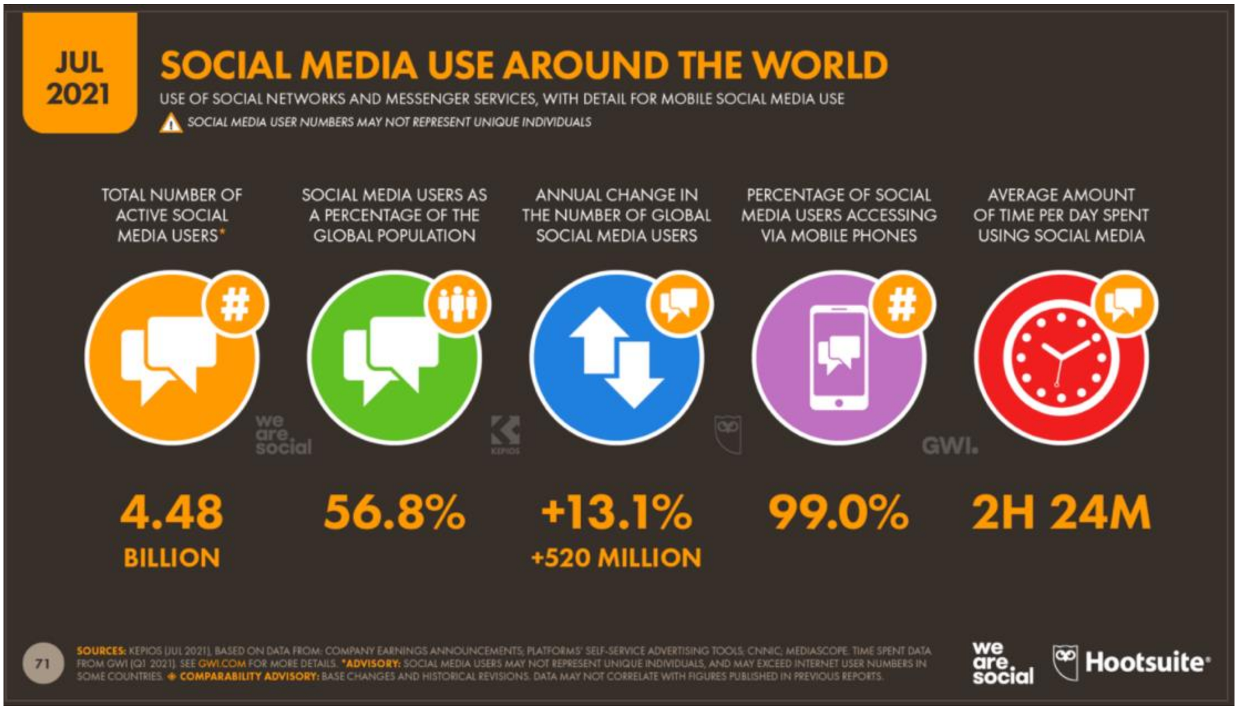
of the world population. Extreme examples can be found in Russia, Turkey, the United Arab Emirates, and Iran, among others, as autocratic governments are taking advantage of digital tools to quash freedom of expression online. These tactics include Iran's attempt at creating an alternative Internet; Russia's "internet sovereignty" law dictating that service providers must implement technology that lets the Kremlin monitor, filter and reroute online traffic; and Turkey and the United Arab Emirates' steering of citizens' use of foreign sites to messaging apps of national origin.[254]

The COVID-19 crisis and consequent lockdowns and restrictions have had a significant impact on social media participation. Because of the uncertainty initial lockdowns brought to businesses and people everywhere, social media became the go-to source for entertainment, news, human interaction, and information. As many places for social activities closed, either temporarily or permanently, due to COVID-19, the turn to social media to compensate for the lack of personal interaction is not unexpected. eMarketer, prior to the COVID-19 outbreak, had projected that social media usage would rise by only 6 seconds in 2020. That wasn't the case, however, as they updated that figure up to 7 minutes in May 2020.[255]

[254] Peter Reynolds, "Governments are finding new ways to quash freedom of expression online," *The Economist*, October 2021, https://www.economist.com/international/2021/10/16/governments-are-finding-new-ways-to-squash-free-expression-online

[255] David Cohen, "eMarketer Ups 2020 Projections for Time Spent on Social Networks Due to Covid-19," *Adweek*, May 2020, https://www.adweek.com/performance-marketing/emarketer-ups-2020-projections-for-time-spent-on-social-networks-due-to-covid-19/

The *Digital 2021 July Global Statshot Report* by DataReportal notes that more than 1 in 9 of present-day's social media users only began using social platforms 12 months prior to aforementioned publication. What's more, from April to July the social media's user total increased by 147 million.[256] The next figure shows DataReportal's key findings on social media use around the world:



JUL 2021

SOCIAL MEDIA USE AROUND THE WORLD

USE OF SOCIAL NETWORKS AND MESSENGER SERVICES, WITH DETAIL FOR MOBILE SOCIAL MEDIA USE

⚠ SOCIAL MEDIA USER NUMBERS MAY NOT REPRESENT UNIQUE INDIVIDUALS

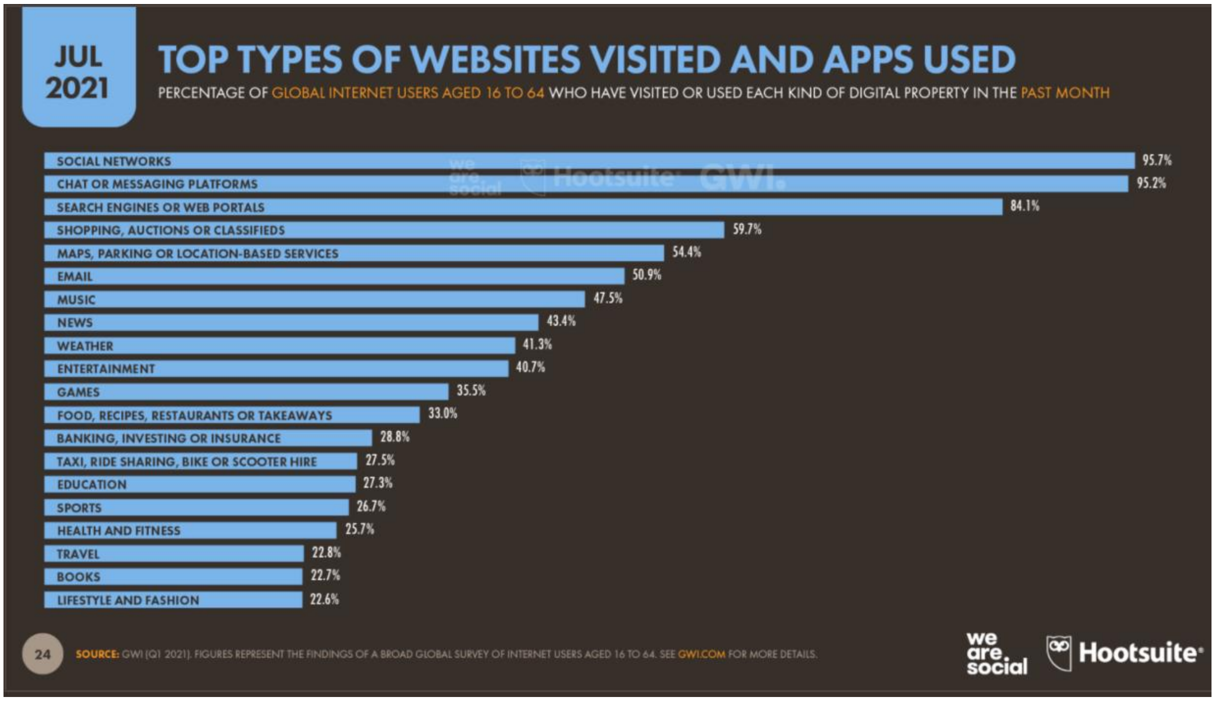
TOTAL NUMBER OF ACTIVE SOCIAL MEDIA USERS*	SOCIAL MEDIA USERS AS A PERCENTAGE OF THE GLOBAL POPULATION	ANNUAL CHANGE IN THE NUMBER OF GLOBAL SOCIAL MEDIA USERS	PERCENTAGE OF SOCIAL MEDIA USERS ACCESSING VIA MOBILE PHONES	AVERAGE AMOUNT OF TIME PER DAY SPENT USING SOCIAL MEDIA
4.48 BILLION	56.8%	+13.1% +520 MILLION	99.0%	2H 24M

71

SOURCES: KEPIOS (JUL 2021), BASED ON DATA FROM: COMPANY EARNINGS ANNOUNCEMENTS; PLATFORMS' SELF-SERVICE ADVERTISING TOOLS; CNNIC; MEDIASCOPE. TIME SPENT DATA FROM GWI (Q1 2021). SEE GWI.COM FOR MORE DETAILS. *ADVISORY: SOCIAL MEDIA USERS MAY NOT REPRESENT UNIQUE INDIVIDUALS, AND MAY EXCEED INTERNET USER NUMBERS IN SOME COUNTRIES. ◈ COMPARABILITY ADVISORY: BASE CHANGES AND HISTORICAL REVISIONS. DATA MAY NOT CORRELATE WITH FIGURES PUBLISHED IN PREVIOUS REPORTS.

[256] DataReportal, "Digital 2021 July Global Statshot Report," July 2021, https://datareportal.com/reports/digital-2021-july-global-statshot

Moreover, social media use is also the most prevalent of web activities individuals engage in:[257]



JUL 2021

TOP TYPES OF WEBSITES VISITED AND APPS USED

PERCENTAGE OF GLOBAL INTERNET USERS AGED 16 TO 64 WHO HAVE VISITED OR USED EACH KIND OF DIGITAL PROPERTY IN THE PAST MONTH

SOURCE: GWI (Q1 2021). FIGURES REPRESENT THE FINDINGS OF A BROAD GLOBAL SURVEY OF INTERNET USERS AGED 16 TO 64. SEE GWI.COM FOR MORE DETAILS.

Given that the number of social media users now encompasses more than half of the world population, social platforms are the most visited sites/apps, and the average amount of time spent on social media has increased, one can contend that the resultant scope of personal data on an individual has become more considerable than ever before, invigorating surveillance practices in such networks and contributing to their allure and ubiquity. On another note, this research has already established that the aims of social media monitoring vary as they intersect with different strategies for different sectors, and it may be argued that the COVID-19 crisis adds another

[257] DataReportal, "Digital 2021 July Global Statshot Report," July 2021, https://datareportal.com/reports/digital-2021-july-global-statshot

justification for social media surveillance, in this case on the premise of tracking and analyzing pandemic-provoked sentiment and trends. The Center for Disease Control's (CDC) "strategy to reinforce confidence in COVID-19 vaccines," for example, endorses social media monitoring tools "to help organizations in conducting social listening."[258]

Another area where smart technologies and their concomitant monitoring capacities are being deployed is the home, making up the so-called "smart home". A consensus definition of smart home does not exist, but it is commonly understood today as a "residence equipped with high-tech network, linking sensors and domestic devices, appliances, and features that can be remotely monitored, accessed or controlled, and provide services that respond to the needs of its inhabitants."[259]

The smart home has two main functions. First, to regulate and adapt the household to optimize the safety and comfort of its residents by, for example, locking doors when children are home alone, playing television or music upon request, or moderating temperatures.[260] Environmental regulations can be set up by residents. Apple's HomeKit lets inhabitants program "scenes" which make certain devices adjust or activate at a given time or in response to certain events like the homeowner exiting the home.[261] In another fashion, environmental adjustments can be tailored to

[258] US Department of Health and Human Services, "Social Listening and Monitoring Tools," *Centers for Disease Control and Prevention*, 2021, https://www.cdc.gov/vaccines/covid-19/vaccinate-with-confidence/rca-guide/downloads/CDC_RCA_Guide_2021_Tools_AppendixE_SocialListening-Monitoring-Tools-508.pdf

[259] Nazmiye Balta-Ozkan et al., "Social barriers to the adoption of smart homes," *Energy Policy* 63 (2013): 364, https://www.sciencedirect.com/science/article/abs/pii/S0301421513008471

[260] Richard Harper, ed., *Inside the Smart Home* (London: Springer, 2003), PDF version, 17-18.

[261] Apple, "Create Scenes and Home automations with the Home app," https://support.apple.com/en-us/HT208940

residents on the basis of behavioral patterns and patterns informed by sensor data. Amazon's Alexa, for instance, meets a vague music request by selecting and playing a song or genre that the resident is likely to appreciate.[262] Second, the goal of deploying sensors and sensor data is to adjust inhabitants' behavior.[263] Such adjustments can take various forms. A Google patent filed in 2020 describes a smart home automation system that might seek to deter "undesirable actions." In this system, undesirable behavior by inhabitants is recorded and reported, noting the use of foul language, "mischief" between children, and non-finalization of household work.[264]

Although recent improvements and uptake of smart home appliances have been pushed by policy objectives that encourage or mandate energy efficiency, climate change targets at national and EU levels, as well as advancements in ICTs like wireless devices and high-speed internet – lending impressive traction to the smart home[265] –, the emergence of the smart home is not recent. Rather, it is "the latest iteration of a long-held vision of a mechanized, automated home."[266] For Maalsen and Sadowski, the smart home is the latest instance of a few "utopian domestic futures" familiar in 20th century U.S, which covers the "space age hypermodern home of the 1950s, to the home-as-

[262] Bo Xiao, "How Alexa Can Use Song-Playback Duration to Learn Customers' Preferences," *Amazon Science* (blog), July 16, 2018, https://www.amazon.science/blog/how-alexa-can-use-song-playback-duration-to-learn-customers-preferences

[263] Sophia Maalsen and Jathan Sadowski, "The Smart Home on FIRE: Amplifying and Accelerating Domestic Surveillance," *Surveillance & Society* 17, no. 1/2 (2019): 119, https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/12925/8484

[264] Anthony M. Fadell et al., Smart-Home Automation System That Suggests or Automatically Implements Selected Household Policies Based on Sensed Observations, US Patent No. US 20200012242 A1, pub. January 9, 2020, 16-17, https://patentimages.storage.googleapis.com/86/c5/e3/d9b9efe49d003c/US20200012242A1.pdf

[265] In 2016, the global smart home market was already valued at 24.1 billion US dollars. Statista, "Smart home market size," https://www.statista.com/statistics/682204/global-smart-home-market-size/

[266] Philip Doty, "Oxymorons of privacy and surveillance in "smart homes"," *Journal of the Association for Information Science and Technology* 57, no. 1 (2020): 2, https://asistdl.onlinelibrary.wiley.com/doi/abs/10.1002/pra2.222?af=R

computer of the 1980s and 90s."[267] All of those visions claimed that the accompanying devices would diminish housework while enhancing leisure, home security, and household efficiency in previously unimaginable ways. However, the mechanical devices of 20th century homes – dish washers, automatic garage door openers, humidifiers, coffee makers, among others – were inherently different from the devices that power contemporary smart homes. This is so because firstly, mechanical devices stand apart from other devices as they aren't connected to the internet. Secondly, they are unintelligent in the sense that they make no assertions of purported machine learning and automated improvements. Thirdly, mechanical devices can only start and stop through direct human intervention. Lastly, such devices are intentionally controlled to be either on or off.

Today's smart homes are powered by smart technologies. The Internet of Things (IoT), for instance, which enables connected devices to amass data on household practices, correspond with cloud platforms, harmonize with other appliances, control components of the home, and equip manufacturers, users, and third parties with real-time feedback, has augmented recent embodiments of the smart home.[268] To start or stop they usually rely on passive detection of individuals' behavior and their use of devices and the internet to start, stop or continue operation

[267] Sophia Maalsen and Jathan Sadowski, "The Smart Home on FIRE: Amplifying and Accelerating Domestic Surveillance," 118.

[268] Mark Burdon, *Digital Data Collection and Information Privacy Law* (Cambridge: Cambridge University Press, 2020), PDF version, 37, 38; Kirsten Gram-Hanssen and Sarah J. Darby, ""Home is where the smart is"? Evaluating smart home research and approaches against the concept of home," *Energy Research & Social Science* 37 (2018), https://ora.ox.ac.uk/objects/uuid:3d5ca446-c101-42de-b965-b244afcf415c/download_file?file_format=pdf&safe_filename=Home%2Bis%2Bwhere%2Bthe%2Bsmart%2Bis.%2Bsubmitted_150917.pdf&type_of_work=Journal+article

(e.g., voice-activated assistants like Amazon's Alexa); and/or machine-controlled learning (e.g. a thermostat such as Nest Learning Thermostat that learns a person's heating and cooling preferences and then automatically arranges a personalized schedule). Furthermore, smart home technologies are designed to always be on – once powered by and connected to the IoT, they ceaselessly collect, analyze, and share data concerning themselves and interconnected technologies. The smart home is no longer solely a site for resource flows (gas, water, electricity, information), but also one with the prospective for external control of said flows. These variations in the configuration of home devices of the 20th century to 21st century smart home technologies are what make smart homes a considerable sector of surveillance of modern society.

The surveillance ties are strengthened and multiplied by smart homes, assimilating the household into the larger surveillance infrastructure. The above-mentioned Google patent, for instance, includes a smart home system that can collect and integrate an enormous amount of data concerning ostensibly innocuous home activities that were previously outside surveillance technology's bounds, such as audio signals to detect movements of utensils that imply dinner is being consumed and vapor detection to verify the presence of food.[269] As a result, the smart home has the ability to become a key node in the larger surveillance network.[270]

An example of a smart home technology that appears to directly incorporate the home into a space of surveillance is Amazon's Astro, a household robot specifically designed for "home

[269] Anthony M. Fadell et al., Smart-Home Automation System That Suggests or Automatically Implements Selected Household Policies Based on Sensed Observations, 14.

[270] Sophia Maalsen and Jathan Sadowski, "The Smart Home on FIRE: Amplifying and Accelerating Domestic Surveillance," 120.

monitoring."[271] Astro is a surveillance-focused robot capable of identifying up to ten family members, following them around and playing videos and music, and moving small items. Its most principal feature – monitoring – is what makes Astro a "watchdog on wheels"[272] as its sensitive sensors and advanced learning algorithms allow it to autonomously move around the home and monitor unusual activity.

As observed in previously described surveillance apparatuses, it is not only monitoring-service-providers that enact surveillance of their targeted sector, but also third parties with a vested interest in collecting data, underwriting the wider political economy of datafication. Maalsen and Sadowski contend that the smart home is no different seeing that the power of the smart home to monitor dwellings has also enticed companies from the finance, real estate, and insurance (FIRE) sectors that obtain substantial value extraction in maintaining assets, managing risk, and monetizing information through data collection and analysis vis-à-vis individuals' domestic habits, actions, and environments,[273] which has potentially unfavorable implications for the above-described second function of the smart home:

> Every minute you go without replacing the batteries in that chirping Nest Protect can mean added points to your risk score and adjusted premiums. Rental payment platforms may either reward or penalize you, depending on whether you are a 'responsible' tenant, regardless of broader contexts and circumstances. The smart

[271] Amazon, "Introducing Amazon Astro," https://www.amazon.com/Introducing-Amazon-Astro/dp/B078NSDFSB
[272] John Gapper, "Amazon's Astro robot is a symbol of the surveillance age," *Financial Times*, October 2021, https://www.ft.com/content/c2cf67d6-a143-4aff-9eb1-b7a4e93c3c73
[273] Ibid.

> home purports to offer a model of efficient living, but if FIRE has its way the 'data factory' we live inside will also be used to produce people who conform to its interests.[274]

Another form of surveillance that is present in the smart home is sousveillance, which focuses on boosting people's ability to access and collect information about their surveillance. Smart home technologies, through surveillance and data processing, can outline to its owners where improvements can be made, allowing users to oversee and analyze their personal data, and adjust accordingly. Seeing that the determinations of smart homes are to increase resource efficiency and optimize productivity, the uptake of such technologies somewhat implies that inhabitants who acquire them also aim for such, hence becoming voluntary subjects of surveillance and the quantified self simultaneously – in the former they are monitored by the devices they procure, and in the latter, they monitor their own home life through accessing the data captured by such devices. Thus, smart devices' sensory capabilities allow people to better "quantify" their existence and, as a result, make more educated, data-driven decisions based on an improved understanding of their behavior.[275]

However, the smart home does not just implicate voluntary subjects of self-monitoring. Take, for instance, a home device that monitors one family member's health condition. In this case even genetics data reveals and reflects information about said member's both immediate and extended

[274] "Maalsen and Sadowski, "The Smart Home on FIRE," 123.

[275] Gina Neff and Dawn Nafus, *Self-Tracking* (Massachusetts: The MIT Press, 2016), PDF version, 7-8; Mark Hoogendoorn and Burkhardt Funk, *Machine Learning for the Quantified Self: On the Art of Learning from Sensory Data* (Springer, 2018), PDF version, 1-2.

families. Therefore, while the quantified self is usually recounted as an individual pursuit, the resultant data has clear implications for other people.

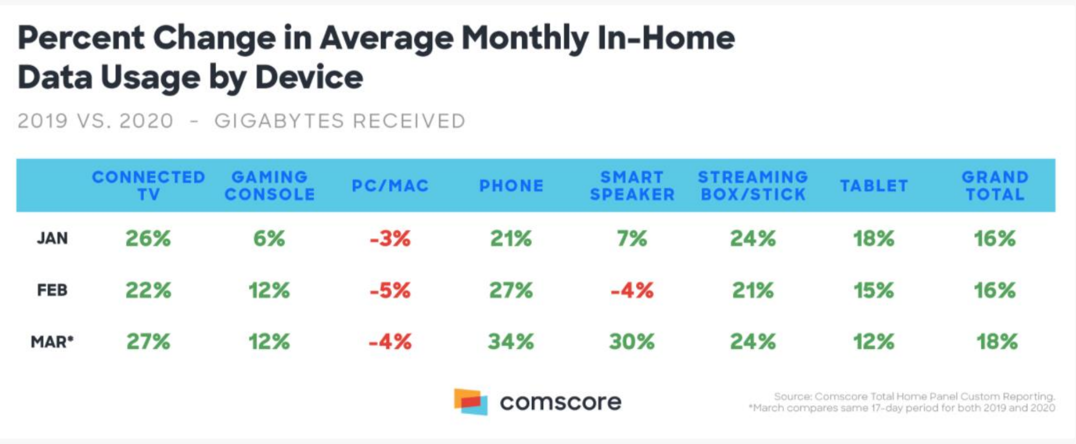
While the house has traditionally been a space for the concentration of intimacy, personal activities, and emotional behavior in some cultures,[276] sensorized and digital technologies have introduced a new variety of activities, formerly reserved for the external world, within its confines. Following widespread lockdown orders enacted in response to the COVID-19 pandemic, this trend appears to have accelerated. For many people around the world, home life has assumed a new significance as homes have become living spaces, schools, workplaces, and gyms all rolled into one due to national lockdowns.

Homes are able to support all these activities because of digital technologies and subsequent data production. Without teleconferencing and exam supervisions services, working and studying at home would not be suitable, respectively. The pandemic-induced lockdowns hence provoke an acceleration of the rate at which smart and digital technologies cross our homes' threshold: "[t]o stay at home we need to let other people in – government, authorities, employers, landlords – and digital technologies are the conduit through which this is done."[277]

[276] Mark Burdon, *Digital Data Collection and Information Privacy Law*, 39.

[277] Sophia Maalsen and Robyn Dowling, "Covid-19 and the accelerating smart home," *Big Data & Society* 7, no. 2 (2020): 4, https://journals.sagepub.com/doi/pdf/10.1177/2053951720938073

According to a Comscore report, the average daily in-home data usage increased 18% from 2019 to 2020.[278] What's more, the second highest percentage change was with the smart speaker with an increase of 30% since 2019:



Percent Change in Average Monthly In-Home Data Usage by Device

2019 VS. 2020 - GIGABYTES RECEIVED

	CONNECTED TV	GAMING CONSOLE	PC/MAC	PHONE	SMART SPEAKER	STREAMING BOX/STICK	TABLET	GRAND TOTAL
JAN	26%	6%	-3%	21%	7%	24%	18%	16%
FEB	22%	12%	-5%	27%	-4%	21%	15%	16%
MAR*	27%	12%	-4%	34%	30%	24%	12%	18%

comscore

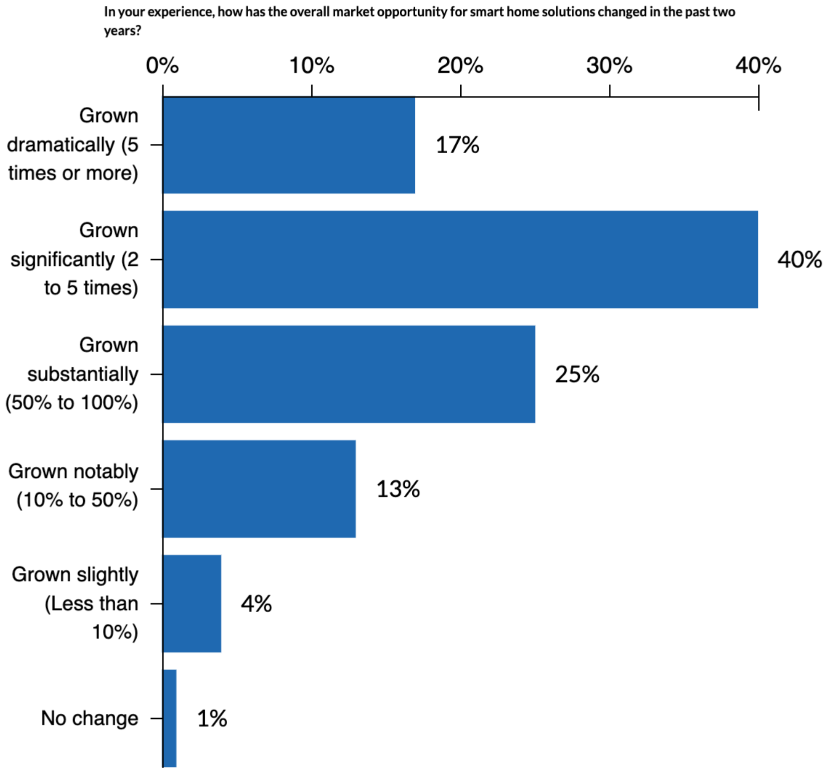
Source: Comscore Total Home Panel Custom Reporting.
*March compares same 17-day period for both 2019 and 2020

During COVID-19, people spent more time at home, which has driven changes in how they live in, interact with, and plan their homes, and smart home technologies provided a solution to the tremendous changes the pandemic brought. A study by Xiaomi has found that, since March 2020, 51% of consumers have acquired at least one smart device during the pandemic. Furthermore, 80% of consumers agree that there are substantial advantages to powering a home with smart devices.[279]

[278] Comscore, "Comscore Reports Surging Levels of In-Home Data Usage," https://www.comscore.com/Insights/Press-Releases/2020/3/Comscore-Reports-Surging-Levels-of-In-Home-Data-Usage

[279] Techcrunch, "New Xiaomi survey explores how Covid-19 is driving the new smart home, and what it means for 2021 and beyond," https://techcrunch.com/sponsor/xiaomi/new-xiaomi-survey-explores-how-covid-19-is-driving-the-new-smart-home-and-what-it-means-for-2021-and-beyond/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJowKP7QJ9qpPUe0BT_EDTcff79tc1AKtGO-S9I_HSspOfTWSy2i4QwDN2i_l8InptdEIK6tYjqaxsT-r-JR2A0KbhcEl67-8u-mxRdYkmQ7fCcsLcPo6irz1M4WXJ74DIEjxbPTAyeUvez2ESN10V7tfW4fWX3lxC112wLR6kYt

According to the International Data Corporation (IDC) Worldwide Quarterly Smart Home Device Trackers, global shipments of smart home technologies hit 801.5 million units in 2020, up 4.5% from 2019.[280] Despite the economic overturn and high unemployment caused by COVID-19, the smart home market remained resilient and still presented positive growth throughout all device categories. Indeed, smart home technology providers have seen the smart home market opportunity grow, as revealed in a study of 215 decision-makers at smart home original equipment manufacturers, detailed in the figure below:



[280] Jabil, "Smart Home Trends: What's Now and What's Next?" https://www.jabil.com/blog/connected-home-and-building-tech-trends.html

As people adopt and invite more smart technologies into their homes, they are giving even more access to their personal lives along with the data they generate. The strong concentration of varying activities into homes makes them a fruitful source of data for the detection of behavioral patterns.[281] And, once again, the technologies that are enabling lives to resume almost uninterrupted in the course of COVID-19 lockdowns, may very well normalize the heightened surveillance as well as control creep post-pandemic.

[281] Maalsen and Sadowski, "The Smart Home on FIRE,"

Chapter 3: Bridging Surveillance Theory and Practice – Debating the Potential Implications

In relation to **Smart Cities**, it may be argued that technological solutions alone may not be able to solve the deep-rooted structural issues because they do not tackle their root causes. Instead, they just make it possible to manage the manifestations of those difficulties more efficiently. Ironically, although most of the discourse on smart city applications is characterized by a pursuit of a more sustainable city,[282] Kate Crawford demonstrates in great detail the sizable extent of environmental damage that production and upkeep of digital technologies engender, noting already that "the carbon footprint of the world's computational infrastructure has matched that of the aviation industry at its height, and it is increasing at a faster rate."[283]

Some technologies have the greatest social influence not because of what they allow people to accomplish, but because of what they disclose about how the world works. While fear of technology is often communicated through narratives of its negative consequences, such unease is occasionally rooted in what technology reveals that was present all along. In this sense, COVID-19 serves as proof of smart cities' benefits seeing that cities with a robust digital infrastructure in place, able to gather and analyze data, can more quickly determine where adjustments are needed. However, while democratic smart city responses to the pandemic such as Seoul's indicates

[282] Angeliki Maria Toli, and Niamh Murtagh, "The Concept of Sustainability in Smart City Definitions," *Frontiers in Built Environment*, June 2020, https://www.frontiersin.org/articles/10.3389/fbuil.2020.00077/full
[283] Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, 42, 28-45.

successful stemming of the Coronavirus without complete disruption of social life, China likewise incites the efficiency and allure of a digital, authoritarian, and draconian response to the pandemic.

For sensors and networks to communicate with each other, and deliver real-time feedback in smart city operations, interoperability and data integration are key. This means that when cities acquire smart city technology from one service provider, all future procurements are done either from the same provider or one that is fully compatible. Since the US banned the Chinese tech firm Huawei's development of 5G mobile networks in its country, other countries have since joined,[284] signaling the emergence of a decoupling on 5G technologies. Seeing that there have already been occurrences of Huawei's surveillance cameras and data centers having left data exposed or leaked it (in Pakistan and Papua New Guinea, for instance), countries have raised concerns about national and data security:

> Because Huawei is required by law to cooperate with China's intelligence operations if asked, and because it has long benefitted from state support, countries that depend on the company are vulnerable to pressure from Beijing.[285]

5G networks are key to cloud computing and autonomous robotics, which we've already identified as an enabling technology to smart city applications. Part of the Sino-American trade war context,

[284] Shannon Tiezzi, "Sweden Becomes Latest – and Among Most Forceful – to Ban Huawei From 5G," *The Diplomat*, October 2020, https://thediplomat.com/2020/10/sweden-becomes-latest-and-among-most-forceful-to-ban-huawei-from-5g/

[285] Jonathan E. Hillman, "Huawei Strikes Back: To Beat China on Tech, America Must Invest in the Developing World," *Foreign Affairs*, November 2021, https://www.foreignaffairs.com/articles/china/2021-11-09/huawei-strikes-back

many other Chinese technology companies have now been included in the US's blacklist,[286] prohibiting the transfer of software and technology of US companies to such companies whose products, interestingly, are central to the smart city architecture, namely facial recognition technology, video surveillance cameras, microchips, among others.

The budding technological decoupling is not just a challenge for China and the US, but for Europe as well. In general, Europe remains divided with respect to the approach to embrace toward smart city proposal and Chinese technologies,[287] owing to divergent assessments of the security threat suggested by the concerned technology, differing types of relationships with China, and diverse levels of Huawei's technologies' presence in European countries. As a result, EU member states and institutions have also begun to push for more strategic autonomy in crucial technologies to relieve some dependence on the US or China. On the realm of smart city development, the EU's developed legal environment – particularly the General Data Protection Regulation (GDPR)[288] – already frames the way in which smart cities develop on European territory, and how EU-external smart city technology providers will have to alter and adapt their devices to the European market.

China's smart city architecture places great emphasis on security and hinges on a vast amount of data gathering and analysis, as well as a direct connection with public authorities such as the police.

[286] Takashi Kawakami, and Taisei Hoyama, "Trump's blacklist squeezes 200 Chinese companies as net widens: Huawei receives another reprieve while list ensnares AI startups," *NikkeiAsia*, November 2019, https://asia.nikkei.com/Economy/Trade-war/Trump-s-blacklist-squeezes-200-Chinese-companies-as-net-widens

[287] Hilary Clarke, "European split over Huawei 'threat' risks ruffling Western alliances as EU states build 5G partnerships despite accusations of spying," *South China Morning Post*, December 2018, https://www.scmp.com/news/world/europe/article/2177521/european-split-over-huawei-threat-risks-ruffling-western-alliance

[288] EUR-lex, "General Data Protection Regulation," https://eur-lex.europa.eu/eli/reg/2016/679/oj

In the future, it is likely that China's smart city model will differ even more from Europe and the US's smart cities, for a few reasons. Firstly, because, contrasting with the Chinese context, the trend in Europe along with other democratic states is toward additional regulation on data collection and use. Most importantly, though, because the Sino-American trade tensions which have already become technological tensions has engendered a competitive environment that will shape smart city development on a global scale. It is highly improbable that cities will be capable of easily combining American/Western and Chinese smart city technologies in the future. Curiously, all of the current spheres of competition between the US and China, namely AI, 5G, and Big Data, are amassed and concentrated in the smart city framework. Accordingly, it may be said that smart cities are coming to be the new battleground of Sino-American competition.

A more likely outcome is the development of *two* models of smart cities, with two kinds of infrastructures, norms, standards, networks, as well as different smart city definitions and conception of an optimal urban governance model. The bipolarization of globalization and of urbanization may engender two differing smart city architectures, as well as two differing kinds of urban life. Contemplating from a geostrategic standpoint, a bifurcated technology-5G-smart city ecosystem could very well lead to the rise of divided spheres of influence. Thus, the smart city not only involves the battleground for technological and economic competition among companies, but also that of competition between social and political systems, incorporating additional spheres of influence as well as geostrategic competition. To add to the perplexity of the reality as well as potential effects involved in the political economy of the smart city, in the words of American politician Henry Kissinger:

> Uncertainty over the nature, scope, or attribution of a cyber action may render seemingly basic factors a matter of debate – such as whether a conflict has begun, with whom or what the conflict engages, and how far up the escalation ladder the conflict between the parties may be. In that sense, major countries are engaged in a kind of cyber conflict now, though one without a readily definable nature or scope.[289]

Smart cities thus require much more attention than has been given regarding the implications for the liberal international order and global balance of power, especially when considering that out of the aforementioned 56 countries that employ smart city solutions, 50 are employing some degree of Chinese technology. Moreover, the digital services provided by smart city programs "created in one country could become the arteries and lifeblood of another country,"[290] and, should they become critical urban infrastructure, could give the country that exported this technology great leverage over each country that relies on it. Additionally, the Democracy Gap in 2020 – a metric of democratic backsliding – reached the highest level witnessed in the past 15 years, as the number of countries whose freedom declined was 73, and whose freedom improved was 28.[291]

Concerning **workplace surveillance**, we saw that Taylor and his advocacy of scientific management was taken up all around the world, turning the workplace into one where employee

[289] Henry Kissinger, Eric Schmidt, and Daniel Huttenlocher, *The Age of AI: And Our Human Future* (Little, Brown and Company, 2021) Kindle edition, 130 out of 205.
[290] Ibid., 110 out of 205.
[291] Sarah Repucci, and Amy Slipowitz, "Freedom in the World 2021: Democracy under Siege," *Freedom House*, https://freedomhouse.org/report/freedom-world/2021/democracy-under-siege

monitoring became a principle means to increase efficiency and productivity, since de-skilling work activities, relieving cognitive demand that was traditionally placed on workers, and dividing labor in spaces of rising mass production along with number of employees involved organization and oversight by managers.

Although some scholars argue that Taylorism had already been exhausted before the 21st century,[292] recent discussions regarding the organizational powers of digital technologies have conceptualized Taylorism as still present, possibly enhanced even by the increasingly digitized workplace. Bain et al., and Briken and Taylor, for instance, have outlined the reiteration of Taylorist techniques in call centers and online retail, respectively, where employees' output is precisely quantified and their work is contingent on monitoring and tight control.[293] Crowley et al. also make the case for defining the current work as being more suitably "neo-Taylorist" than "post-Fordist,"[294] demonstrating the recent expansion of Taylorism beyond manual and into managerial settings as well.

[292] E.g. Ulrich Jürgens, Thomas Malsch, and Knuth Dohse, *Breaking From Taylorism: Changing Forms of Work in the Automobile Industry* (Cambridge: Cambridge University Press, 1993)

[293] Peter Bain et al., "Taylorism, targets and the pursuit of quantity and quality by call centre management," *New Technology Work and Employment*, November 2002, 170-185, https://www.researchgate.net/publication/227630515_Taylorism_Targets_and_the_Pursuit_of_Quantity_and_Quality_by_Call_Centre_Management ; Kendra Briken and Phil Taylor, "Fulfilling the 'British way': beyond constrained choice – Amazon workers' lived experiences in workfare," *Industrial Relations Journal* 49, no. 5 (2018): 438-458, https://www.researchgate.net/publication/328784595_Fulfilling_the_'British_way'_beyond_constrained_choice-Amazon_workers'_lived_experiences_of_workfare

[294] Martha Crowley et al., "Neo-Taylorism at Work: Occupational Change in the Post-Fordist Era," *Social Problems* 57, no. 3 (2010): 421-447, https://academic.oup.com/socpro/article-abstract/57/3/421/1663710?redirectedFrom=fulltext

Brown et al. have likewise argued that a few of Taylorism's key concepts have been revived, coining this development as "Digital Taylorism," which involves:

> translating the knowledge work of managers, professionals, and technicians into working knowledge by capturing, codifying, and digitalizing their work in software packages, templates, and prescripts that can be transferred and manipulated by others regardless of location.[295]

The primary hypothesis is that, although new occupations are increasingly tied to employees' abilities and qualifications, tasks are contingent on the same scientific management methods which craft and chain work originally underwent within Taylorist methods. According to Digital Taylorism, intellectual and creative tasks – previously regarded as non-machinable – are likewise subject to the same "rationalizing" procedure as chain work. Once digitalized and codified, the human faculty for judgment and decision can be supplanted by automatic programs by using automated decision protocols. Moreover, jobs are also easier to change, export or replace since processes are more easily relocated owing to increased possibilities for technical mobility and computerized global networks. As companies begin to employ digital management tools that codify performance along with an employee's job description, the result is that workers are ceaselessly under pressure to elevate their performance.

[295] Phillip Brown, Hugh Lauder, and David Ashton, *The Global Auction: The Broken Promises of Education, Jobs and Incomes* (Oxford: Oxford University Press, 2011), PDF version, 72.

Astra Taylor asserts that “the kind of efficiency to which techno-evangelists aspire emphasizes standardization, simplification, and speed, not diversity, complexity, and interdependence.”[296] Interestingly, these aims fall right in line with Taylor’s objectives, thus validating the convergence of Taylorism and technological developments in the modern workplace. Even in work settings where the methods of scientific management are not explicitly employed, the Taylor-imbued tradition of employee surveillance for performance scrutiny measured alongside productivity scores is extensive. In this sense, it is useful to mention Professor Lucy Taksa’s description of the continuity of scientific management by framing it as a hegemonic ideology:

> While Taylor’s all-encompassing aims were not accomplished exactly in accordance with his aspirations, nevertheless, I suggest that SM has operated as a hegemonic ideology, which is still influencing organizational cultures today through a range of different management strategies.[297]

As working from home becomes the new norm against the COVID-19 backdrop, it is worth highlighting Suresh Gupta’s insights on the feasibility of such. She argues that to work from home, work needs to be standardized and unitized, otherwise it is not possible.[298] While moving labor to home-based production is not recent, with the use of apps, customer ratings, GPS, and other forms

[296] Quoted in Crawford, *Atlas of AI*, 72.

[297] Lucy Taksa, “Scientific Management,” in *The Oxford Handbook of Management*, ed. Wilkinson, Armstrong, and Lounsbury (Oxford: Oxford University Press, 2017), 5. https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780198708612.001.0001/oxfordhb-9780198708612
SM stands for Scientific Management

[298] Quoted in Brown, Lauder, and Ashton, *The Global Auction: The Broken Promises of Education, Jobs and Incomes*, 78.

of monitoring, employers have remained capable of instituting Taylorist techniques despite workplace dislocation.[299]

Noting the shift from traditional workplace surveillance to the current one wherein digital employee monitoring technology is a central feature, it may be argued that Bentham's Panopticon metaphor is more appropriately descriptive of the latter. Granted that the Panopticon entailed three key elements, namely the inspector's omnipresence which is warranted by his total invisibility, the complete visibility of surveillance objects, and the assumption of constant inspection by the watched – which produces a psychological shift in the worker –, it is possible to infer that the traditional employee surveillance paradigm never met these requirements. Firstly, the manager or supervisor, being always visible, was not omnipresent. Secondly, universal employee visibility did not exist, and workers were aware that they were being observed only when the manager was there, and hence there could be no supposition of workers being continuously monitored.

The emergence of computerized means of surveillance has profoundly altered the workplace, and for workers subjected to digital surveillance one could contend that the Panopticon's three main premises are increasingly being fulfilled. The digital gathering and storing of all productivity-related information establishes the employer's omnipresence. Employees' universal visibility is ensured because everything they do, from work output to bathroom breaks, can be monitored. As such, employees must assume that they are watched or watchable at all times. On another note,

[299] Matthew Cole, Hugo Radice, and Charles Umney, "The Political Economy of Datafication and Work: A New Digital Taylorism?" in *Beyond Digital Capitalism: New ways of living*, eds. Leo Panitch and Greg Albo (London: The Merlin Press, 2020), PDF version, 82.

Bentham's assertion that the Panoptic gaze, once internalized, exercised discipline and likewise led to self-discipline – or "technologies of the self," as Foucault put it –, are two dimensions of power which are greatly enhanced in the modern workplace given the enabled scrutiny and ubiquity as well as real-time feedback and analytics regarding workers' performance by digital surveillance technologies.

As the transition to working from home signals an increased uptake of employee monitoring tools – allowing for progressively individualized nudges –, so too have the effects of discipline and self-discipline amplified. Some considerations for the potential consequences of amplified surveillance in the workplace can be drawn, as some studies show that employee surveillance has increased stress in the workplace.[300] Productivity scores, while beneficial to employer's knowledge of the extent to which an employee's labor was fruitful, introduce a risk of bias for employees. Given that different roles command differing methods of working, and that even in similar roles people accomplish tasks through differing means, setting an all-encompassing definition of productivity may lead to biased scores. If productivity is prescribed by active time spent on the screen, and a worker spends only five hours actively during the day, it would attribute a low productivity score. What was not registered by the system was that this employee is a single father who had to abandon screen time to tend to his children, but completed the required amount of daily tasks nonetheless.

[300] Cornerstone, "Learning Corner With Jeffrey Pfeffer: To Build Trust, Cut Down on Surveillance—Even for Employees Working at Home," https://www.cornerstoneondemand.com/resources/blogs/learning-corner-jeffrey-pfeffer-build-trust-cut-down-surveillance-even-employees-working-home/; O'Connor, "Workplace surveillance may hurt us more than it helps," *Financial Times*.

Another concern is the potential for function creep, which breaks down transparency between employers and employees, and subsequently trust. This means that workers could be completely unaware of the degree to which they are monitored if the employer chooses not to be transparent about a system's usage. As employees are vaguely cognizant of the tracking but not the extent to which they are tracked, it may lead to more stress in the workplace. Finally, it is important to highlight that surveillance technology tends to be fashioned with employers being the end beneficiaries: the development of surveillance systems considers the impact on employers, but does not necessarily give employees the same concern. This only further proliferates the power asymmetries between employers and employees, tipping in favor of the former. While the employer is able to select which forms of surveillance benefits them, employees have little to no say on whether they even want to be monitored, and if yes, to what extent – and COVID-19 has only exacerbated this development. Since the COVID-19 pandemic appears to have created the ideal environment for surveillance technology to spread by requiring the bulk of the workforce to move to working from home, it is crucial to address the impact of such technology on employees' mental well-being.

The **smart home** can be seen as one surveillance environment where both disciplinary and modulatory powers overlap, as theorized by Foucault and Deleuze, respectively. While the smart home does not represent the form of disciplinary enclosure that Foucault envisioned, it does refine the home's integration into the larger digital surveillance infrastructure, realizing the breakdown of the boundary between other disciplinary domains and the home, as Deleuze foresaw.[301]

Despite this, it retains both modulatory and disciplinary qualities. The smart home is a spatial enclosure wherein residents can be subjected to disciplinary power. Disciplinary targeting, though, is derived from a dividualized[302] enclosure empowered by the diffusion of sensor networks which allow several activities traditionally carried out in distinct spaces to be practiced via a slew of distinct data infrastructures. When they subscribe to digital networks, individuals can undertake a number of activities such as labor, consumption, political participation, and education in various physical settings, which is quintessential of being mobile. On the other hand, subscription likewise aids these diverse activities' convergence into one physical space, like the home.

The infrastructure of screen and sensors affords increasingly more data, facilitating the creation of more advanced dividualized outputs.[303] More sensors thus imply more dividualized segments, which portend more prescriptive results and, as a consequence, more opportunities for economic (and possibly political) exploitation of behavioral patterns.[304] In the smart home, the morals, punishments, and abstracted rules of the disciplinary society can combine with modulation's reach, interminability, and circularity – disassociating discipline from a confined space. Disciplinary

[301] Deleuze, "Postscript on the Societies of Control," 4.

[302] "Dividuals", a term coined by Deleuze, represent the individual's data fragments. Anything referred to as dividualized therefore entails its division into any number of codified pieces which are then separated, analyzed, and distributed across "databanks".

[303] Mark Andrejevic, "Automating Surveillance," *Surveillance & Society* 17, no. 1/2 (2019): 11 https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/12930/8469

[304] Mark Andrejevic and Mark Burdon, "Defining the Sensor Society," *Television and New Media* 16, no. 1 (2015): 3, 5, https://eprints.qut.edu.au/120799/8/120799.pdf

conduct can now be exerted wherever a modulatory link exists. Herein lies the danger of the smart home's increased vulnerability of individuals – for powerful data collectors like Google and Amazon, everything may be dividualized and individualized, turned visible from the invisible, definitive and unceasing, fixed and yet pliable, linear and circular, as well as part of hierarchy and continuity.

As previously demonstrated, **social media surveillance** combines many surveillance actors that are keen on extracting information from social networking platforms – some are visible, others not. In the case of consumer surveillance, it is worth mentioning Shoshana Zuboff's account of the hidden processes of surveillance of personal data for which social media is a fecund source. In her book, Zuboff describes the magnitude of the technological changes affecting political and social life. These changes are the result of what she terms "surveillance capitalism", a new logic of accumulation that profits from the collection, rendering, and scrutiny of consumer data – which she calls "behavior surpluses" – by way of "instrumentarian" approaches which seek to promote "radical indifference", a manner of watching without witness.[305]

Surveillance capitalism entails more than the massive collection of personal data. Technology companies and their specialists, dubbed "the new priesthood", are establishing new kinds of power

[305] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Public Affairs, 2019), PDF version, 353-354, 479-482.
Instrumentarianism is the associated power of surveillance capitalism which signifies human behavior's instrumentation for the purposes of prediction, modification, control, and monetization. Radical indifference corresponds to the maximization of data flows while remaining indifferent to the implications for the targeted consumer.

and behavioral modification methods that operate outside of human knowledge and public responsibility:

> Data about the behaviors of bodies, minds, and things take their place in a universal real-time dynamic index of smart objects within an infinite global domain of wired things. This new phenomenon produces the possibility of modifying the behaviors of persons and things for profit and control.[306]

The problem here is that using personal histories and similarities with other consumers leaves corporations with added leverage in the marketplace that undermines the idea of consumer sovereignty, thus begetting disproportionate corporate power.

On government surveillance of social media, Freedom House details the negative implications of such practice.[307] First, authorities can gather and analyze information about personal relationships, sexual preferences, and spiritual beliefs, and distribute them to third parties. Second, immigration officials can disallow individuals' entry based on their social, religious, or political views expressed on social networks, or that of their family and friends. Third, authorities are able to disrupt nonviolent protests before they even begin, as well as track the names of those in attendance.

[306] Shoshana Zuboff, "Big Other: surveillance capitalism and the prospects of an information civilization," *Journal of Information and Technology* 30 (2015): 85, https://cryptome.org/2015/07/big-other.pdf

[307] Adrian Shahbaz and Allie Funk, "Freedom on the Net 2019 Key Finding: Governments harness big data for social media surveillance," *Freedom House*, 2019, https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance

These are just a few examples, and though it is still the case that Autocracies remain at the forefront of state surveillance, it is likewise worth highlighting how these misuses are not exclusive to autocratic countries. Freedom House has also documented reports of abuse in countries with considerable protections for fundamental freedoms, namely in the UK and US.[308] Although Western applications of surveillance are less invasive, we've already seen that the effects are not entirely different from authoritarian exercises of surveillance. Thus, as observed by John Gray, it is not hard to picture how "soft paternalism" may risk morphing into "soft totalitarianism," wherein all features of human behavior would be susceptible to social engineering.[309]

Russia and Turkey (among others) are both trying to get their populations to use domestically-produced social media platforms, for the speculated purposes of attaining greater access to their citizens' data.[310] Evidently, the aforementioned bipolarization of globalization is not just a discussion involving great powers such as the US, EU and China, but all these other countries around world that are also exploring ways to create home-grown versions of state surveillance – getting citizens to transition from a foreign network platform that is hard to surveil to one that is domestically controlled and, therefore, easy to surveil. As Kissinger, Huttenlocher, and Schmidt point out in their book:

[308] Shahbaz and Funk, "Freedom on the Net 2019 Key Finding: Governments harness big data for social media surveillance," *Freedom House*.

[309] John Gray, "Surveillance Capitalism Vs. The Surveillance State," *Noema*, June 2020, https://www.noemamag.com/surveillance-capitalism-vs-the-surveillance-state/

[310] See Chapter 2.2 (Social Media Surveillance) for reference of these countries' moves to control online speech.

> In time, spheres of regional technology standards could develop, with various AI-enabled network platforms and the activities or expressions they support evolving along parallel but entirely distinct lines and with communication and exchange between them growing increasingly foreign and difficult.[311]

In this sense, technology that was formerly believed to be a tool for bridging national divides and disseminating objective truth, seems likelier now than ever to turn into the methods by which nations and individuals diverge into disparate and "mutually unintelligible realities."[312]

On a more general note of surveillance practices, although it's quite clear that the COVID-19 pandemic has altered and will continue to shape the urban landscape as we know it, it's still too early to make any conclusions vis-à-vis surveillance practices from this experience. In fact, Francis Fukuyama even stated that identifying the underlying ramifications of the current crisis might take years, asserting that "[f]uture historians will trace comparably large effects to the current coronavirus pandemic; the challenge is figuring them out ahead of time."[313]

Nevertheless, it is still possible to trace the potential impact of globally widespread surveillance apparatuses. As we've seen, information and communication technology give great leeway to surveillance practices, and some scholars like Gary T. Marx argue even that it has qualitatively altered the nature of surveillance.[314] Demonstrated above, COVID-19 has greatly spurred and

[311] Kissinger, Schmidt, and Huttenlocher, *The Age of AI: And Our Human Future*, 110 out of 205.
[312] Ibid., 21 out of 205.
[313] Francis Fukuyama, "The Pandemic and Political Order: It Takes a State," *Foreign Affairs*, July/August 2020. https://www.foreignaffairs.com/articles/world/2020-06-09/pandemic-and-political-order
[314] Gary T. Marx, *Undercover: Police Surveillance in America* (Berkeley: University of California Press, 1988), 208.

intensified the adoption of increasingly pervasive surveillance systems all over the world, as digital technologies have been framed as the best weapon to stemming a virus that thrives off human contact, and individuals have acquiesced to such conditions more or less out of necessity and concern for their physical health. Here it may be useful to frame this historical moment as another episode of "surveillance exceptionalism" seeing that the democratic mechanisms that citizens rely on to defend their rights and freedoms against such invasive practices seem to have been disregarded by a sneaking technological determinism.

As a result of the COVID-19 crisis, not only has surveillance moved into spaces previously considered free of institutional, economic, and governmental interference, such as the home, it likewise signifies that today, no physical realm exists wherein humans are exempt from surveillance. The amount of data that such systems generate has never before reached such colossal heights, as more and more aspects our actions and decisions are monitored, captured, transformed, and stored. John Gray points out that when considering the expansion in the West and China of surveillance states for purposes of bio-monitoring, the significant shift from physical mobility and contact to virtual connection, as well as the extension of government intervention in the economy we arrive at a potentially permanently altered landscape.[315] As such, the COVID-19-induced accelerated development and employment of surveillance technologies – which has thus far outpaced legislation – will presumably have far-reaching economic, cultural, and political

[315] John Grey in "Yuval Harari, Elif Shafak, Dambisa Moyo, Eric Schmidt & Others: How COVID Will Change Us," *Noema*, June 2020, https://www.noemamag.com/yuval-harari-elif-shafak-dambisa-moyo-eric-schmidt-how-covid-will-change-us/

consequences, substantially reshaping the structures of emerging societies as well as our personal lives. The normalization of mass surveillance poses dangers and raises problems that should be the focus of continuing, critical discussion.

On this matter, it seems appropriate to draw from Foucault's account of the plague and how such experience sanctioned increased social control of populations. With COVID-19, it appears fairly obvious that we have been witnessing a comparable systematic, underlying process. To stem the virus, prevention and regulation in the name of health make the development of profiles, surveillance, and statistics essential considerations, thus resulting in the extension and further reinforcement of biopolitics into all spheres of life. Through biometric surveillance, which involves technologies like facial recognition and temperature screening, health monitoring occurs everywhere, including the workplace, home, airports, supermarkets, to name a few. As a consequence, the exercise of biopower becomes widespread and consolidated, which is precisely what Bentham had dreamt of when he advocated that permanent visibility of identities would deter certain forms of behavior.

Aside from obvious concerns over the erosion of *privacy* – since increased surveillance renders a few of the legal means for privacy protection largely obsolete – and *harmful predictions* – since predictive capabilities may be used to discipline or punish individuals based on propensities and not their actions, which denies free will and corrodes human dignity, the greatest threat may very well be that individuals may become victims of a data *dictatorship*, wherein surveillance actors fetishize the information and the output of analyses, leading to their eventual misuse. Big data, when used appropriately and responsibly, is a valuable tool for rational decision-making. When used improperly, "it can become an instrument of the powerful, who may turn it into a source of repression, either by simply frustrating customers and employees or, worse, by harming citizens."[316] Therefore, guarding against overreliance on data is crucial.

An important reminder is that for all surveillance tools, the outcomes depend on who wields it and for what purposes they are wielded. The rapid spread of technologies of datafication is changing what counts as known, likely, and certain, redefining the conditions of social life for the human subject in the process. Therefore, it is crucial to seek answers regarding which actors are behind such systems and what their objectives are, with an emphasis on questioning if such applications are making society better, and not only whether they are making things more efficient. If Democracies are to implement such ubiquitous monitoring operations, it is absolutely vital for both the regime's endurance and citizens' welfare that they ensure that surveillance is practically effective, socially acceptable, and legally sanctioned. Yuval Noah Harari rightly underscores the need for politicians to "find the right balance between useful surveillance and dystopian nightmares."[317]

[316] Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, 152.
[317] Yuval Noah Harari, "Lessons From a Year of Covid," *Financial Times*, February 2021, https://www.ft.com/content/f1b30f2c-84aa-4595-84f2-7816796d6841

Conclusion

What binds most surveillance studies fields together is an overall consensus that surveillance is crucial to the functioning of modern societies. While some may disagree that monitorization is the most important cultural logic or social process, its influence and pervasiveness are hard to contest. “It is how organizations and people make sense of and manage the world. It is also how power relations are established and reproduced.”[318] Thus, rather than jump straight into an analysis of the present extent and nature of surveillance practices, this research started with an overview of the philosophical background of surveillance tools for social purposes in order to aid understanding of the normative frameworks which condone, recommend, limit, and make it meaningful, as well as to encourage inquiry into the true function of surveillance, which is seldom visible.

Jeremy Bentham’s Panopticon, although not of the same nature as the algorithmic oversight of present surveillance systems, was already a proponent of ever-present monitoring, given that one of its main features is the illusion of uninterrupted surveillance (wherein the watched may not be constantly monitored but believe they are). Moreover, the Panopticon inspector’s omnipresence – ensured by his invisibility – and the ubiquitous visibility of subjects, are equally important elements to consider for bridging the relations between traditional and digital forms of surveillance. Michel Foucault depicts the plague of the 19th century as having given rise to disciplinary projects, of which the Panopticon is the architectural figure. The Panopticon, for Foucault, represents a transformation from the plague because it is a permanent structure,

[318] *Surveillance Studies: A Reader*, xxxi

becoming normal and no longer exceptional. Essentially, Foucault portrayed the power mechanism in the Panopticon – Panopticism – as being a generalizable power design of the governing technique that fosters “docile bodies,” and deemed it as a model of disciplinary control in the modern world.

Frederick Winslow Taylor, a major proponent of Scientific Management, provides essential contributions to the extension of surveillance to the workplace, which currently constitute smart technologies that previously did not exist, thus strengthening the disciplinary power enmeshed in Taylorist techniques. Finally, in the transition from the disciplinary society, Gilles Deleuze asserts that, with new technologies, power and control are seemingly more flexible and dispersed, and the globalization and subsequent prevalence of capitalism also shifted organization from hierarchical observations to decoding as well as recoding of information, thus more accurately describing modern digital surveillance practices and the associated power relations.

Although social life has always involved monitoring mechanisms, with the advancement of modernity and the accompanying digital revolution, along with that of a centralized bureaucratic state, their scope has especially broadened. Traditionally, data used to be a scarce commodity that, given its value, was either expensively traded or covetously guarded. In the preceding decades, however, political lobbying and technological developments have completely reversed this position. Data now flow to lengths previously unfeasible, are sustained by robust infrastructures and are low in cost, and are progressively accessible and open. The result is the ongoing data revolution that is already, as shown in previous sections, reshaping how business is conducted, knowledge is produced, and governance enacted, along with raising various questions vis-à-vis surveillance, security, privacy, intellectual property rights, social sorting, and profiling.

The global spread of COVID-19 adds a new wrinkle to the debate over surveillance and privacy as it has paved the way for data collecting and tracking on a scale that would have been unthinkable in previous times, hence underscoring the importance of looking at how and to what extent this pandemic is influencing surveillance practices and further implementation of technology. On all accounts, the government strategies of surveillance involving AI, development of smart city projects and their accompanying monitoring capabilities, employee surveillance in the workplace and at home, data collection and processing on social networks, smart home technologies and consequent surveillance of the private home space, have all intensified as a result of the COVID-19 crisis. This shouldn't come as a surprise in light of Foucault's prescient account of how plagues tend to fast-forward historical processes.

Interestingly, Bentham's Panopticon metaphor appears more suited to describe modern employee surveillance operations than traditional forms of employee monitoring, as the opaqueness of smart surveillance systems better ensures the invisibility of the overseer and better perpetuates the belief among the watched that they are (or may be) constantly monitored. The smart home creates an ominous setting in which disciplinary power (Foucault) can transcend enclosure through modulatory tethers (Deleuze), and begets the home's integration into the larger digital surveillance infrastructure, magnifying the opportunities for data collection and analysis. Seeing that COVID-19 significantly boosted employee oversight in the transition to remote work with an accept-it-orquit plot, Taylorism is less easy to reject, and its effects may be even more pressing given the efficiency with which digital technologies take over the duty of oversight, culminating in the formation of what some scholars term Digital Taylorism or Neo-Taylorism. In social networks, deriving consumer data by corporations is an obvious trend of what Zuboff dubs surveillance capitalism, which has implications for the capacities of behavior modification.

Beyond surveillance theory, some discernments concerning the impact of surveillance are possible. Smart cities further reinforce geopolitical tensions, especially between the US and China seeing that all of the current spheres of competition between these two countries, namely AI, 5G, and Big Data, are amassed and concentrated in the smart city framework. Moreover, the discourse associated with smart city endeavors involving the positive pursuit of a more sustainable urban space is somewhat paradoxical since it has been demonstrated that the production and upkeep of smart technologies generates considerable environmental damage. In relation to government surveillance, abuse of these technologies has already been reported by Freedom House even in countries with strong democratic norms, signaling democracy’s increased vulnerability and risk of backsliding, which calls into question the notion that digital and more traditional surveillance operations are innocuous intrusions that are employed in democratic societies with adequate oversight and restraint. Nevertheless, authoritarian governments remain at the forefront of state surveillance, as some dictatorships are capitalizing on digital technologies and surveillance to quash dissent, extending beyond China’s Great Firewall to encompass Russia’s attempt at creating an alternative YouTube (Rutube), Iran an alternative internet, among others. As autocrats successfully harness these tools, they further reinforce their regime's durability.[319] Consequently, the continuation of these programs, while not certain, has a *high potential* for a reconfiguration of the current world order.

Considering this, it may be inferred that the historical development of smart machines and Big Data which converge to create the modern surveillance apparatus has developed technologies that target the obscure gap between the world and human experience – technologies which form new boundaries and patterns of intelligibility. Particularly, surveillance systems are instituting a different set of control and power mechanisms, now inclusive of processes that were once self-driven and/or relatively unofficial. Aside from obvious concerns over the erosion of privacy and harmful predictions associated with surveillance systems, the greatest threat may very well be that individuals may become victims of a data dictatorship, wherein surveillance actors fetishize the information and the output of analyses, leading to their eventual misuse. Therefore, guarding against overreliance on data is crucial, lest we make the same mistake as Icarus, who valued his technical power to fly but misused it, leading to his fatal fall into the sea.

An important reminder is that for all surveillance tools, the outcomes depend on who wields it and for what purposes they are wielded. The swift spread of technologies of datafication is changing what counts as known, likely, and certain, redefining the conditions of social life for the human subject in the process. Accordingly, the ethical and political stakes must actively tackle what kinds

[319] Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright, "The Digital Dictators: How Technology Strengthens Autocracy," *Foreign Affairs* 99, no. 2 (2020): 104

of precepts these technologies are being built to support as well as what spaces for alternatives are left.

Bibliography

Abika. "Abika Consulting." https://www.abikaconsulting.com/

ActivTrak. "How ActivTrak Works." https://www.activtrak.com/how-it-works/

AI for Humanity. "French Strategy for Artificial Intelligence." https://www.aiforhumanity.fr/en/

Albino, Vito, Uberto Berardi, and Rosa Maria Delgado. "Smart cities: definitions, dimensions, and performance," *Journal of Urban Technology* 22, no. 1 (2015): 1723-1738. http://cl.uw.edu.pl/dok/smart_cities.pdf

Alibaba Cloud, "Apsara Stack." https://www.alibabacloud.com/product/apsarastack

Apple. "Create Scenes and Home automations with the Home app." https://support.apple.com/en-us/HT208940

Andrejevic, Mark. "The Work of Watching One Another: Lateral Surveillance, Risk, and Governance." *Surveillance & Society* 2, no. 4 (2005): 479-497. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3359/3322

Andrejevic, Mark. "Automating Surveillance." *Surveillance & Society* 17, no. 1/2 (2019): 7-13. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/12930/8469

Andrejevic, Mark, and Mark Burdon. "Defining the Sensor Society," *Television and New Media* 16, no. 1 (2015): 19-36 https://eprints.qut.edu.au/120799/8/120799.pdf

Angwin, Julia. “The Web’s New Gold Mine: Your Secrets” *The Wall Street Journal*, July 2010. https://www.wsj.com/articles/SB10001424052748703940904575395073512989404

Aronson, Samuel L. “Crime and Development in Kenya: Emerging Trends and the Transnational Implications of Political, Economic, and Social Instability.” *Inquiries Journal/Student Pulse* 2 no. 9 (2010). http://www.inquiriesjournal.com/a?id=278

Asawateera, Pracha, “Phuket Smart City Road Map.” https://phuketrealestateassociation.files.wordpress.com/2016/10/pkt-smartcity-ws-update.pdf

Australian Government Department of Health. “COVIDSafe App.” https://www.health.gov.au/resources/apps-and-tools/covidsafe-app

BAAI. “Beijing AI Principles.” https://www.baai.ac.cn/news/beijing-ai-principles-en.html

Bain, Peter, Aileen Watson, Gareth Mulvey, Phil Taylor, and Gregor Gall. “Taylorism, targets and the pursuit of quantity and quality by call centre management,” *New Technology Work and Employment*, November 2002. https://www.researchgate.net/publication/227630515_Taylorism_Targets_and_the_Pursuit_of_Quantity_and_Quality_by_Call_Centre_Management

Ball, Kirstie, Kevin Haggerty, and David Lyon, ed. *Routledge Handbook of Surveillance Studies*. Oxford: Routledge, 2012. PDF version.

Balta-Ozkan, Nazmiye, Rosemary Davidson, Martha Bicket, and Lorraine Whitmarsh. "Social barriers to the adoption of smart homes." *Energy Policy* 63 (2013): 363-374. https://www.sciencedirect.com/science/article/abs/pii/S0301421513008471

Basu, Medha. "Exclusive: Phuket's smart city vision," *GovInsider*, December 2017." https://govinsider.asia/smart-gov/phuket-smart-city-digital-economy-pracha-asawathira/

Bentham, Jeremy, and Miran Božovič. *The Panopticon Writings*. London: Verso Books, 1995. PDF version.

Beveiliging Niews. "Rotterdam deploys camera trucks against 'corona offenders'." https://beveiligingnieuws.nl/nieuws/rotterdam-zet-camerawagens-in-tegen-corona-overtreders

Bowring, John, ed. *The Works of Jeremy Bentham*, 11 Vols. Edinburgh: William Tait, 1838-1843. PDF version.

Boyne, Roy. "Post-Panopticism." *Economy and Society* 29, no. 2 (2000): 285-307. https://www.tandfonline.com/doi/abs/10.1080/030851400360505

Briken, Kendra, and Phil Taylor. "Fulfilling the 'British way': beyond constrained choice – Amazon workers' lived experiences in workfare." *Industrial Relations Journal* 49, no. 5 (2018): 438-458. https://www.researchgate.net/publication/328784595_Fulfilling_the_'British_way'_beyond_constrained_choice-Amazon_workers'_lived_experiences_of_workfare

Brown, Philip, Hugh Lauder, and David Ashton. *The Global Auction: The Broken Promises of Education, Jobs and Incomes*. Oxford: Oxford University Press, 2011. PDF version.

Browning, Gary. *A History of Modern Political Thought: The Question of Interpretation*. Oxford: Oxford University Press, 2016. PDF version.

Brunon-Ernst, Anne, ed. *Beyond Foucault: New Perspectives on Bentham's Panopticon*. Surrey: Ashgate Publishing, 2012. PDF version.

Burdon, Mark. *Digital Data Collection and Information Privacy Law*. Cambridge: Cambridge University Press, 2020. PDF version

Catchacheat. "How to Catch Your Cheating Lover." https://www.catchacheat.com/

CIFAR. "Pan-Canadian AI Strategy." https://cifar.ca/ai/

CIFAR, "Pan-Canadian AI Strategy Impact Report (AICAN 2020)." https://cifar.ca/wp-content/uploads/2020/11/AICan-2020-CIFAR-Pan-Canadian-AI-Strategy-Impact-Report.pdf

Chen, Zifeng, and Clyde Yichen Wang. "The Discipline of Happiness: The Foucauldian Use of the "Positive Energy" Discourse in China's Ideological Works." *Journal of Current Chinese Affairs* 48 (2): 2020, 201-225 https://journals.sagepub.com/doi/pdf/10.1177/1868102619899409

Cheung, Weng Shen. "Amsterdam institutions leading AI collaboration to fight COVID-19." *Iamsterdam,* April 2020. https://www.iamsterdam.com/en/business/news-and-insights/news/2020/amsterdam-institutions-ai-collaboration-coronavirus

China's State Council. "A Next Generation Artificial Intelligence Development Plan." https://na-production.s3.amazonaws.com/documents/translation-fulltext-8.1.17.pdf

China.org.cn. "National New-Generation AI Innovation & Development Pilot Zone established in Beijing." http://www.china.org.cn/china/2019-02/22/content_74493744.htm

Clarke, Hilary, "European split over Huawei 'threat' risks ruffling Western alliances as EU states build 5G partnerships despite accusations of spying." *South China Morning Post*, December 2018. https://www.scmp.com/news/world/europe/article/2177521/european-split-over-huawei-threat-risks-ruffling-western-alliance

Clayton, James. "Facial recognition beats the Covid-mask challenge." *BBC*, March 2021. https://www.bbc.com/news/technology-56517033

Cohen, David. "eMarketer Ups 2020 Projections for Time Spent on Social Networks Due to Covid-19." *Adweek,* May 2020. https://www.adweek.com/performance-marketing/emarketer-ups-2020-projections-for-time-spent-on-social-networks-due-to-covid-19/

Cole, Mathew, Hugo Radice, and Charles Unmey. "The Political Economy of Datafication and Work: A New Digital Taylorism?" In *Beyond Digital Capitalism: New ways of living*, eds. Leo Panitch and Greg Albo. London: The Merlin Press, 2020). PDF version.

Comparitech. “The world’s most surveilled cities.” https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

Comscore. “Comscore Reports Surging Levels of In-Home Data Usage.” https://www.comscore.com/Insights/Press-Releases/2020/3/Comscore-Reports-Surging-Levels-of-In-Home-Data-Usage

Cornerstone. “Learning Corner With Jeffrey Pfeffer: To Build Trust, Cut Down on Surveillance—Even for Employees Working at Home.” https://www.cornerstoneondemand.com/resources/blogs/learning-corner-jeffrey-pfeffer-build-trust-cut-down-surveillance-even-employees-working-home/

Crawford, Kate. Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. New Haven: Yale University Press, 2021. PDF version.

Crozier, Ry. “Govt to release source code of forthcoming ‘COVID trace’ app.” *itnews*, April 2020. https://www.itnews.com.au/%20news/govt-to-release-sourcecode-of-forthcoming-covid-traceapp-546884

Crowley, Martha, Daniel Tope, Lindsey Joyce Chamberlain, and Randy Hodson. “Neo-Taylorism at Work: Occupational Change in the Post-Fordist Era.” *Social Problems* 57, no. 3 (2010): 421-447. https://swab.zlibcdn.com/dtoken/9bfec8f5254eabe869aac01c9f58b061

DataReportal. “Digital 2021 July Global Statshot Report.” July 2021. https://datareportal.com/reports/digital-2021-july-global-statshot

Deleuze, Gilles. "Postscript on the Societies of Control." *October* 59 (1992): 4. https://www.blogs.hss.ed.ac.uk/crag/files/2015/09/deleuze_control.pdf?fbclid=IwAR1chxk3wkw78GY1CWDUw__BzsmR8oIAs528XO-sVnLcVK_b52HMU_Rad4I

Deleuze, Gilles. *Foucault*. Minneapolis: University of Minnesota Press, 1988. PDF version.

Doty, Philip. "Oxymorons of privacy and surveillance in "smart homes"." *Journal of the Association for Information Science and Technology* 57, no. 1 (2020): 1-11. https://asistdl.onlinelibrary.wiley.com/doi/abs/10.1002/pra2.222?af=R

DutchNews. "Dutch police facial recognition database includes 1.3 million people." https://www.dutchnews.nl/news/2019/07/dutch-police-facial-recognition-database-includes-1-3-million-people/

Eden Strategy Institute, "Top 50 Smart City Governments." 2021. https://www.smartcitygovt.com/202021-publication

Elden, Stuart. "Plague, Panopticon, Police." *Surveillance & Society* 1, no. 3 (2003): 240-253. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3339/3301

Elmer, Greg. "A diagram of panoptic surveillance." *New Media & Society* 5, no. 2 (2003): 231-247. https://www.dhi.ac.uk/san/waysofbeing/data/data-crone-elmer-2003.pdf

Encyclopedia Britannica. "Artificial Intelligence." https://www.britannica.com/technology/artificial-intelligence

ESI Thought Lab. “Smart City Solutions for a Riskier World.” https://econsultsolutions.com/wp-content/uploads/2021/03/ESITL-Smart-City-Solutions-eBook-Final.pdf

EUR-lex, “General Data Protection Regulation.” https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Commission. “Biometrics Technologies.” https://ati.ec.europa.eu/reports/technology-watch/biometrics-technologies-key-enabler-future-digital-services

Facebook AI. “Learning from videos to understand the world.” https://ai.facebook.com/blog/learning-from-videos-to-understand-the-world/

Facebook. “Data Policy.” https://www.facebook.com/about/privacy/update

Fadell, Anthony M., Yoky Matsuoka, David Sloo, Maxime Veron. Smart-Home Automation System That Suggests or Automatically Implements Selected Household Policies Based on Sensed Observations. US Patent No. US 20200012242 A1. January 9, 2020. https://patentimages.storage.googleapis.com/86/c5/e3/d9b9efe49d003c/US20200012242A1.pdf

Federal Register of Legislation. “Biosecurity Act 2015.” https://www.legislation.gov.au/Details/C2020C00127

Feldstein, Steven. *The Global Expansion of AI Surveillance*. Washington: Carnegie Endowment for International Peace, 2019. PDF version https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf

Fonseca, Esperanza. “Worker Surveillance Is on the Rise, and Has Its Roots in Centuries of Racism.” *Truthout*, June 2020. https://truthout.org/articles/worker-surveillance-is-on-the-rise-and-has-its-roots-in-centuries-of-racism/

Foucault, Michel. *Discipline and Punish*. New York: Vintage Books, 1995. PDF version.

Foucault, Michel, ed. "The Eye of Power." In *Power/Knowledge: Selected Interviews and Other Writings (1972-1977)*. New York: Pantheon Books, 1980. PDF version.

Foucault, Michel, ed. *Power: essential works of Foucault 1954-1984*. London: Penguin Books, 2002. PDF version.

Foucault, Michel. “Society Must Be Defended.” In *Lectures at the Collège de France 1975-76*. New York: Picador, 2003. PDF version.

Foucault, Michel. *History of Madness*. Abingdon: Routledge, 2006. PDF version.

Foucault, Michel, ed. *Psychiatric Power: Lectures at the Collège de France 1973-1974*. New York: Palgrave Macmillan, 2006. PDF version.

Ford, Martin. *Rise of the Robots: Technology and the Threat of a Jobless Future*. New York: Basic Books, 2015. PDF version.

Freedom House, “Freedom on the Net 2018.” https://freedomhouse.org/sites/default/files/FOTN_2018_Final.pdf

Fry, Hannah. Hello World: Being Human in the Age of Algorithms. New York: W. W. Norton & Company, 2018. PDF version.

Fuchs, Christian, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval, ed., *Internet Surveillance: The Challenges of Web 2.0 and Social Media*. New York: Routledge, 2012. PDF version

Fukuyama, Francis. "The Thing That Determines a Country's Resistance to the Coronavirus." *The Atlantic*, March 2020. https://www.theatlantic.com/ideas/archive/2020/03/thing-determines-how-well-countries-respond-coronavirus/609025/

Fukuyama, Francis. "The Pandemic and Political Order: It Takes a State." *Foreign Affairs*, July/August 2020. https://www.foreignaffairs.com/articles/world/2020-06-09/pandemic-and-political-order

Furedi, Frank. *Culture of Fear: Risk-Taking and the Morality of Low Expectation*. London: Bloomsburry Continuum, 2018. EPUB version.

Fyiscreening. "Employment Screening and Background Checks." https://fyiscreening.com/

Gapper, John. "Amazon's Astro robot is a symbol of the surveillance age." *Financial Times*, October 2021. https://www.ft.com/content/c2cf67d6-a143-4aff-9eb1-b7a4e93c3c73

Gandy, Oscar H., *The Panoptic Sort: Towards a Political Economy of Personal Information*. Oxford: Westview, 1993. PDF version.

Giddens, Anthony. *The Nation State and Violence*. Cambridge: Polity Press, 1985. PDF version.

GOVTECH Singapore. "Responding to COVID-19 With Tech." https://www.tech.gov.sg/products-and-services/responding-to-covid-19-with-tech/

Gram-Hanssen, Kirsten, and Sarah J. Darby. "“Home is where the smart is”? Evaluating smart home research and approaches against the concept of home." *Energy Research & Social Science* 37 (2018): 1-18. https://ora.ox.ac.uk/objects/uuid:3d5ca446-c101-42de-b965-b244afcf415c/download_file?file_format=pdf&safe_filename=Home%2Bis%2Bwhere%2Bthe%2Bsmart%2Bis.%2Bsubmitted_150917.pdf&type_of_work=Journal+article

Gray, John. “Surveillance Capitalism Vs. The Surveillance State.” *Noema*, June 2020. https://www.noemamag.com/surveillance-capitalism-vs-the-surveillance-state/

Halegoua, Germain. “An Introduction to Smart Cities.” In *Smart Cities*. Cambridge: The MIT Press, 2020. EPUB version.

Haggerty, Kevin D., and Richard V. Ericson. “The Surveillant Assemblage.” *British Journal of Sociology* 51, no. 4 (2000): 605-22. https://www.uio.no/studier/emner/matnat/ifi/INF3700/v17/bakgrunnsnotat/the_surveillant_assemblage.pdf

Harari, Yuval Noah. "The World After Coronavirus," *Financial Times*, March 2020. https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

Harari, Yuval Noah. “Lessons From a Year of Covid.” *Financial Times*, February 2021. https://www.ft.com/content/f1b30f2c-84aa-4595-84f2-7816796d6841

Harper, Richard, ed. *Inside the Smart Home*. London: Springer, 2003. PDF version

Harwell, Drew. “Managers turn to surveillance software, always-on webcams to ensure employees are (really) working from home.” *Washington Post*, April 2020. https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance/

Hasselberger, William. “Ethics beyond Computation: Why We Can’t (and Shouldn’t) Replace Human Moral Judgement with Algorithms.” *Social Research: An International Quarterly* 86, no. 4 (2019): 977-999.

Hillman, Jonathan E. “Huawei Strikes Back: To Beat China on Tech, America Must Invest in the Developing World.” *Foreign Affairs*, November 2021. https://www.foreignaffairs.com/articles/china/2021-11-09/huawei-strikes-back

Hoffman, Marcelo. “Disciplinary Power.” In *Michel Foucault: Key Concepts*. Ed. Dianna Taylor. London: Routledge, 2014. PDF version.

Hong, Sun-Ha, *Technologies of Speculation: The Limits of Knowledge in a Data-drive Society*. New York: New York University Press, 2020. PDF version.

Hoogendoom, Mark, and Burkhardt Funk. *Machine Learning for the Quantified Self: On the Art of Learning from Sensory Data*. Springer, 2018. PDF version.

Huawei. “Kenyan Safe City Can Now Sleep Better.” https://archive.li/pBsxf#selection-4471.1-4471.38

Huawei. "Video Surveillance as the Foundation of 'Safe City' in Kenya." https://www.huawei.com/en/industry-insights/technology/digital-transformation/video/videosurveillance-as-the-foundation-of-safe-city-in-kenya

Hubstaff. "Hubstaff features." https://hubstaff.com/features/employee_monitoring

IBM Institute for Business Value. "COVID-19 and the Future of Business." https://www.ibm.com/downloads/cas/1APBEJWB

IBM Institute for Business Value. "Digital Acceleration." https://www.ibm.com/downloads/cas/MBV83XAY

IBM. "What is a Digital Twin?" https://www.ibm.com/topics/what-is-a-digital-twin

Institute for Management and Development, and Singapore University for Technology and Design. "2020 Smart City Index." https://www.imd.org/globalassets/wcc/docs/smart_city/smartcityindex_2020.pdf

Isaak, Adam. "Employee tracking is increasingly widespread, and it could be doing more harm than good." *CNBC*, June 2020. https://www.cnbc.com/2020/06/17/employee-surveillance-software-is-seeing-a-spike-as-workers-stay-home.html

ITU, "Measuring the Information Society Report 2018." Volume 1. https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf

Jabil. "Smart Home Trends: What's Now and What's Next?" https://www.jabil.com/blog/connected-home-and-building-tech-trends.html

Johnson, Debora, and Priscilla Regan. "Introduction." In *Transparency and Surveillance as Sociotechnical Accountability: A House of Mirrors*. Abingdon: Routledge, 2014. PDF version

Jolly, David. "Germany Plans Limits on Facebook Use in Hiring." *New York Times*, August 2010. https://www.nytimes.com/2010/08/26/business/global/26fbook.html

Jürgens, Ulrich, Thomas Malsch, and Knuth Dohse. *Breaking From Taylorism: Changing Forms of Work in the Automobile Industry*. Cambridge: Cambridge University Press, 1993. PDF version.

Kakar, Sudhir, *Frederick Taylor: A Study in Personality and Innovation*. Livonics Infotech, 2018. PDF version.

Kanigel, Robert. *The One Best Way: Frederick Winslow Taylor and the Enigma of Efficiency*. New York: Viking, 1997. PDF version.

Kanigel, Robert. "Taylor-Made: How the World's First Efficiency Expert Refashioned Modern Life in His Own Image." *The Sciences* 37, no. 3 (1997): 1-5 http://www.ams.sunysb.edu/~weinig/Taylor-made.pdf

Karvonen, Andrew, Fredrico Cugurullo, Frederico Caprotti, ed. *Inside Smart Cities: Place, Politics and Urban Innovation*. London: Routledge, 2019. PDF version.

Kawakami, Takashi, and Taisei Hoyama. "Trump's blacklist squeezes 200 Chinese companies as net widens: Huawei receives another reprieve while list ensnares AI startups." *NikkeiAsia*, November 2019. https://asia.nikkei.com/Economy/Trade-war/Trump-s-blacklist-squeezes-200-Chinese-companies-as-net-widens

Kendall-Taylor, Andrea, Erica Frantz, and Joseph Wright. "The Digital Dictators: How Technology Strengthens Autocracy." *Foreign Affairs* 99, no. 2 (2020): 103-115. https://www.foreignaffairs.com/system/files/pdf/articles/2020/99210.pdf

Kitchin, Rob. *The Data Revolution*. London: Sage, 2018. PDF version.

Kissinger, Henry, Daniel Huttenlocher, and Eric Schmidt. *The Age of AI: And Our Human Future*. Little, Brown, and Company, 2021. Kindle edition. 205 pages

Kremlin, "Artificial Intelligence Conference," http://en.kremlin.ru/events/president/news/64545

Kremlin. "On the development of artificial intelligence in the Russian Federation." http://www.kremlin.ru/acts/bank/44731/page/1

Kunzmann, Klaus R. "Smart Cities After COVID-19: Ten Narratives." *disP – The Planning Review* 56, no. 2 (2020): 20-31 https://www.tandfonline.com/doi/full/10.1080/02513625.2020.1794120

Laney, Doug. "3D Data Management: Controlling Data Volume, Velocity, and Variety." *Meta Group*, February 2001. https://toaz.info/doc-viewer

Lauer, Josh. "Surveillance history and the history of new media: An evidential paradigm." *New Media Society* 4, no. 14 (2012): 566-582.

Lee, Dave. “Amazon to roll out tools to monitor factory workers and machines.” *Financial Times*, December 2020. https://www.ft.com/content/58bdc9cd-18cc-44f6-bc9b-8ca4ac598fc8

Lin, Liza. “China’s Plan to Make Permanent Health Tracking on Smartphones Stirs Concern.” *The Wall Street Journal*, May 2020. https://www.wsj.com/articles/chinas-plan-to-make-permanent-health-tracking-on-smartphones-stirs-concern-11590422497

Lisboa Inteligente. “Plataforma de Gestão Inteligente de Lisboa.” https://lisboainteligente.cm-lisboa.pt/lxi-iniciativas/plataforma-de-gestao-inteligente-de-lisboa/

Lyon, David. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press, 1994. PDF version.

Lyon David, ed. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge, 2003. PDF version.

Lyon, David. *Surveillance Studies: An Overview*. Cambridge: Polity Press, 2017. PDF version.

Lyon, David, ed. *Theorizing Surveillance: The Panopticon and Beyond*. Exitor: William Publishing, 2006. PDF version.

Lynch, Jennifer. “Government Uses Social Networking Sites for More than Investigations.” *Electronic Frontier Foundation*, August 2010. https://www.eff.org/deeplinks/2010/08/government-monitors-much-more-social-networks

Maalsen, Sophia, and Jathan Sadowski. “The Smart Home on FIRE: Amplifying and Accelerating Domestic Surveillance.” *Surveillance & Society* 17, no. 1/2 (2019): 118-124. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/12925/8484

Maalsen, Sophia, and Robyn Dowling. “Covid-19 and the accelerating smart home.” *Big Data & Society* 7, no. 2 (2020): 1-5. https://journals.sagepub.com/doi/pdf/10.1177/2053951720938073

Maltha, Joost. “Philips launches national portal for digital exchange of COVID-19 patient data in the Netherlands.” *Phillips*, April 2020. https://www.philips.com/a-w/about/news/archive/standard/news/articles/2020/20200415-philips-launches-national-portal-for-digital-exchange-of-covid-19-patient-data-in-the-netherlands.html

Manokha, Ivan. “New Means of Workplace Surveillance.” *Monthly Review*, February 2019. https://monthlyreview.org/2019/02/01/new-means-of-workplace-surveillance/

Manuel, Anja. “US, Europe and UK must unite to keep Chinese tech at bay: Great Powers always triumph thanks to their technological edge. Today is no different.” *Financial Times*, October 2020. https://www.ft.com/content/bc7abf86-f13e-4025-a120-004361aef21a

Marx, Gary T. *Undercover: Police Surveillance in America*. Berkeley: University of California Press, 1988. PDF version.

Mayer-Schonberger, Viktor, and Kenneth Cukier. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. London: John Murray, 2013. PDF version.

Mcconaughey, Woody. “Unjustified parking fines by scan cars.” *Netherlandsnewslive*, May 2021. https://netherlandsnewslive.com/unjustified-parking-fines-by-scan-cars-dailyauto-nl/164745/

Merriam-Webster. “Definition of Internet of Things.” https://www.merriam-webster.com/dictionary/Internet%20of%20Things

Merriam-Webster. “Cloud Computing.” https://www.merriam-webster.com/dictionary/cloud%20computing

MIT Technology Review. “What is Machine Learning?” https://www.technologyreview.com/2018/11/17/103781/what-is-machine-learning-we-drew-you-another-flowchart/

MIT Technology Review. “Artificial Intelligence.” https://www.technologyreview.com/topic/artificial-intelligence/

Monahan, Torin, and David Murakami Wood, ed. *Surveillance Studies: A Reader*. New York: Oxford University Press, 2018. PDF version.

Mosendz, Polly, and Anders Melin. “Bosses Panic-Buy Spy Software to Keep Tabs on Remote Workers.” *Bloomberg*, March 2020. https://www.bloomberg.com/news/features/2020-03-27/bosses-panic-buy-spy-software-to-keep-tabs-on-remote-workers

Murakami Wood, David. “Editorial: Foucault and Panopticism Revisited.” *Surveillance & Society* 1, No.3 (2003): 234-239. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3338/3300

NEC Corporation. “NEC’s intelligent management platform makes Lisbon smarter.” *Asmag*, October 2019. https://www.asmag.com/showpost/30622.aspx

Neff, Gina, and Dawn Nafus. *Self-Tracking*. Massachusetts: The MIT Press, 2016. PDF version.

Netlingo. “Smart Tech.” https://www.netlingo.com/word/smart-tech.php

NIST, “NIST Evaluation Shows Advance in Face Recognition Software’s Capabilities.” https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities

O’Connor, Sarah. “Workplace surveillance may hurt us more than it helps.” *Financial Times*, January 2021. https://www.ft.com/content/27faa953-1723-4597-a5a0-2ff9e617feab

PeoplePublicRecords. http://www.peoplepublicrecords.org/

Pollard, Martin. “Even mask-wearers can be ID’d, China facial recognition firm says.” *Reuters*, March 2020. https://www.reuters.com/article/us-health-coronavirus-facial-recognition-idUSKBN20W0WL

“Phuket governor says island needs 1,500 additional CCTV cameras.” *The Phuket News*, June 2017. https://www.thephuketnews.com/phuket-governor-says-island-needs-1-500-additional-cctv-cameras-62769.php

Repucci, Sarah, and Amy Slipowitz. “Freedom in the World 2021: Democracy under Siege.” *Freedom House*. https://freedomhouse.org/report/freedom-world/2021/democracy-under-siege

Richardson, Michael. “‘Pandemic drones’: useful for enforcing social distancing, or for creating a police state?” *The Conversation*, March 2020. https://theconversation.com/pandemic-drones-useful-for-enforcing-social-distancing-or-for-creating-a-police-state-134667

Rio Prefeitura. “Centro de Controle Operacional (CCO).” https://www.rio.rj.gov.br/web/gmrio/centro-de-controle-operacional

Rosenblat, Alex, Tamara Kneese, and Danah Boyd. “Workplace Surveillance.” *Open Society Foundations Future of Work Commissioned Research Papers*. New York: Data & Society Research Institute, 2014. https://datasociety.net/wp-content/uploads/2014/10/WorkplaceSurveillance.pdf

Rtl News. “‘Dutch corona app will be tested in June.’” https://www.rtlnieuws.nl/tech/artikel/5135056/ontwerp-corona-app-nederland-design-github

Sachs, Jeffrey D. *The Ages of Globalization*. New York: Columbia University Press, 2020. PDF version.

Satariano, Adam. ““How My Boss Monitors Me While I Work From Home.” *The New York Times*, May 2020. https://www.nytimes.com/2020/05/06/technology/employee-monitoring-work-from-home-virus.html

Saval, Nikil. *Cubed: A Secret History of the Workplace*. New York: Doubleday, 2014. PDF version.

Schofield, Philip. *Utility and Democracy: The Political Thought of Jeremy Bentham*. New York: Oxford University Press, 2006. PDF version.

Schofield, Philip. *Bentham: A Guide for the Perplexed*. London: Continuum, 2009. PDF version.

Schreiner, Clara. "International Case Studies of Smart Cities – Rio de Janeiro, Brazil." *Inter-American Development Bank*, 2016. https://publications.iadb.org/publications/english/document/International-Case-Studies-of-Smart-Cities-Rio-de-Janeiro-Brazil.pdf

Shen, Olivia. "Coronavirus and Techno-Authoritarianism." *The China Story*, May 2020. https://www.thechinastory.org/coronavirus-and-techno-authoritarianism/

Sentry. "More than parental control." https://sntry.io/

Semple, Janet. *Bentham's Prison*. Oxford: Clarendon Press, 2003. PDF version

Semple, Janet. "Bentham's Haunted House." In *The Bentham Newsletter*, No. 11 (1987): 35-45. https://www.ucl.ac.uk/bentham-project/sites/bentham-project/files/newsletter_11.pdf

SIPRI. "Military Expenditure Database." https://www.sipri.org/databases/milex

Shahbaz, Adrian, and Allie Funk. "Freedom on the Net 2019 Key Finding: Governments harness big data for social media surveillance." *Freedom House*, 2019.

https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance

Shi-Kupfer, Kristin, Mareike OHlberg Simon Lang, and Bertram Lang. "Ideas and Ideologies Competing for China's Political Future." *Mercator Institute for China Studies*, October 2017. PDF version. https://merics.org/sites/default/files/2020-04/171004_MPOC_05_Ideologies_0_web_1.pdf

Spokeo. "Know More." https://www.spokeo.com/

Smart Nation Singapore. "Singapore's Technology Driven Response To The Pandemic." https://www.smartnation.gov.sg/whats-new/combating-covid-19-with-technology#suite3

Sonn, Jung Won, and Jae Kwang Lee. "The smart city as time-space cartographer in COVID-19 control: The South Korean strategy and democratic control of surveillance technology." *Eurasian Geography and Economics* 61, no. 4-5 (2020): 1-11. https://www.tandfonline.com/doi/full/10.1080/15387216.2020.1768423

Statista. "Smart home market size." https://www.statista.com/statistics/682204/global-smart-home-market-size/

SterlingBackcheck, https://www.sterlingbackcheck.ca/

Szewcow, Barbara, and Jonathan Andrews. "Kuala Lumpur to build 'City Brain' with Alibaba Cloud." *ITU*, February 2018. https://www.itu.int/en/myitu/News/2020/04/07/13/14/Kuala-Lumpur-to-build-City-Brain-with-Alibaba-Cloud

Taksa, Lucy. “Scientific Management.” In *The Oxford Handbook of Management*, ed. Wilkinson, Armstrong, and Lounsbury. Oxford: Oxford University Press, 2017. https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780198708612.001.0001/oxfordhb-9780198708612

Taylor, Frederick Winslow. *The Principles of Scientific Management*. New York: Harper & Brothers, 1919. PDF version.

Techcrunch. “New Xiaomi survey explores how Covid-19 is driving the new smart home, and what it means for 2021 and beyond.” https://techcrunch.com/sponsor/xiaomi/new-xiaomi-survey-explores-how-covid-19-is-driving-the-new-smart-home-and-what-it-means-for-2021-and-beyond/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJowKP7QJ9qpPUe0BT_EDTcff79tc1AKtGO-S9I_HSspOfTWSy2i4QwDN2i_l8InptdEIK6tYjqaxsT-r-JR2A0KbhcEl67-8u-mxRdYkmQ7fCcsLcPo6irz1M4WXJ74DIEjxbPTAyeUvez2ESN10V7tfW4fWX3lxC112wLR6kYt

Teramind. “Remote Employee Monitoring.” https://www.teramind.co/solutions/remote-employee-monitoring

Tiezzi, Shannon. “Sweden Becomes Latest – and Among Most Forceful – to Ban Huawei From 5G.” *The Diplomat*, October 2020. https://thediplomat.com/2020/10/sweden-becomes-latest-and-among-most-forceful-to-ban-huawei-from-5g/

Toli, Angeliki Maria, and Niamh Murtagh. “The Concept of Sustainability in Smart City Definitions.” *Frontiers in Built Environment,* June 2020. https://www.frontiersin.org/articles/10.3389/fbuil.2020.00077/full

Trottier, Daniel. *Social Media as Surveillance: Rethinking Visibility in a Converging World*. Farnham: Ashgate, 2012. EPUB version.

Trumpwhitehouse. “Artificial Intelligence for the American People.” https://trumpwhitehouse.archives.gov/ai/

US Department of Health and Human Services. “Social Listening and Monitoring Tools.” *Centers for Disease Control and Prevention*, 2021. https://www.cdc.gov/vaccines/covid-19/vaccinate-with-confidence/rca-guide/downloads/CDC_RCA_Guide_2021_Tools_AppendixE_SocialListening-Monitoring-Tools-508.pdf

Vaan Teeffelen, Kristel. “Drones check whether you comply with the corona rules, but is that actually allowed?” *Trouw*, April 2020. https://www.trouw.nl/nieuws/drones-controleren-of-u-zich-aan-de-coronaregels-houdt-maar-mag-dat-eigenlijk-wel~b3e551a4/

Various Authors. “Yuval Harari, Elif Shafak, Dambisa Moyo, Eric Schmidt & Others: How COVID Will Change Us.” *Noema*, June 2020. https://www.noemamag.com/yuval-harari-elif-shafak-dambisa-moyo-eric-schmidt-how-covid-will-change-us/

Venkataramakrishnan, Siddharth. “Algorithms and the coronavirus pandemic.” *Financial Times*, January 2021. https://www.ft.com/content/16f4ded0-e86b-4f77-8b05-67d555838941

Wartzman, Rick. “Workplace tracking is growing fast: most worker don’t seem very concerned.” *Fast Company*, March 2019. https://www.fastcompany.com/90318167/workplace-tracking-is-growing-fast-most-workers-dont-seem-very-concerned

Westin, Alan. *Privacy and Freedom*. New York: Ig Publishing, 1967. PDF version.

Xiao, Bo. “How Alexa Can Use Song-Playback Duration to Learn Customers’ Preferences.” *Amazon Science* (blog), July 2018. https://www.amazon.science/blog/how-alexa-can-use-song-playback-duration-to-learn-customers-preferences

Zikopoulos, Paul, Chris Eaton, Dirk Deroos, Tom Deutsch, and George Lapis. *Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data*. New York: McGraw Hill, 2012. PDF version.

Zhang, Daniel, Suarabh Mishara, Eirk Brynjolfsson, John Etchemendy, Deep Ganguli, Barbara Grosz, Terah Lyons, James Manyika, Juan Carlos Niebles, Michael Sellitto, Yoav Shoham, Jack Clark, and Raymond Perrault. “The AI Index 2021 Annual Report.” AI Index Steering Committee, Human Centered AI Institute, Stanford University. March 2021. https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report_Master.pdf

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019. PDF version.

Zuboff, Shoshana. *In the Age of the Smart Machine: The Future of Work and Power*. New York: Basic Books, 1988. PDF version.

Zuboff, Shoshana. “Big Other: surveillance capitalism and the prospects of an information civilization.” *Journal of Information and Technology* 30 (2015): 75-89. https://cryptome.org/2015/07/big-other.pdf

9 News Australia. “Woman caught breaching home isolation.” *Youtube*. Video File. August 18, 2021. https://www.youtube.com/watch?v=3yuTrgR30eg