

2023

## Surveillance Normalization

Christian Sundquist

University of Pittsburgh School of Law, [sundquist@pitt.edu](mailto:sundquist@pitt.edu)

Follow this and additional works at: [https://scholarship.law.pitt.edu/fac\\_articles](https://scholarship.law.pitt.edu/fac_articles)



Part of the [Civil Rights and Discrimination Commons](#), [Constitutional Law Commons](#), [Criminal Law Commons](#), [Health Law and Policy Commons](#), [Health Policy Commons](#), [Inequality and Stratification Commons](#), [Law and Race Commons](#), [Law and Society Commons](#), [Law Enforcement and Corrections Commons](#), [Medicine and Health Commons](#), and the [Public Policy Commons](#)

---

### Recommended Citation

Christian Sundquist, *Surveillance Normalization*, 58 *Harvard Civil Rights-Civil Liberties Law Review* 117 (2023).

Available at: [https://scholarship.law.pitt.edu/fac\\_articles/577](https://scholarship.law.pitt.edu/fac_articles/577)

This Article is brought to you for free and open access by the Faculty Publications at Scholarship@PITT LAW. It has been accepted for inclusion in Articles by an authorized administrator of Scholarship@PITT LAW. For more information, please contact [leers@pitt.edu](mailto:leers@pitt.edu), [shephard@pitt.edu](mailto:shephard@pitt.edu).

# Surveillance Normalization

---

*Christian Powell Sundquist*<sup>1</sup>

## ABSTRACT

*Since the start of the COVID-19 pandemic, the government has expanded public surveillance measures in an attempt to combat the spread of the virus. As the pandemic wears on, racialized communities and other marginalized groups are disproportionately affected by this increased level of surveillance. This article argues that increases in public surveillance as a result of the COVID-19 pandemic give rise to the normalization of surveillance in day-to-day life, with serious consequences for racialized communities and other marginalized groups. This article explores the legal and regulatory effects of surveillance normalization, as well as how to protect civil rights and liberties in the face of such expansion.*

## TABLE OF CONTENTS

INTRODUCTION .....	118
I. THE FUNCTION OF SURVEILLANCE .....	118
A. <i>Surveillance and the Law</i> .....	119
B. <i>The Stages of Surveillance: Punishment, Discipline, and Control</i> .....	126
C. <i>Racializing Surveillance</i> .....	131
II. SURVEILLANCE NORMALIZATION .....	134
CONCLUSION .....	141

## INTRODUCTION

The expansion of health surveillance measures in response to the COVID-19 pandemic has created the conditions necessary for increased public acceptance of mass governmental surveillance, with racialized persons disparately impacted. Crises, such as the COVID-19 pandemic, often facilitate reactionary governmental measures informed by subtle racial heuristics that further entrench social inequality. In particular, crises create situations in which norms of egalitarianism are opaque and where the socially desirable response is not clearly defined, thereby encouraging the expression of racism in ways that seem natural and non-biased. The racialization of crisis therefore functions to stabilize civil society by legitimizing the control of marginalized groups for the supposed greater public

---

<sup>1</sup> Professor of Law, University of Pittsburgh, School of Law

good, while mediating the normative tension between universal equality and the persistence of socio-economic inequality.

The impact of the significant expansion of surveillance tools to control the spread of COVID-19 has disproportionately fallen upon racialized communities and other marginalized groups. As we approach the third year of the pandemic, it is increasingly likely that society has (or will become) accustomed to public health surveillance measures as a minimal price to pay for maintaining the general health of the populace—notwithstanding that most information gleaned from such surveillance (such as health and genetic data, movement and location tracking, and so forth) has little legal safeguards to prevent it from being sold to private companies or misused in the immigration and criminal justice contexts.<sup>2</sup>

The erosion of expectations of privacy in public health following the emergence of the COVID-19 pandemic may also lead to the normalization of public surveillance writ large—most notably with respect to the already unequal police surveillance of racialized communities. There is, in other words, a strong prospect for surveillance creep in ways that will further increase racial disparities along a number of social metrics (such as health, incarceration, and access to public aid).

This Article examines the looming normalization of surveillance in everyday life as society becomes increasingly accustomed to COVID-19 protocols, controls, and testing. Relying on empirical findings from psychological studies, it argues that the public is at significant risk of becoming habituated, and even favorably disposed, to governmental surveillance in non-health related contexts as a result of the unprecedented expansion of surveillance technologies to control the spread of COVID-19. The possible normalization of state surveillance comes with dire implications for racialized communities, who are already subjected to disparate criminal surveillance that leads to disproportionately higher rates of arrest and incarceration. This Article will explore the legal and regulatory ramifications of surveillance normalization, while suggesting privacy reforms to better protect our civil rights and liberties.

## I. THE FUNCTION OF SURVEILLANCE

Our lives are increasingly subject to unprecedented levels of digital surveillance as technology rapidly evolves in the absence of meaningful privacy regulation. The United States' lack of a coherent omnibus approach to privacy protections<sup>3</sup> has rendered privacy rights unstable and the legality of private or public surveillance of individuals and groups unpredictable. The vagaries of surveillance law are also influenced by often shifting social

---

<sup>2</sup> See *infra* Part I for a detailed discussion of American privacy law.

<sup>3</sup> See Rebecca Lipman, *Online Privacy and the Invisible Market for our Data*, 120 PENN. ST. L. REV. 777, 787-89 (2016) (noting the lack of omnibus approach to U.S. privacy laws and how this has given rise to private entities taking steps to regulate data privacy).

norms concerning the appropriateness of certain types of behavior and which privacy rights should be protected by the power of the state.<sup>4</sup>

The heart of modern American privacy law, after all, involves an assessment of the objective and subjective reasonableness of an individual's assertion of a "right to be let alone" in light of cultural mores.<sup>5</sup> Privacy law thus assumes that the denizenry has voluntarily consented to certain intrusions of privacy, while relying on the touchstone of reasonableness in demarcating the spheres of activity that are protected from observation by law. Given that judicial examinations of reasonableness are often influenced by bias and political expediency,<sup>6</sup> certain marginalized communities (in particular, political dissidents and racial and religious minorities) have long been subjected to disproportionate surveillance.<sup>7</sup>

### A. *Surveillance and the Law*

The law of surveillance in the United States has developed in a hodgepodge fashion over time and is embodied in judicial interpretations of the First, Fourth, Ninth, and Fourteenth Amendments of the U.S. Constitution, various statutes operating in the criminal justice, national security, health, and consumer contexts, federal and state common law, and human rights theory. The legality of the surveillance of persons in the United States depends on a number of different variables: Is the person(s) being surveilled by a governmental actor or a private individual? Is the surveillance occurring in a "public" or a "private" space? Has the person being surveilled explicitly or implicitly assented to the privacy intrusion? Is the surveillance being conducted by the government as a matter of national security? Does the person have a reasonable expectation of privacy in the activities being surveilled? Is the privacy interest decisional or informational in nature?

The United States lacks a comprehensive omnibus approach to privacy protection, and as such personal information ostensibly collected as part of the fight against COVID-19 has minimal privacy protections under current

---

<sup>4</sup> See, e.g., Daniel Solove, *A Taxonomy of Privacy*, 154 UNIV. PENN. L. REV. 477, 483-84 (2006) (noting that "[p]rivacy cannot be understood independently from society" and that "the need for privacy is a socially created need" [quoting Barrington Moore, Jr., *PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY* 73 (1984)]).

<sup>5</sup> Victoria Schwartz, *Leveling Up to a Reasonable Woman's Expectation of Privacy*, 93 UNIV. COLORADO L. REV. 115, 130 (2022) (observing that American courts "continue to evaluate reasonableness throughout privacy law by considering the social privacy norms that exist in society").

<sup>6</sup> See Asha Amin, *Implicit Bias in the Courtroom and the Need for Reform*, 30 GEO. J. LEGAL ETHICS 575, 575 (2017) (emphasizing the "two possible sources for a judge's disparate treatment of different parties: explicit bias and implicit bias").

<sup>7</sup> Chaz Arnett, *Race, Surveillance, Resistance*, 81 OHIO ST. L.J. 1103, 1111 (2020) (noting the history of disproportionate levels of surveillance experienced by racial minorities); Katelyn Ringrose, *Religious Profiling: When Government Surveillance Violates the First and Fourth Amendments*, 2019 U. ILL. L. REV. ONLINE 1, 1 (2019) (noting that "government surveillance has a long history in the United States, consistently intertwined within the political landscape, with a deep and disparate impact on religious minorities").

federal statutory law. The Health Insurance Portability and Accountability Act (“HIPPA”) safeguards a narrow range of personal health information, and yet is limited in protecting against COVID-19 related privacy violations in that HIPPA lacks a private right of action, is applicable only to certain covered entities and their business associates, and is riddled with public purpose exceptions.<sup>8</sup> The protections provided by the 21st Century Cures Act and the Genetic Information Non-Disclosure Act are similarly limited in scope in that they are inapplicable to most types of personal health information collected during the pandemic.<sup>9</sup>

A pending bill, The American Data Privacy and Protection Act (“ADPPA”), does expand privacy rights in its attempt to “create a comprehensive federal consumer privacy framework.”<sup>10</sup> The bill would apply to private entities that are not subject to HIPAA that nonetheless “collect, process, or transfer ‘covered data’” such as “information that identifies or is linked or reasonably linkable. . . to an individual” and “any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare treatment of an individual.”<sup>11</sup> If enacted into law, ADPPA would provide meaningful privacy protections for COVID-19 related health data—such as information collected from cell phones and wearable technology. ADPPA also has the potential to shape social expectations related to the disclosure of health information by introducing foundational privacy norms (such as “affirmative express consent,” data minimization, and transparency) to the general public.<sup>12</sup> Nonetheless, ADPPA is limited to consumer privacy issues and thus does not apply to HIPPA-covered entities that collect and process similar health data.<sup>13</sup> Of particular note, ADPPA would not apply to individuals “acting in a non-commercial context” (such as governmental entities), employee or publicly available information, or to de-identified data.<sup>14</sup> Legislation has recently been introduced in the Senate that would fill some of the gaps in ADPPA and HIPPA protections by banning data brokers from commodifying personal health and location data, and yet it remains unclear whether our fractured Congress will pass either bill.<sup>15</sup>

---

<sup>8</sup> See Jennifer D. Oliva, *Surveillance, Privacy, and App Tracking, in COVID-19 POLICY PLAYBOOK: LEGAL RECOMMENDATIONS FOR A SAFER, MORE EQUITABLE FUTURE*, 41 (Scott Buriss et al. eds., 2021) (providing a general overview of American privacy law and how it relates to COVID-19 data).

<sup>9</sup> The Genetic Information Non-Disclosure Act provides that health insurance plans and employers cannot discriminate against employees based on genetic information (122 Stat. 881), while the 21st Century Cures Act provides limited privacy protections to research subjects (130 Stat. 1033).

<sup>10</sup> H.R. 8152.

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> *Id.*

<sup>14</sup> *Id.* at §§ 2, 8-9.

<sup>15</sup> The Health and Location Data Privacy Act bill was introduced June 15, 2022 by Senators Warren, Wyden, Whitehouse, Sanders, and Murray. S. 4408, 117th Cong. (2022).

Privacy rights are also not immediately apparent from the text of the United States Constitution. The Constitution includes no amendment or other textually explicit provision that ensures an individual's right to be free from unwanted observation or surveillance. The First Amendment of the United States Constitution certainly does protect "freedom of speech [and of] the press," and creates enforceable rights of "the people peaceably to assemble" and thus a right to freedom of association.<sup>16</sup> And yet the First Amendment does not clearly articulate a broad individual right to privacy.

The Fourth Amendment more directly speaks to possible rights sounding in privacy in that it creates a "right of the people to be secure in their persons houses, papers, and effects, against unreasonable searches and seizures."<sup>17</sup> While this right only applies to privacy invasions by governmental actors, it nonetheless places important limitations on the ability of local, state, and federal governments to conduct surveillance on individuals and groups of people.<sup>18</sup> The meaning of a Fourth Amendment right to be secure in one's "houses, papers, and effects," however, is notoriously unpredictable<sup>19</sup> and the contours of the right have not kept pace with modern technological innovations.<sup>20</sup> Justice Brandeis, who first articulated the possibility of a legal right "to be let alone" in his co-authored law review article in 1890, planted the seeds for a reading of the Fourth Amendment that allows for individual privacy rights in his dissent to the *Olmstead v. United States* (1928) decision.<sup>21</sup> The *Olmstead* case presented a novel question to the Supreme Court: does the Fourth Amendment protect against governmental eavesdropping on (ostensibly private) telephone conversations when the wiretaps were applied to phone lines outside of the individual's house? The majority applied a textualist interpretation of the Fourth Amendment in finding that it only protected against unreasonable trespasses within a person's private house, papers, or effects, and thus did not create any privacy rights (which the majority framed as "property" rights) beyond the four walls of

---

<sup>16</sup> U.S. CONST. amend. I; *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958) (recognizing that the First Amendment's freedom of assembly included a right to freely associate with others in the exchange of ideas).

<sup>17</sup> U.S. CONST. amend. IV.

<sup>18</sup> See Grace Egger, *Ring, Amazon Calling: The State Action Doctrine & the Fourth Amendment*, 95 WASH. L. REV. ONLINE 245, 247 (2020) (emphasizing that "the Fourth Amendment usually provides strong protection for private individuals against intrusions by state actors because it requires state actors to gain consent, obtain a warrant, or have probable cause in order to access private property or track citizens.").

<sup>19</sup> See Kaitlin D. Corey, *How Far Will the Third Party Doctrine Extend?*, 51 MD. B. J. 14, 15 (2018) (emphasizing that as technology develops, "searches. . . are becoming much more complex than simply searching a person's physical property.")

<sup>20</sup> See Russell L. Weaver, *The Fourth Amendment, Privacy and Advancing Technology*, 80 MISS. L.J. 1131, 1137 (2011) (emphasizing that "while the Fourth Amendment has been interpreted to provide citizens with some protection against modern technology, early United States Supreme Court decisions dealing with technology and the Fourth Amendment tended to adhere to more traditional views of the Fourth Amendment and were virtually unresponsive (except in the dissents) to the problems presented by new technologies.").

<sup>21</sup> 277 U.S. 438, 471 (1928).

one's home.<sup>22</sup> Justice Brandeis, in dissent, argued against such rigid formalism in light of technological advancements (such as wiretapping) that broadened the threat to individual privacy, presciently noting that:

The progress in science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.<sup>23</sup>

Nearly four decades later, the Supreme Court came to embrace Justice Brandeis' conception of the Fourth Amendment in its seminal decision *Katz v. United States*.<sup>24</sup> The *Katz* court found that the warrantless eavesdropping upon a criminal suspect's telephone conversations via electronic listening devices violated the Fourth Amendment.<sup>25</sup> In so doing, the Court rejected the rigid formalism of textualism while reaching the common-sense conclusion that the Fourth Amendment "protects people, not places."<sup>26</sup> The analytical framework advanced by Justice Harlan's concurrence has come to define Fourth Amendment privacy law, providing that Fourth Amendment protections apply when "first, . . . a person 'exhibit[s] an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"<sup>27</sup> The *Katz* court nonetheless recognized the limits of using the Fourth Amendment as a vehicle to protect privacy, concluding that "the Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'"<sup>28</sup> The *Katz* court thus re-framed the Fourth Amendment analysis as concerning the subjective and objective privacy expectations of the persons being surveilled, as opposed to the strict physical trespass doctrine applied by *Olmstead* and earlier decisions.<sup>29</sup> The Supreme Court relied on the constitutional principles advanced by *Katz* in

---

<sup>22</sup> *Id.* at 465-66. See also *Lopez v. United States*, 373 U.S. 427, 440 (1995) (applying similar reasoning to hold that there was no actionable "search" within the meaning of the Fourth Amendment when the Internal Revenue Service wiretapped the defendant, since there was no "physical invasion").

<sup>23</sup> *Olmstead*, 277 U.S. at 465-66.

<sup>24</sup> 389 U.S. 347 (1967).

<sup>25</sup> *Id.* at 359.

<sup>26</sup> *Id.* at 351.

<sup>27</sup> *Id.* at 362. Justice Harlan's concurrence also gave rise to the modern "plain view" doctrine, which provides that statements a person "exposes to the 'plain view' of outsiders are not 'protected,' because no intention to keep them to himself [sic.] has been exhibited." *Id.*

<sup>28</sup> *Id.* at 350 (noting that while the Fourth Amendment "protects individual privacy against certain kinds of governmental invasion" (emphasis added), "its protections go further, and often have nothing to do with privacy at all.")

<sup>29</sup> See *Olmstead v. United States*, 277 U.S. 438, 466 (1928); *Goldman v. United States*, 316 U.S. 129, 134-36 (1942). The *Katz* privacy framework has since been interpreted by the Supreme Court in a number of varying (and at times, conflicting) ways. .

recognizing that individuals have a reasonable expectation of privacy in personal health data under the Fourth Amendment.<sup>30</sup>

The language of the Ninth and Fourteenth Amendments similarly do not *directly* address specific privacy rights. Whereas the Fourteenth Amendment provides for certain “due process” and “equal protection” rights,<sup>31</sup> the Ninth Amendment simply states that “[t]he enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.”<sup>32</sup> It was against this backdrop of unenumerated privacy rights that the Supreme Court first recognized a general constitutional right to privacy in its landmark 1965 decision in *Griswold v. Connecticut*.<sup>33</sup> The *Griswold* court recognized a privacy right for couples to use contraception in the privacy of their own home,<sup>34</sup> a decision with profound importance for women’s equality.<sup>35</sup> The Court acknowledged that a general right to privacy was not explicit from the text of the Constitution, but nonetheless referenced recent precedent recognizing similar “peripheral” constitutional rights.<sup>36</sup> The *Griswold* court analogized to such cases as examples in which the Supreme Court had recognized unenumerated yet peripheral rights that were necessary to uphold the textual guarantees of the Constitution. Most of these rights were derived from the Court’s reading of the First Amendment,<sup>37</sup> while others had been recognized in order to uphold the protections of the Fourth and Fifth Amendments.<sup>38</sup> The Court reasoned that those cases, as well as the literal terms of the Ninth Amendment (which protect unenumerated rights

<sup>30</sup> See *Ferguson v. City of Charleston*, 532 U.S. 67, 86 (2001) (finding that a hospital violated patients’ reasonable expectations of privacy by disclosing patient test records without consent).

<sup>31</sup> U.S. CONST. amend. XIV. The Fourteenth Amendment also provides that states cannot “make or enforce any law which. . . abridge[s] the privileges or immunities of citizens of the United States.” *Id.*

<sup>32</sup> U.S. CONST. amend. IX.

<sup>33</sup> 381 U.S. 479, 484 (1965).

<sup>34</sup> *Id.* at 486.

<sup>35</sup> Lauren A. DiMartino, *The Procreation Prescription: Sexuality, Power, and the Veil of Morality*, 22 CUNY L. REV. 41, 46-49 (2019).

<sup>36</sup> *Griswold*, 381 U.S. at 482-83.

<sup>37</sup> See, e.g., *Pierce v. Society of Sisters*, 268 U.S. 510, 534-35 (1925) (recognizing the right to educate one’s children as one chooses, the Court found that the challenged statute “unreasonably interferes with the liberty of parents and guardians to direct the upbringing and education of children under their control.”); *Meyer v. Nebraska*, 262 U.S. 390, 403 (1923) (recognizing the right to study the German language in a private school); *Martin v. City of Struthers*, 319 U.S. 141, 157 (1943) (recognizing the right to distribute and receive literature); *Wieman v. Updegraff*, 344 U.S. 183, 191 (1952) (recognizing pedagogical freedom); *NAACP v. Alabama*, 357 U.S. 449, 462 (1958) (recognizing the “freedom to associate and privacy in one’s associations.”).

<sup>38</sup> See *Boyd v. United States*, 116 U.S. 616, 630 (1886) (recognizing a right against governmental intrusions “of the sanctity of a man’s [sic] home and the privacies of life.”); *Mapp v. Ohio*, 367 U.S. 643, 656 (1961) (recognizing the Fourth Amendment as protecting a “right to privacy, no less important than any other right carefully and particularly reserved to the people”); *Accord Breard v. Alexandria*, 341 U.S. 622 (1951); *Public Utilities Comm’n v. Pol-lak*, 343 U.S. 451 (1952); *Monroe v. Pape*, 365 U.S. 167 (1961); *Lanza v. New York*, 370 U.S. 139 (1962); *Frank v. Maryland*, 359 U.S. 360 (1959); *Skinner v. Oklahoma*, 316 U.S. 535 (1942) (recognizing a fundamental right to procreation in striking down a sterilization law).



retained by the people), “suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance.”<sup>39</sup> The Court further found that the guarantees provided by the Bill of Rights “create zones of privacy” that were entitled to constitutional protection.<sup>40</sup> Upon the facts of the case, the *Griswold* majority found that the anti-contraceptive law at issue intrudes upon a “relationship lying within the zone of privacy created by several fundamental constitutional guarantees” and was therefore unconstitutional.<sup>41</sup>

The logic of *Griswold* recognizing broad privacy rights stemming from the Bill of Rights was extended to recognize a Fourteenth Amendment privacy interest in health data,<sup>42</sup> the fundamental constitutional right for a woman to decide whether to continue a pregnancy,<sup>43</sup> the right of both married and unmarried persons to use contraceptives,<sup>44</sup> the right to marry a person of a different “race,”<sup>45</sup> the right to freedom from governmental intrusion in one’s intimate relationships,<sup>46</sup> and the right for same-sex couples to marry.<sup>47</sup> The Supreme Court has also recognized a litany of additional unenumerated

---

<sup>39</sup> *Griswold*, 381 U.S. at 484.

<sup>40</sup> *Id.* at 485 (noting that the foregoing cases “bear witness” to a “right of privacy”).

<sup>41</sup> *Id.* at 485-86. In reaching this conclusion, the Court explained that “We deal with a right of privacy older than the Bill of Rights—older than our political parties, older than our school system. Marriage is a coming together for better or for worse, hopefully enduring, and intimate to the degree of being sacred. It is an association that promotes a way of life, not causes; a harmony in living, not political faiths; a bilateral loyalty, not commercial or social projects.” *Id.* at 486; see also *Eisenstadt v. Baird*, 405 U.S. 438, 453-54 (1972) (extending *Griswold* to uphold the right of unmarried persons to make decisions about contraceptives) (“If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child”).

<sup>42</sup> *Whalen v. Roe*, 429 U.S. 589, 606 (1977).

<sup>43</sup> *Roe v. Wade*, 410 U.S. 113, 153 (1973) (recognizing the right of women to choose whether to end a pregnancy based on “the Fourteenth Amendment’s concept of personal liberty and restrictions upon state action” and “the Ninth Amendment’s reservation of rights to the people.”); see also *Lawrence v. Texas*, 539 U.S. 558, 565 (2003) (noting that *Roe* “recognized the right of a woman to make certain fundamental decisions affecting her destiny.”). *But see Dobbs v. Jackson Women’s Health Org.*, 142 S. Ct. 2228, 2242 (2022) (overruling *Roe v. Wade*).

<sup>44</sup> *Carey v. Population Services, Int’l*, 431 U.S. 678, 689 (1977) (relying on *Griswold* to invalidate a New York law that prohibited the sale of contraceptives to minors); *Eisenstadt v. Baird*, 405 U.S. 438, 453 (1972) (invalidating law that prohibited the distribution of contraceptives to unmarried persons, holding that if “the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child”).

<sup>45</sup> *Loving v. Virginia*, 388 U.S. 1, 11 (1967) (invalidating anti-miscegenation laws as being “odious to a free people whose institutions are founded upon the doctrine of equality” (quoting *Hirabayashi v. United States*, 320 U.S. 81, 100 (1943))).

<sup>46</sup> *Lawrence v. Texas*, 539 U.S. 558, 562 (2003) (finding that under the Fourteenth Amendment “[l]iberty protects the person from unwarranted government intrusions into a dwelling or other private places” in striking down a Texas statute that criminalized same-sex sexual conduct).

<sup>47</sup> *Obergefell v. Hodges*, 576 U.S. 644, 675 (2015) (finding “that the right to marry is a fundamental right inherent in the liberty of the person, and under Due Process and Equal Protection Clauses of the Fourteenth Amendment couples of the same-sex may not be deprived of that right and that liberty.”)

rights based on the need to protect the guarantees of the Bill of Rights, including the rights to desegregated public education,<sup>48</sup> to educate a child in a foreign language,<sup>49</sup> to be free from laws that “shock the conscience,”<sup>50</sup> to not have mental illness criminalized,<sup>51</sup> to be free from excessive punitive damages in civil cases,<sup>52</sup> to have children,<sup>53</sup> to travel freely within the United States,<sup>54</sup> to refuse unwanted medical treatment,<sup>55</sup> to attend and report on criminal trials,<sup>56</sup> to contract,<sup>57</sup> and “to enjoy those privileges long recognized at common law as essential to the orderly pursuit of happiness by free men [sic].”<sup>58</sup>

The recognition of a general right to privacy, as well as that of other unenumerated rights, has been critical to the Supreme Court’s perceived legitimacy by “the people.”<sup>59</sup> And yet these fundamental unenumerated rights—relied upon by generations and often critical to the pursuit of gender, racial, and LGBTQ+ equality—have recently been called into question by the Supreme Court’s 2022 decision in *Dobbs v. Jackson*.<sup>60</sup> The *Dobbs* court overruled the *Roe* and *Casey* decisions that recognized a woman’s right to choose whether to continue with a pregnancy in finding that the “Constitution makes no reference to abortion, and no such right is implicitly protected by any constitutional provision. . .”<sup>61</sup> In so doing, the Court—for the first time in America’s history—invalidated a right previously recognized as fundamental to the Constitution.

The Court reached its decision, in part, through simplistic textualism in noting that “a right to privacy. . . is. . . not [explicitly] mentioned” in the Constitution.<sup>62</sup> It is difficult to overstate the potential consequences of this holding for other unenumerated constitutional rights generally, and for privacy rights in particular. While Justice Samuel Alito noted in the majority opinion that *Dobbs* should not be “understood to cast doubt on precedents

<sup>48</sup> *Brown v. Board of Education*, 347 U.S. 483 (1954) (emphasizing the right to desegregated public education under the Equal Protection Clause of the Fourteenth Amendment).

<sup>49</sup> *Pierce v. Society of Sisters*, 268 U.S. 510, 534 (1925) (citing *Meyer v. Nebraska*, 262 U.S. 390 (1923)).

<sup>50</sup> *Rochin v. California*, 342 U.S. 165, 172 (1952).

<sup>51</sup> *O’Connor v. Donaldson*, 422 U.S. 563, 575 (1975).

<sup>52</sup> *BMW v. Gore*, 517 U.S. 559, 562 (1996).

<sup>53</sup> *Skinner v. Oklahoma*, 316 U.S. 535, 541 (1942).

<sup>54</sup> *Saenz v. Roe*, 526 U.S. 489, 502-04 (1999) (applying the Privileges and Immunities Clause of the U.S. Constitution).

<sup>55</sup> *Cruzan v. Dir. Mo. Dep’t of Health*, 497 U.S. 261, 278 (1990).

<sup>56</sup> *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 580 (1980).

<sup>57</sup> *Meyer v. Nebraska*, 262 U.S. 390, 399 (1923); see also *The Slaughter-House Cases*, 83 US 36, 79 (1872).

<sup>58</sup> *The Slaughter-House Cases*, 83 U.S. at 105.

<sup>59</sup> See, e.g., *Carpenter v. United States*, 138 S.Ct. 2206, 2214 (2018) (emphasizing the expansion of Fourth Amendment protections with advances in technology).

<sup>60</sup> *Dobbs v. Jackson Women’s Health Org.*, 142 S.Ct. 2228 (2022).

<sup>61</sup> *Id.* at 2242.

<sup>62</sup> *Id.* at 2245.

that do not concern abortion,”<sup>63</sup> the majority’s disdain for unenumerated rights, as well as for interpretive doctrines developed under the 5th, 9th, and 14th Amendments, is unmistakably clear.

The crumbling of core democratic values as the result of the far-right extremist ideology that has seized America has made it significantly more likely that the law will continue to be marshalled to eviscerate the privacy rights of marginalized groups—such as women, racialized persons, and the LGBTQ+ community. Justice Clarence Thomas—who joined the majority decision in *Dobbs*—has made it clear that he would like the Supreme Court to actively seek to dismantle the constitutional privacy rights of other marginalized groups:

“In future cases, we should reconsider all of this Court’s substantive due process precedents, including *Griswold* [providing a constitutional right to contraception], *Lawrence* [providing a constitutional right to enter a same-sex relationship], and *Obergefell* [providing a constitutional right for same-sex marriage].”<sup>64</sup>

The nation’s steady move towards anti-majoritarianism and minority rule<sup>65</sup>—as exemplified by the *Dobbs* decision—has created the conditions necessary for the derogation of existing privacy rights while almost certainly subjecting marginalized groups to increased surveillance.<sup>66</sup>

### B. *The Stages of Surveillance: Punishment, Discipline, and Control*

The nature of surveillance can change with the advent of new technologies, new modes of governance, and shifts in the underlying economic system of society.<sup>67</sup> While the underlying focus of surveillance is to simply observe a subject (or subjects) in order to obtain information, the function of “macro surveillance”<sup>68</sup> can similarly shift as societies transition into new socio-political structures.<sup>69</sup> Is the function of surveillance to impose the vio-

<sup>63</sup> *Id.* at 2280.

<sup>64</sup> *Id.* at 2301 (Thomas, J., Concurring) (explanatory material added in brackets).

<sup>65</sup> See, Mara Liasson, *Democrats Increasingly Say American Democracy is Sliding Toward Minority Rule*, NPR (June 9, 2021, 5:00 AM) <https://www.npr.org/2021/06/09/1002593823/how-democratic-is-american-democracy-key-pillars-face-stress-tests> [<https://perma.cc/W77X-7CD7>] (noting the different processes that give rise to anti-majoritarianism and minority rule).

<sup>66</sup> The disparate surveillance of women, racialized minorities, and LGBTQ+ persons will be explored more fully in Part II of this Article.

<sup>67</sup> Masa Galic, Tjerk Timan, & Bert-Jaap Koops, *Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation*, 30 *PHILOSOPHY & TECHNOLOGY* 9, 10 (2016) (providing an overview of prominent theories regarding the function of surveillance).

<sup>68</sup> Vernon Cisney and Nicolae Morar, *BIOPOWER: FOUCAULT AND BEYOND* (eds. Vernon W. Cisney and Nicolae Morar) (2016), at 336.

<sup>69</sup> Khaled Ali Beydoun, *The New State of Surveillance: Societies of Subjugation*, 79 *WASH. & LEE L. REV.*, 769, 784-789 (2022). Professor Beydoun argues that the field of sur-

lence of state power upon physical bodies for violating the law? Or perhaps to discipline subjects that do not follow social norms of behavior? Or to control individuals in order to maintain social and economic hierarchies in a capitalist state? All of the above?

The growing field of surveillance studies posits that the function of mass surveillance is determined by changes to the mode of governance of a society as civilization progresses.<sup>70</sup> The first phase of civilization, according to foundational surveillance philosophers Michel Foucault and Gilles Deleuze, is marked by pre-modern feudal societies organized around principles of sovereignty.<sup>71</sup> The sovereign society thus utilizes surveillance to maintain the power of the “King” and to “affirm control over a territory and secure the loyalty of subjects”<sup>72</sup> through the threat of physical violence and public spectacles of arcane punishment.<sup>73</sup>

The transition of a sovereign society to an early modern democratic society, in which power lies not in the hands of the sovereign but rather is dispersed through various State and non-State institutions, shifts the ends of surveillance to social normation and discipline. Jeremy Bentham’s eighteenth-century conception of the “Panopticon” has been significantly influential to understanding the nature of surveillance in liberal societies.<sup>74</sup> Bentham strove to envision an ideal prison which, by means of an octangular architectural design, would lead prisoners (subjects) to believe that they were being constantly surveilled.<sup>75</sup> The physical and spatial design of the prison as an “enclosed, segmented space” with an invisible—yet omnipresent—overseer was critical to create the illusion among subjects that their “slightest movements are supervised, in which all events are recorded. . . in which power is exercised without division.”<sup>76</sup>

---

veillance studies has failed to account for the dynamics of surveillance in non-Western, non-capitalist societies. He argues, in part, that the purpose of surveillance in an authoritarian society (subjugation) differs from the purpose of surveillance in an ostensibly democratic society committed to capitalism (control). *Id.* at 797.

<sup>70</sup> Galic, Timan & Koops, *supra* note 67, at 10.

<sup>71</sup> See, e.g., MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (1995).

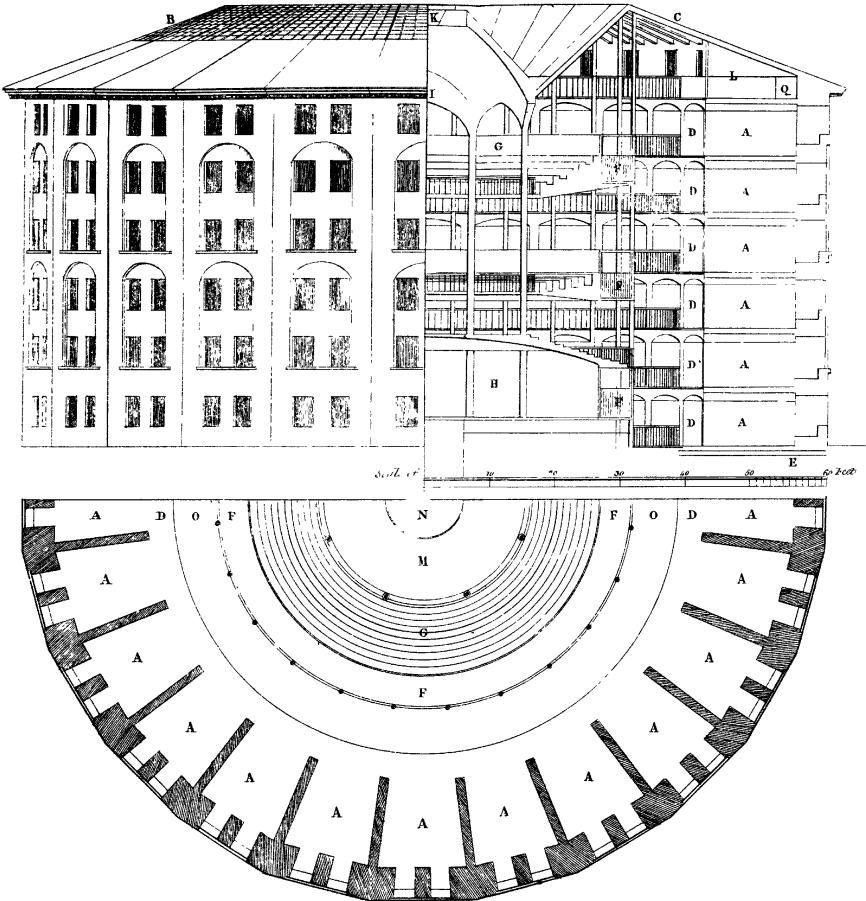
<sup>72</sup> Galic, Timan & Koops, *supra* note 67, at 12.

<sup>73</sup> Beydoun, *supra* note 69, at 784.

<sup>74</sup> Danielle Couch, Paul Komesaroff, and Pricilla Robinson, *COVID-19—Extending Surveillance and the Panopticon*, National Library of Medicine (Aug 25, 2020), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7445799/#:~:text=IN%20this%20manner%20panoptic%20surveillance,all%20aspects%20of%20social%20life,> [https://perma.cc/3MBD].

<sup>75</sup> JEREMY BENTHAM, PANOPTICON (1786); JEREMY BENTHAM, THE INSPECTION-HOUSE (1790-91).

<sup>76</sup> Michel Foucault, “Panopticism” from *Discipline & Punish: The Birth of the Prison*, RACE/ETHNICITY: MULTIDISCIPLINARY GLOBAL CONTEXTS, Vol. 2, No. 1, The Dynamics of Race and Incarceration: Social Integration, Social Welfare, and Social Control, 1, 3 (2008).



The Panopticon thus employs physical and spatial architecture to discipline the subject into believing that perpetual surveillance is inevitable and unavoidable. As such, Bentham and Foucault argued that the subject would be conditioned to self-regulate their behavior to conform with State norms in order to avoid (what appeared to be) certain punishment for infractions. As Professor Khalid Beydoun succinctly describes:

The ubiquitous gaze of the boss, the schoolteacher, the parents, or the prison warden, all of which embody the surveillance state, make the subject perpetually aware that she is being surveilled. This knowledge of being watched. . . had a *disciplining* effect, conditioning the subject to obey state authority without having to dispense of the physical punishment that characterized the previous society of sovereignty.<sup>77</sup>

<sup>77</sup> Beydoun, *supra* note 69, at 785 (emphasis in original). Professor Beydoun further observes that the “coming of the disciplinary society, [Foucauldian] theory holds, rendered pun-

The disciplinary process, according to Foucauldian theory, leads the subject to conform to the norms of behavior deemed acceptable by the State, thus creating a “docile” and law-abiding citizenry.<sup>78</sup> Disciplinary surveillance of this kind therefore focuses on the individual, as opposed to the aggregate, in determining whether social norms have been violated.<sup>79</sup>

Post-panoptical and infrastructural theories of surveillance extend many of the key insights of Foucauldian discourse while analyzing the impact of globalization, capitalism, and new technology on the nature of mass surveillance in modern societies. Contemporary surveillance theory recognizes that surveillance today involves not only surveillance by the State (the primary focus of both sovereign and disciplinary societies), but also mass surveillance conducted by private non-state corporate entities.<sup>80</sup> Indeed, the State is now reliant on the technological advancements of the corporate sector (such as Google, Meta (Facebook and Instagram), and Amazon) for access to vast troves of personal information linked to millions of Americans.<sup>81</sup> Whereas surveillance in the disciplinary societies of yore relied on the observation of individual bodies using physical technologies, surveillance in today’s society “is networked and relies primarily on digital. . . technologies” to analyze the citizen-consumer’s digital representation.<sup>82</sup>

Modern surveillance theory thus views contemporary democratic societies as transitioning from disciplinary societies to “control societies” as the result of global capitalism and significant advancements in surveillance technology (largely cultivated by the private sector). The function of mass surveillance in a control society (such as ours today) is to translate the individual physical body into a digital representation that can be commodified, constantly monitored, and controlled by both corporate and governmental entities.<sup>83</sup>

The COVID-19 pandemic is taking place during such a period of surveillance capitalism, where technology is increasingly embraced for its

---

ishment unnecessary and aberrant” (*Id.* at 785-86) as it “convert[s] the surveilled into its *co-surveillant*, simultaneously serving the master and collaborating in her own confinement.” (*Id.* at 786) (emphasis in original)).

<sup>78</sup> See Galic, Timan & Koops, *supra* note 67, at 14 (“As the body is subjected to discipline, it is ordered, subjected to normation.”).

<sup>79</sup> Cisney & Morar, *supra* note 68, at 4 (noting that under Foucauldian theory the individual body is disciplined “into systems of efficient and economic controls”).

<sup>80</sup> See generally Galic, Timan, & Koops, *supra* note 67, at 16; Beydoun, *supra* note 69, at 787.

<sup>81</sup> Egger, *supra* note 18, at 246-47 (noting that “many are concerned that Amazon has created a surveillance state by partnering with law enforcement agencies and local governments across the United States. . . . As a result, Amazon gains endorsement by government officials and an expansion of its network.”).

<sup>82</sup> Galic, Timan, & Koops, *supra* note 67, at 9.

<sup>83</sup> *Id.* at 18-33. (noting that “with the datafication of society, surveillance combines the physical with the digital, government with corporate surveillance, and top-down with self-surveillance”).

seeming ability to provide solutions to all of the world's problems.<sup>84</sup> Governments across the world have fanned the flames of techno-solutionism in response to the pandemic, working in concert with Big Tech to enmesh daily surveillance as an ordinary, positive, and necessary condition of civic life.<sup>85</sup> As David Lyon observes, "COVID-19 has become a showcase for government agencies and private capital to present their capabilities and control over society as a positive force."<sup>86</sup>

Foucault, and other surveillance scholars, have described how the Plague and other disease outbreaks led to increased systems of social control through "internalized self-surveillance" and "conformity to prescribed norms."<sup>87</sup> Foucault described the "plague-town" as involving permanent surveillance with "everyone ordered to stay indoors. . . a segmented, immobile, frozen space [where] each individual is fixed in his place [and] inspection functions ceaselessly."<sup>88</sup> The bioethicists Danielle Couch, Priscilla Robinson, and Paul Komesaroff provide an excellent framing of the expansion of COVID-19 surveillance in Foucauldian terms:

[I]ts very conspicuousness and its dependence on the active participation of the individuals subject to it guarantees what Foucault referred to as their 'own subjection' enforced through internalized self-surveillance and self-disciplinary practices. The knowledge gleaned from the masses of data and power flowing seamlessly from it generates conformity to prescribed norms and rapidly emerging habitual practices. What had once seemed alien quickly becomes incorporated into the mundane greyness of the everyday.<sup>89</sup>

Surveillance in a control society is much more difficult to constrain by existing law given the enmeshment of private non-state actors in the surveillance of digitized individuals who (often) voluntarily assent to the collection

---

<sup>84</sup> DAVID LYON, PANDEMIC SURVEILLANCE 9 (2022) (noting that the COVID-19 pandemic "was the first to occur in the context of surveillance capitalism" at a moment when many nation-states recognized that "they did not have the capacity to develop technologies deemed 'necessary' for a digital era").

<sup>85</sup> Imran Malek, Divya Ramjee, Pollyanna Sanderson, *COVID-19 and Digital Contact Tracing: Regulating the Future of Public Health Surveillance*, CARDOZO L. REV. DE NOVO 101, 103-104 (2021) (noting that "pressure is mounting to develop epidemiologically-useful digital tools, as states across the United States continue lifting stay-at-home orders and attempt to return to normal operations."). David Lyon argues that "[s]tate and corporate power [now] work together as never before to create the conditions of pandemic surveillance" Lyon, *supra* note 84, at 118.

<sup>86</sup> Lyon, *supra* note 84, at 125 (quoting Professor Baca in part).

<sup>87</sup> Couch, Robinson, & Komesaroff, *supra* note 74.

<sup>88</sup> Michel Foucault, DISCIPLINE & PUNISH: THE BIRTH OF THE PRISON 195 (1995); *see also* Lyon, *supra* note 84, at 54 (describing the implications of Foucault's "plague-town" description to the COVID-19 pandemic).

<sup>89</sup> *See* Foucault, *supra* note 88 at 195.

of private information.<sup>90</sup> The core findings of surveillance theory therefore suggest that mass surveillance in a control (or even, disciplinary) society can quickly become normalized as access to digital information becomes so routinized that it renders privacy norms seemingly obsolete in an advanced technocratic world. One recent empirical examination of the impact of COVID-19 surveillance technology on privacy expectations concluded as much, finding that the routinization of COVID-19 technologies have “foster[ed] people’s resignation to accepting privacy violations as inevitable.”<sup>91</sup> Notwithstanding the benign intentions of many state officials and private corporations to utilize technology to reduce the spread of COVID-19 (e.g., techno-utopianism), it appears as though the widespread use of surveillance technologies—such as COVID-19 tracking apps—are reshaping social expectations of privacy.

### C. Racializing Surveillance

Foundational theories of the “sovereign society,” “disciplinary society,” and “control society” have nonetheless largely ignored the racial dynamics of mass surveillance in the modern state.<sup>92</sup> The colorblind analysis of surveillance by classic surveillance studies (dominated by white men) is perhaps not surprising as “race remains the *dark matter*, the often invisible substance that in many ways structures the universe of modernity.”<sup>93</sup> Given that surveillance is a tool of social control<sup>94</sup> (and at times one of punishment and discipline) and of “social sorting,” a consideration of our history of racial oppression makes it thoroughly clear that, as Professor Beydoun states, “[r]ace is not incidental to surveillance, but rather is built into surveillance technology.”<sup>95</sup>

---

<sup>90</sup> See *Smith v. Maryland*, 442 U.S. 735 (1979) (affirming that an individual does not have a legitimate expectation of privacy regarding information they voluntarily turn over to a third party).

<sup>91</sup> John S. Seberger, Sameer Patil, *Post-COVID Public Health Surveillance and Privacy Expectations in the United States: Scenario-Based Interview Study*, JMIR MHEALTH UHEALTH (2021).

<sup>92</sup> See Markus Kienschferf, *Classifying and Dividing Labor: The Political Economy of Racializing Surveillance*, in TRUST AND TRANSPARENCY IN AN AGE OF SURVEILLANCE 85 (Lora Anne Viola & Pawel Laidler eds., Routledge 2022) (noting that “[s]urveillance studies’s focus on the modern state similarly hides an analysis of the settler colonialist and white supremacist logics of surveillance that precede the ascendancy of the modern state.”) (quoting ethnologist Andrea Smith)); Beydoun, *supra* note 69, at 790-792; SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS 17 (2015) (describing how foundational surveillance theory, and in particular the insights by Michel Foucault and George Orwell, “conceptualized surveillance as integral to modernity, [yet] surveillance ‘has been racialized in a manner they did not foresee. . . .’”).

<sup>93</sup> Howard Winant, *The Dark Matter: Race and Racism in the 21st Century*, 2 CRITICAL SOCIO. 313-324, 322 (2015).

<sup>94</sup> See DAVID LYON, PANDEMIC SURVEILLANCE 13 (2022) (defining “surveillance as a social sorting” to understand the “classifying drive of contemporary surveillance”).

<sup>95</sup> Beydoun, *supra* note 69, at 794.



Technologies of surveillance in America were shaped, in part, by the need to control and maintain the institution of chattel slavery.<sup>96</sup> Chattel slavery introduced expansive and novel forms of mass surveillance of enslaved Black persons as “an exercise of both sovereign power and racialized disciplinary power” that served to secure the economic foundations of America.<sup>97</sup> The sociologist Simone Browne concluded in her seminal work that plantation surveillance was the “earliest form of surveillance practiced in the Americas,”<sup>98</sup> with such surveillance practices continuing in different and evolving forms following the end of chattel slavery.<sup>99</sup>

The surveillance of persons classified as “non-white” by our factitious racial taxonomy not only serves to maintain physical and social boundaries but has a racializing function as well in that it creates and shapes norms that define racial difference and normalize folk notions of race-based inferiority.<sup>100</sup> Browne has provided perhaps the most detailed definition of racializing surveillance as a “technology of social control . . . [which] reif[ies] boundaries, borders, and bodies along racial lines, and where the outcome is often discriminatory treatment of those who are negatively racialized by such surveillance.”<sup>101</sup> The racial biases that are often embedded in new sur-

<sup>96</sup> See BARTON GELLMAN & SAM ADLER-BELL, *THE DISPARATE IMPACT OF SURVEILLANCE*, 6 (2017) (finding that “[s]urveillance in America owes its origins, in part, to the slave economy.”); Browne, *supra* note 92 at 50 (finding that the “historical formation of surveillance is not outside of the historical formation of slavery”).

<sup>97</sup> Browne, *supra* note 92, at 52.

<sup>98</sup> Browne, *supra* note 92, at 52; Kienschferf, *supra* note 92, at 93 (similarly finding that “in the United States. . . it was the colonial regime of slavery that prompted the development of a racial black-white binary and the associated practices of racializing surveillance”); Gellman & Adler-Bell, *supra* note 96, at 6 (“Plantation ledger books served as proto-biometric databases, recording the slaves as physical specimens in fine detail. The slave pass, the slave patrol, and the fugitive slave poster—three pillars of information technology in their day—prefigured modern policing, tracking, and photo ID.”)

<sup>99</sup> See, e.g., Andrew Guthrie Ferguson, *Illuminating Black Data Policing*, 15 Ohio St. J. Crim. L. 503, 517 (2018) (“From the post-slavery patrols, to surveillance of the civil rights movement in the 1960s, to monitoring of the Black Lives Matter movement in this decade, African-Americans have felt the negative impact of police surveillance in pointed and pervasive ways.”); Kienschferf, *supra* note 92, at 96 (finding that “discourses of criminality and welfare dependence are now mobilized for legitimating the disproportionate surveillance of the racialized poor”); Anita L. Allen, *Dismantling the “Black Opticon:” Privacy, Race Equity, and Online Data-Protection Reform*, 131 Yale L.J. F. 907, 917-21 (2022) (discussing the historical and modern over-surveillance of Black persons); Frank Rudy Cooper, *Surveillance and Identity Performance: Some Thoughts Inspired by Martin Luther King*, 32 N.Y.U. Rev. L. & Soc. Change 517 (2008) (discussing the disparate surveillance of Black persons, with a particular focus on the FBI’s surveillance of civil rights icon Martin Luther King, Jr.); Torin Monahan, *Reckoning with COVID, Racial Violence, and the Perilous Pursuit of Transparency*, 19 Surveillance & Society 1, 5(2021) (“surveillance is woven into and inseparable from the history of slavery and anti-nonwhite racism”).

<sup>100</sup> See, e.g., Mary Anne Franks, *Democratic Surveillance*, 30 Harv. J.L. & Tech. 425, 441 (2017) (noting that the “surveillance of marginalized populations has a long and troubling history. Race, class, and gender have all helped determine who is watched in society, and the right to privacy has been unequally distributed according to the same factors.”)

<sup>101</sup> BROWNE, *supra* note 92, at 16 (similarly describing racializing surveillance as involving situations where “surveillance practices, policies, and performances concern the production of norms pertaining to race and exercise a ‘power to define what is in or out of place.’”)

veillance technologies—such as predictive crime analytics, forensic genetics, and facial recognition software—are modern examples of how the expansion of surveillance can function to solidify pre-existing social hierarchies.<sup>102</sup>

The central theories of surveillance studies thus must be problematized with regard to structures of race and other social hierarchies. Contemporary society—which may be viewed as a “control society” centered on the regulation of data under foundational theory—has not transcended the violence that characterized past “sovereign societies” nor the punishment and normative inculcation of “disciplinary societies.”<sup>103</sup> Browne concluded, in her examination of racializing surveillance, that “[d]isciplinary power did not do away with or supplant the majestic and often gruesome instantiations of sovereign, power” but rather that “both formulations of power – sovereign and disciplinary – worked together” to uphold the racial order.<sup>104</sup> The conception of “control” in modern surveillance studies nonetheless remains useful in understanding racializing surveillance, as contemporary surveillance is now primarily digital<sup>105</sup> and yet often serves to control (and limit) access by racialized persons to “white spaces.”<sup>106</sup>

Foundational surveillance theory also posited that technological innovation would ultimately humanize mass surveillance to the benefit of civilization.<sup>107</sup> And yet continuing racial disparities in the deployment of surveillance technology has shown that “advancements in surveillance technology [has] not temper[ed] state reliance on mass discipline and punish-

---

(quoting in part John Fiske, *Surveilling the City: Whiteness, the Black Man and Democratic Totalitarianism*, at 81, Theory, Culture & Society (May 1, 1998)).

<sup>102</sup> See, e.g., RUHA BENJAMIN, RACE AFTER TECHNOLOGY: ABOLITIONIST TOOLS FOR THE NEW JIM CODE 125 (2019); Browne, *supra* note 92 at 8; Molly Griffard, *Article: Bias-free Predictive Policing Tool?: An Evaluation of the NYPD’s Patternizr*, 47 FORDHAM URB. L.J. 43, 65 (2019); Daniel Cossins, *Discriminating Algorithms: 5 Times AI Showed Prejudice*, NEW SCIENTIST, (April 12, 2018) <https://www.newscientist.com/article/2166207-discriminating-algorithms-5-times-ai-showed-prejudice/> [<https://perma.cc/DF3J-QWLF>]; Jack Smith IV, (*Exclusive*) *Crime-prediction Tool PredPol Amplifies Racially Biased Policing, Study Shows*, MIC (Oct. 9, 2016), <https://www.mic.com/articles/156286/crime-prediction-tool-pred-pol-only-amplifies-racially-biased-policing-study-shows#TkG1Q7OY5> [<https://perma.cc/WT2S-PTRR>].

<sup>103</sup> See Beydoun, *supra* note 69, at 790; Browne, *supra* note 92, at 9.

<sup>104</sup> Browne, *supra* note 92, at 36.

<sup>105</sup> Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 U. BALT. L. REV.1, 7-8 (detailing how digital surveillance through apps and other forms of tracking increased during the COVID-19 pandemic).

<sup>106</sup> Elijah Anderson, *The White Space*, 1 SOCIO. RACE & ETHNICITY 10, 10 (2015) (defining “white space”); See Kienscherf, *supra* note 92, at 85 (describing racial surveillance as “a colonial technology for (re)producing racial divisions within the US working class while also drawing out the dialectical relations between transparency and opacity in contemporary racializing surveillance”); Arnett, *supra* note 7, at 1111 (describing “targeted form(s) of [racial] surveillance. . . as. . . a tool of exploitation and social control”); Sara E. Yates, *The Digitization of the Carceral State: The Troubling Narrative Around Police Usage of Facial Recognition Technology*, 19 COLO. TECH. L.J. 483, 486 (finding that “targeted surveillance, investigations, and arrests of people of color can be understood as methods [of] racialized social control”).

<sup>107</sup> Foucault, *supra* note 77, at 11.

ment” but rather has contributed to new patterns of subjugation.<sup>108</sup> Indeed, it has been shown by Browne and others that “advancements in surveillance technology often had the effect of inflicting *more* violence when the surveilled subjects were Black”<sup>109</sup> or otherwise racialized as “other.”<sup>110</sup> There have already been many global examples of racialized groups being disproportionately targeted by state authorities for COVID-19 surveillance, with such surveillance contributing to increased police profiling, discrimination, and stigma.<sup>111</sup>

## II. SURVEILLANCE NORMALIZATION

Mass surveillance can serve a number of different, and at times conflicting, ends. Surveillance systems have been created to improve the quality of health care, assist with disease tracking, maintain friendship networks via social media sites, provide accountability for police misconduct, enhance work productivity, and aid public safety. In other words, surveillance can be utilized to promote the greater good of society. Surveillance systems can also be used for purposes unrelated to promoting the public good, such as to maximize corporate profits, engage in racial and religious profiling, censor free speech, and target oppositional political groups.

Notwithstanding the underlying purpose of mass surveillance, the potential for privacy right violations (with marginalized social groups often disproportionately targeted) has been exacerbated by the recent expansion of surveillance technology. The exponential growth of surveillance systems in the United States (and globally) over the last few years has been driven by a number of factors, including significant advancements in technology,<sup>112</sup> the rise of surveillance capitalism,<sup>113</sup> lax privacy regulation,<sup>114</sup> and crisis opportunism. Surveillance in response to the ongoing COVID-19 crisis has been

---

<sup>108</sup> Beydoun, *supra* note 69, at 792.

<sup>109</sup> Beydoun, *supra* note 69, at 794; Benjamin, *supra* note 102.

<sup>110</sup> Beydoun, *supra* note 69, at 795 (applying surveillance theory to non-Western, non-democratic societies marked by racial and religious difference). *See also* Jeffrey L. Vagle, *The History, Means, and Effects of Structural Surveillance*, 9 NE. U.L. REV. 103, 112 (2017) (“Surveillance—specifically, the coding of information describing these activities—is critical to the state’s power/violence monopoly, because it provides a framework for effectively scaling direct supervision to nation-state sizes.”) (applying Johan Galtung’s theory of structural violence to the surveillance context).

<sup>111</sup> *See generally* Maya Sabetello, Mary Jackson Scroggins, Greta Goto, Alicia Santiago, Alma McCormick, Kimberly Jacoby Morris, Christina R. Daulton, Carla L. Easter & Gwen Darien, *Structural Racism in the COVID-19 Pandemic: Moving Forward*, 21 AM. J. BIOETHICS 56, 61 (2020); Tereza Hendl, Ryoa Chung, & Verina Wild, *Pandemic Surveillance and Racialized Subpopulations: Mitigating Vulnerabilities in COVID-19 Apps*, BIOETHICAL INQUIRY 831 (2020).

<sup>112</sup> *See, e.g.*, Benjamin, *supra* note 102, at 128-29 (examining the relationship between emerging technologies and social inequality).

<sup>113</sup> Modern democracies, such as the United States, have ostensibly entered the “control society” stage envisioned by Foucauldian surveillance theory as discussed *supra* in Part I of this Article.

<sup>114</sup> *See supra* Part I of this Article.

influenced by each of these drivers, such that the world is experiencing one of the greatest expansions of mass surveillance in modern history.<sup>115</sup> Surveillance technologies developed by both state and private non-state entities have been rapidly integrated into nearly every sphere of our daily lives—sometimes with our consent (such as PCR testing or the use of health monitoring apps) and at other times without our consent (such as school or workplace digital monitoring, public surveillance via CCTV, or cell site location data).<sup>116</sup> One example of the latter is the Google-Massachusetts ill-fated partnership to secretly install a “MassNotify” COVID-19 tracing app into the Android devices of Massachusetts residents without consent.<sup>117</sup> Similarly, the Center for Disease Control in the United States (as well as the National Health Service in the United Kingdom) has relied on private data analytics companies—such as the notoriously clandestine Palantir—to collect and analyze data to assist in controlling the spread of COVID-19.<sup>118</sup>

COVID-19 surveillance technologies have entered our homes, our schools, our workplaces, and our public spaces, while also being implemented for immigration and travel purposes. The personal information collected by the proliferation of COVID-19 surveillance tools ranges from health-related data (including genetic data) and biometric data to location data, cell phone data, and information concerning private communications.<sup>119</sup>

---

<sup>115</sup> Kristine Eck & Sophia Hatz, *State Surveillance and the COVID-19 Crisis*, 1 J. HUM. RTS. at 603 (2020) (noting that the “outbreak of COVID-19 has ushered in a global rise in state surveillance” with “governments in country after country [turning] to surveillance as a means of tracing the spread of the disease and enforcing lockdowns”); Alan Butler & Enid Zhou, *Disease and Data in Society: How the Pandemic Expanded Data Collection and Surveillance Systems*, 70 AM. U. L. REV. 101, 102 (2021) (“One of the less obvious but more long-lasting changes may well be the expansion of data collection and surveillance systems adopted both in response to, and as a result of, the pandemic.”); Michael K. McKall, Margaret M. Skutsch, & Jordi Honey-Roses, *Surveillance in the COVID-19 Normal: Tracking, Tracing, and Snooping- Trade-Offs in Safety and Autonomy in the E-City*, 10 INT’L J. E-PLANNING RESEARCH (2021) (finding that “[s]urveillance technologies are being deployed at an unprecedented pace in cities throughout the world, amid the fears of COVID-19 and with little discussion about the long-term consequences.”); Emma Mendelson, *How the Fallout from Post-9/11 Surveillance Programs Can Inform Privacy Protections for COVID-19 Contact Tracing Programs*, 24 CUNY L. REV. 35, 36 (2021) (examining the “unprecedented surveillance landscape” ushered in by the COVID-19 pandemic).

<sup>116</sup> A summary of many of the COVID-19 surveillance technologies that have proliferated in response to the disease can be found at Butler & Zhou, *supra* note 115 at 1580 (discussing health-related data collection tools and surveillance technology in schools and the workplace).

<sup>117</sup> See Lyon *supra* note 84 at 117.

<sup>118</sup> Rob Kitchin, *Civil Liberties or Public Health, or Civil Liberties and Public Health? Using Surveillance Technologies to Tackle the Spread of COVID-19*, Space & Polity 362-381, 364 (2020); Natalie Ram & David Gray, *Mass Surveillance in the Age of COVID-19*, Journal of Law and the Biosciences, 1-17, 3 (2020) (describing how the “U.S. government is already tapping bulk cell phone location data for public health surveillance purposes. . . include[ing] tracking the presence and movement of people in certain areas of geographic interest.”).

<sup>119</sup> See, e.g., Butler & Zhou, *supra* note 115 at 1580-81 (noting that as “a result of the pandemic, there has been a broad expansion in the collection of personal data including health and health-related information, location data, biometric data, sensitive communications, and other types of data that would not typically have been created or collected in the past”).

The scope of the privacy intrusion is simply breathtaking, and yet American law provides little to no safeguards on how information gleaned from COVID-19 surveillance tools can be used, whether the information must be permanently de-anonymized (if possible), or how long the surveilling entity (the state or technology companies) can retain (or commodify) the data. While the use of public health surveillance technologies is certainly critical in the continuing fight against COVID-19, there is nonetheless a significant risk that such information will be utilized in altogether separate contexts (such as criminal investigations and school and workplace evaluations) and that pandemic-related surveillance technologies will continue to operate even once the pandemic ends in the future. The prospect of mission creep has already begun to materialize, with surveillance—legitimized on COVID-19 grounds—used for law enforcement, commercial, and other purposes that are completely unrelated to the promotion of public health. The occurrence of such crisis opportunism—by both private companies hoping to profit from the crisis and national governments hoping to increase social control over the populace—in the wake of the COVID-19 pandemic is not altogether surprising. Naomi Klein thoroughly documented how large-scale crises can lead to “disaster capitalism” where state and non-state actors seek to exploit a crisis for other means.<sup>120</sup>

The pervasiveness with which new surveillance technologies have entered daily life have led many to question whether meaningful privacy still exists in the modern world. A related question is whether technologies of surveillance have so altered expectations of privacy such that omnipresent surveillance has become accepted as a reasonable trade-off for the perceived benefits of living in a surveillance state.

There are a number of signs that the COVID-19 crisis is normalizing both governmental and corporate surveillance at the expense of core civil liberties, with disproportionate impacts on racialized and other marginalized persons.<sup>121</sup> The disproportionate public health, educational, employment,

<sup>120</sup> See generally NAOMI KLEIN, *THE SHOCK DOCTRINE* (2007).

<sup>121</sup> See, e.g., McKall et al., *supra* note 115, at 29 (“The current crisis is normalizing surveillance measures at an unprecedented scope and scale” as it “is making it easier to justify new surveillance and control measures” in the name of public health) (“Most critical observers assume the expansion in surveillance will be nearly impossible to scale back ‘post-pandemic.’”); Gemma Newlands, Christoph Lutz, Aurelia Tamò-Larrieux, Eduard Fosch Villaronga, Rehana Harasgama, & Gil Sheitlin, *Innovation Under Pressure: Implications for Data Privacy During the COVID-19 Pandemic*, 7 *BIG DATA & SOC’Y* 1, 2 (2020) (“Concerns centre around how the pandemic could be exploited as an opportunity to normalize governmental surveillance . . . particularly into the domestic and biopolitical sphere); Martin French & Torin Monahan, *Dis-ease Surveillance: How Might Surveillance Studies Address COVID-19?*, 18 *SURVEILLANCE & SOC’Y* 1, 6 (concluding that surveillance studies should examine “the ways that this global health crisis is being used to normalize oppressive surveillance measures, perhaps making them seem more palatable or even necessary as insurance against unknown future contagions or threats.”); Jessica Vitak & Michael Zimmer, *More Than Just Privacy: Using Contextual Integrity to Evaluate the Long-Term Risk from COVID-19 Surveillance Technologies*, 6 *SOC. MEDIA + SOC’Y* 1, 1 (“When considering surveillance and monitoring in response to COVID-19, we recognize that . . . there is a risk that temporary measures established

welfare, and criminal surveillance of Black, non-white, immigrant, and poor persons is well documented.<sup>122</sup> In keeping with Foucauldian surveillance theory, mass surveillance in a neo-control society (such as the United States) tends to sort society into different categories (“Black,” “poor,” “gay,” “immigrant”) that can be controlled to maintain the existing social order.<sup>123</sup> Surveillance technology has already bled into non-public health areas, such as criminal justice,<sup>124</sup> employment,<sup>125</sup> and education.<sup>126</sup> After children and students around the world were forced to transition to remote online learning in the wake of the pandemic, for example, a new Human Rights Watch report discovered that 89% of such online learning platforms placed privacy rights at risk or actively impinged on those rights.<sup>127</sup> Relatedly, a federal judge recently found that remote education technology adopted in response to COVID-19 can violate the privacy rights of students, holding that it was unconstitutional under the Fourth Amendment for virtual exam proctoring software to scan the living space of students.<sup>128</sup>

The surveillance tools used to control the spread of COVID-19 have already disparately impacted racial, religious, and other marginalized communities throughout the world. In the United States, for example, law enforcement has disproportionately applied a variety of COVID-19 public health measures. During the early days of the pandemic, Black, Latinx, and other racialized persons received more than 80% of the summonses issued by New York City police for violating COVID-19 stay-at-home orders and

---

during a crisis become permanent and unnecessarily reduce citizens’ privacy, which was the case in the United States following the September 11 terrorist attack.”); Rob Kitchin, *Civil Liberties or Public Health, or Civil Liberties and Public Health? Using Surveillance Technologies to Tackle the Spread of COVID-19*, 24 *SPACE & POLITY* 362, 371 (2020) (“With good reason then, there are fears that the systems deployed to tackle the pandemic will not be turned off after the crisis, instead becoming part of the new normal in monitoring and governing societies.”).

<sup>122</sup> See generally GELLMAN & ADLER-BELL, *supra* note 96 (summarizing the disparate surveillance of marginalized social groups); BROWNE, *supra* note 92, at 66 (providing a detailed account of racialized surveillance and its connection to maintaining racial hierarchies and inequality); Arnett, *supra* note 7, at 4-5 (analyzing the history of disparate racialized surveillance in the United States).

<sup>123</sup> See DAVID LYON, *PANDEMIC SURVEILLANCE* 96 (2022).

<sup>124</sup> Christian Sundquist, *Pandemic Policing*, 37 *GA. ST. U. L. REV.* 1339, 1354 (2021).

<sup>125</sup> Simon Migliano & Christine O’Donnell, *Employee Monitoring Software Demand Trends 2020-22*, *TOP10VPN* (Aug. 8, 2022), <https://www.top10vpn.com/research/covid-employee-surveillance/> [perma.cc/G8L5-TAY3] (finding that demand for employee surveillance software after the start of the pandemic increased by 80% compared with pre-COVID levels). Employers adopted various surveillance systems to monitor both the health and productivity of their employees following the COVID-19 outbreak. See Butler & Zhou, *supra* note 115, at 104.

<sup>126</sup> Tiffany C. Li, *Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis*, 52 *LOYOLA UNIV. CHI. L. REV.* 767, 790 (2021).

<sup>127</sup> HUMAN RIGHTS WATCH, *“How Dare They Peep Into My Private Life?” Children’s Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic* 89 (2022), <https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments> [https://perma.cc/74WS-CFQV].

<sup>128</sup> *Ogletree v. Cleveland State Univ.*, No. 1:21-cv-00500, 2022 WL 3581569, at \*1 (N.D. Ohio Aug. 22, 2022).

constituted 92% of all people arrested for social distancing violations.<sup>129</sup> Globally, ethnic minorities (often non-citizen immigrants) have been subjected to disparate surveillance, quarantine, and discrimination in the enforcement of COVID-19 public health protocols.<sup>130</sup> In one stark example that aligns with the Foucauldian notion of surveillance as control, Bulgaria deemed persons of the Roma ethnic minority to be a public health threat that needed to be “controlled and contained” via targeted surveillance measures while spraying chemicals from planes to “disinfect” Roma neighborhoods.<sup>131</sup> The disproportionate COVID-19 surveillance of racialized groups during the pandemic is facilitated by pre-existing and continuing disparities in criminal, poverty, and immigration surveillance.<sup>132</sup>

A central concern is whether the surveillance tools employed to combat COVID-19 will become a permanent aspect of daily life—even when, or if, the current pandemic recedes. The United States’ experience following the 9/11 terrorist attacks clearly supports the notion that COVID-19 surveillance practices may become normalized and a permanent cog of the national surveillance apparatus, as most of the laws that expanded surveillance following the attacks are still in force.<sup>133</sup> The COVID-19 pandemic thus has the potential to normalize mass surveillance practices as the result of surveillance capitalism and techno-utopianism.

The manner in which individuals can normalize new events and social systems can be better understood by reference to the cognitive processes of

<sup>129</sup> Josiah Bates, *Police Data Reveals Stark Racial Discrepancies in Social Distancing Enforcement Across New York City*, TIME MAG. (May 8, 2020), <https://time.com/5834414/nypd-social-distancing-arrest-data/> [<https://perma.cc/DJJ2-KLK7>]; Ashley Southall, *N.Y.C. Commissioner Denies Racial Bias in Social Distancing Policing*, N.Y. TIMES (May 13, 2020), <https://www.nytimes.com/2020/05/13/nyregion/nypd-social-distancing-race-coronavirus.html> [<https://perma.cc/Q85Y-RRJH>].

<sup>130</sup> AMNESTY INT’L, *Policing the Pandemic: Human Rights Violations in the Enforcement of COVID-19 Measures in Europe*, 10-11 (2020), <https://www.amnesty.org/download/Documents/EUR0125112020ENGLISH.PDF> [<https://perma.cc/X3S4-559V>]; Daniel Boffey, *Policing of European Covid-19 Lockdowns Shows Racial Bias - Report*, THE GUARDIAN (June 24, 2020), <https://www.theguardian.com/world/2020/jun/24/policing-of-european-covid-19-lockdowns-shows-racial-bias-report> [<https://perma.cc/K94M-DMQL>].

<sup>131</sup> AMNESTY INT’L, *supra* note 130, at 11; Maria Cheng & Teodora Barzakova, *Some European Officials Use Virus as Cover to Target Roma*, ASSOCIATED PRESS (October 15, 2020), <https://apnews.com/article/virus-outbreak-pandemics-police-discrimination-eastern-europe-2cbcd5ee070578b73b1bc35ebdb426e> [<https://perma.cc/8YAQ-HLJX>]. The Roma have been disproportionately policed in many other countries as well, with officials blaming Roma persons for the spread of COVID-19 and subjecting them to harsh quarantines and police abuses of force. AMNESTY INT’L, *supra* note 130, at 20.

<sup>132</sup> GELLMAN & ADLER-BELL, *supra* note 96, at 2 (providing a summary of the disproportionate surveillance of the racialized and poor) (“Mass surveillance society subjects us all to its gaze, but not equally so. . . [as] its power touches everyone, but its hand is heaviest in communities already disadvantaged by their poverty, race, religion, ethnicity, and immigration status.”).

<sup>133</sup> *See, e.g.*, McKall, et al., *supra* note 115, at 29 (noting that history shows that “democratic rights of privacy and data confidentiality surrendered ‘temporarily’ during a crisis are very difficult to crawl back”).

selective attention, habituation, and rationalization.<sup>134</sup> One driver of normalization is the extent to which people focus only on the perceived benefits of a particular surveilling technology (e.g., this is necessary for the greater public good) while failing to consider the possible costs of the privacy intrusion (e.g., the commodification and disclosure of one's health data). The *selective attention* that individuals give to COVID-19 surveillance tools, typically focusing on the touted public health benefits of such surveillance while ignoring (or simply being unaware of) the privacy costs, is well-documented and increases the potential for normalization.<sup>135</sup>

When individuals are unaware of (or simply ignore) the privacy risks attendant to COVID-19 surveillance via internal processes of selective attention, the possibility that they may become *habituated* to mass surveillance increases significantly.<sup>136</sup> As we approach the third year of the COVID-19 pandemic, it appears increasingly likely that “repeated exposure to surveillance might leave people cognitively and emotionally unmoved by ongoing monitoring and analysis.”<sup>137</sup> One empirical study has already found that routinization of COVID-19 tracking apps is imminent.<sup>138</sup> The study sought to examine whether expectations of privacy in the United States had changed during the pandemic through a series of scenario-based interviews with American adults.<sup>139</sup> The interviews presented participants with a scenario regarding a fictional COVID-19 tracking app that was connected to a smart thermometer, which informed participants that the data would both be used to measure the spread of disease and could be accessed “by the authorities, doctors, and scientists.”<sup>140</sup> The scenario further provided that the app would continue to collect and share information “even after the disease outbreak has dissipated.”<sup>141</sup> The researchers found that “[p]articipants routinely expected that data collected through apps related to public health would be shared with unknown third parties for the financial gain of the app makers” and yet were complacent with such surveillance because it was for “the greater good.”<sup>142</sup> The researchers reasoned that their findings were consistent with surveillance capitalism because (1) pandemic surveillance has “increased people’s daily reliance on technology” and (2) such “technological solutions. . . are entangled with institutions whose survival is predicated on

---

<sup>134</sup> See Evan Selinger & Judy Hyojoo Rhee, *Normalizing Surveillance*, 22 N. EUR. J. OF PHIL. 49, 56–61 (2021).

<sup>135</sup> *Id.* at 57.

<sup>136</sup> *Id.* at 57–59.

<sup>137</sup> *Id.* at 57–58. The pandemic has also increased awareness of the privacy intrusions related to COVID-19 surveillance, although this has not led to widespread public resistance. Athina Ioannou & Iis Tussyadiah, *Privacy and Surveillance Attitudes During Health Crises: Acceptance of Surveillance and Privacy Protection Behaviours*, 67 TECH. IN SOC'Y 1, 8 (2021).

<sup>138</sup> Seberger & Patil, *supra* note 91, at 1.

<sup>139</sup> *Id.* at 4–5.

<sup>140</sup> *Id.* at 4.

<sup>141</sup> *Id.*

<sup>142</sup> *Id.* at 1.



data-driven ‘dehumanization’ of the user and corporate initiatives that foster people’s resignation to accepting privacy violations as inevitable.”<sup>143</sup>

These findings, although limited in scope and scale, provide support for the proposition that people are not only becoming habituated to COVID-19 surveillance tools (which may well become permanent), but also may become “favorably disposed” to normalization itself.<sup>144</sup> A recent pre-COVID literature review suggests that broad acceptance of, or at least resignation towards, currently existing surveillance technologies may well be occurring.<sup>145</sup> The authors concluded following a review of rationalization theory that “the diffusion and conveniences of algorithms could be systematically eroding people’s capacity and psychological motivation to take meaningful action” against privacy intrusions.<sup>146</sup> The article sets forth four factors that influence whether people will rationalize, and thus accept (happily or begrudgingly), continued mass surveillance by algorithmic technologies: (1) an awareness of the benefits and conveniences of such technology, (2) an underestimation of the harms of sharing personal information, (3) an awareness of the costs of sharing information, which people develop after the use of technology has taken place, to the extent they develop it at all, and (4) the belief that surveilling technologies have become a permanent aspect of life.<sup>147</sup> All four of these factors are arguably contributing to the normalization of mass surveillance today, given the significant expansion of individual and group surveillance in response to the COVID-19 pandemic.<sup>148</sup>

Normalization Process Theory, developed in the field of sociology, similarly suggests that the wide-spread surveillance practices deployed during the COVID-19 pandemic may become “embedded” in society.<sup>149</sup> The normalization of such mass surveillance can occur when (1) the “coherence” of the benefits of surveillance are clear, (2) the vast majority of society is “cognitively participating” with surveillance tools, (3) there is wide-spread “collective action” to address the pandemic, and (4) these actions are continuously evaluated for effectiveness (such as monitoring by public

---

<sup>143</sup> *Id.* at 2–3 (noting that the “pervasiveness of end-user privacy concerns that arise in relation to surveillance capitalism has been demonstrated to contribute to digital resignation, learned helplessness, and security fatigue”).

<sup>144</sup> Selinger & Rhee, *supra* note 134, at 59–61.

<sup>145</sup> Nathanael J. Fast & Arthur S. Jago, *Privacy Matters . . . Or Does It? Algorithms, Rationalization, and the Erosion of Concern for Privacy*, 31 *CURRENT OP. IN PSYCH.* 44, 44 (2020).

<sup>146</sup> *Id.*

<sup>147</sup> *Id.* at 45–46.

<sup>148</sup> Raluca Csernatonu, *New States of Emergency: Normalizing Techno-Surveillance in the Time of COVID-19*, 6 *GLOBAL AFFS.* 301, 308 (2020) (concluding that “exceptional digital surveillance measures during the current state of emergency have the potential to be normalized and to fundamentally alter the future of (data) privacy and other human rights”).

<sup>149</sup> See Carl May & Tracy Finch, *Implementing, Embedding, and Integrating Practices: An Outline of Normalization Process Theory*, 43 *SOCIO.* 535, 536 (2009).

health officials).<sup>150</sup> These drivers of normalization are also arguably present during the COVID-19 pandemic.

## CONCLUSION

There may not be significant public resistance to the expeditious creep of mass surveillance. Indeed, it seems as though the bulk of society either embraces techno-surveillance as a solution to social problems, is unaware of the potential costs of mass surveillance, has become habituated to ongoing surveillance, or has simply become resigned to living in a surveillance state.

Nonetheless, the potential normalization of mass surveillance practices during the COVID-19 pandemic poses significant risks to the civil liberties critical to a functioning democracy. While surveillance can promote values central to a flourishing society (such as disease mitigation), it also functions to control social and consumer behavior through the imposition of hegemonic norms.<sup>151</sup> The normalization of surveillance can thus undermine the individual autonomy necessary to a free, democratic society. Autonomy in self-definition,<sup>152</sup> social interaction and association,<sup>153</sup> decision-making,<sup>154</sup> and expression is essential to the human flourishing and free exchange of ideas that allows for democratic self-governance.<sup>155</sup>

Professor Jeffrey Vagle aptly notes that the effects of normalized “structural surveillance” include an increase in mistrust of social institutions, civic disengagement, and social ordering.<sup>156</sup> The normalization of surveillance thus not only poses a threat to our civil liberties and institutions, but also increases the likelihood that racialized and other marginalized populations will be disparately impacted by an expansion of surveillance systems.

---

<sup>150</sup> *Id.* at 542–46.

<sup>151</sup> *See supra* Part I.

<sup>152</sup> Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 476 (2015) (noting that “privacy allows a person to experiment with different identities and escape public pressure to conform” (citing Seth F. Kreimer, *Sunlight, Seacrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 69–71 (1991))).

<sup>153</sup> Jennifer A. Brobst, *The Metal Eye: Ethical Regulation of the State’s Use of Surveillance Technology and Artificial Intelligence to Observe Humans in Confinement*, 55 CAL. W.L. REV. 1, 10–11 (2018) (explaining that “privacy and social interaction mutually reinforce each other, allowing a person to safely choose and resist social interactions”).

<sup>154</sup> Thomas B. Kearns, *Technology and the Right to Privacy: the Convergence of Surveillance and Information Privacy Concerns*, 7 WM. & MARY BILL RTS. J. 975, 979 (1999) (noting that autonomy “allows people to make decisions freely and act as individuals” in a democracy).

<sup>155</sup> Kaminski & Witnov, *supra* note 152, at 467 (“Surveillance discourages individuals with unformed ideas from deviating from majority political views . . . if the First Amendment is intended to allow the fullest development of the autonomous self, surveillance interferes with that autonomy.”)

<sup>156</sup> Vagle, *supra* note 110, at 138–47 (while perhaps not solely traceable to the expansion of surveillance, trust in the government has been shockingly low during the COVID-19 pandemic).

\* \* \*