Privacy in the Public Eye: Frogs Boiling and the Right to Privacy

Milton Heumann,[*] Dylan Serrentino-Mullins,[**] Jessica Graham[***]
Eric Fecso,[±] Jessica Han[±±] & Anar Murji[±±±]

This paper presents a qualitative study, consisting of six focus groups organized according to the age of participants, on public attitudes surrounding the right to privacy. Several major findings emerged from these focus groups, including qualitative evidence that suggests that age does not play a major role in respondents' attitudes toward privacy. Based upon these findings and other patterns in respondents' attitudes, we advance a theory that relates people's opinions on the value of privacy within society writ large to their perceptions of an individual's ability to protect his or her personal information. Finally, we conclude by speculating about a new conception of privacy—one that may comport with a world where the pace of technological innovation is extraordinary.

[*]Distinguished Professor of Political Science, Rutgers University—New Brunswick.
[**]Truman Scholar, currently participating in Truman-Albright Fellowship. B.A. Rutgers University—New Brunswick, 2021.
[***]J.D. Candidate, Harvard Law School, Class of 2023. B.A. Rutgers University—New Brunswick, 2020.
[±]B.A. Rutgers University—New Brunswick, 2021.
[±±]Masters Student, London School of Economics, Class of 2022. B.A. Rutgers University—New Brunswick, 2020.
[±±±]B.A. Rutgers University—New Brunswick, 2021. All of the authors would also like to acknowledge contributions from Lance Cassak and Kyle Morgan. This research was supported in part by funding from the Kneller Fellowship of Rutgers University. Correspondence concerning this Article should be addressed to Prof. Milton Heumann, Department of Political Science, Rutgers—The State University of New Jersey, 89 George Street, New Brunswick, NJ 08901-1411. Contact: Heumann@polisci.rutgers.edu.

I. INTRODUCTION

We call this project the "Frog Project" and we call ourselves the "Frog Team." Although we each have had longstanding interests in various privacy policies, the catalyst for bringing us together was revisiting a column in *The New York Times*, which quoted Laurence Tribe, referencing an old parable about a frog relishing the warmth of his bath, only to find it gradually getting unbearably hot. As Tribe stated in the context of privacy:

> The more people grow accustomed to a listening environment in which the ear of Big Brother is assumed to be behind every wall, behind every e-mail, and invisibly present in every electronic communication, telephonic or otherwise—that is the kind of society, as people grow accustomed to it, in which you can end up being boiled to death without ever noticing that the water is getting hotter, degree by degree.[1]

Tribe's reflections, and our own experiences, initially led us to an informal weekly discussion session on privacy-implicated matters. We began by revisiting materials familiar to all students of civil liberties—the famous Supreme Court discovery of a "right to privacy"[2] in the penumbras of the Bill of Rights,[3] the revisiting of the origins of this right in *Roe v. Wade*,[4] and the expansion of the Court's interest from

[1] Bob Herbert, *What's Left Unsaid*, N.Y. TIMES (Jan. 23, 2006), https://www.nytimes.com/2006/01/23/opinion/whats-left-unsaid.html.

[2] *See generally* Jamal Greene, *The So-Called Right to Privacy*, 43 U.C. DAVIS L. REV., 715 (2010) (discussing the use of the right to privacy as the legal basis for court cases moving forward); *see also* Bert-Jaap Koops et al., *A Typology of Privacy*, 38 U. PA. J. INT'L L. 483 (2017) (discussing broadly the right to privacy in a contemporary context).

[3] *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

[4] Roe v. Wade, 410 U.S. 113, 152 (1973).

personal autonomy matters to more of the surveillance issues of the twenty-first century.[5] But what became clear to all of us very quickly was how limited these doctrinal considerations were, and how they dramatically lagged exploring privacy matters in domains that affect most of us the majority of the time.

The gap between our "old reliable" court cases and our daily experiences gave birth to this project. We were interested in "things privacy," and were determined to discern the public opinion about the water seemingly getting hotter—maybe even getting to the boiling point! We were resolved to explore this issue without prejudgment—without wringing our hands about a public cringing in the rapid advent of a dystopian world. There were many ways to proceed, but we opted for exploratory, open-ended, qualitative data collection rather than for a more rigorous (and confining) quantitative approach. More details about our approach can be found in the research design section below.[6] Here we note our overarching research interest—to understand responses to the often-mind-boggling pace of technological innovations and the implications of these innovations for one's privacy. Although our goals included gingerly testing some hypotheses, for the most part, our interests were descriptive: learning how the public felt about a range of privacy issues, and from these views teasing out more themes that capture, in nuanced ways, public attitudes—or lack thereof—on the bathwater very quickly heating up.

II. BACKGROUND

A comprehensive review of the vast compilation of existing privacy literature was beyond the scope of our research. Instead, we began by focusing on Samuel Warren and Louis Brandeis's law review article, *The Right to Privacy*,[7] which fellow scholars have endlessly referenced. Warren and Brandeis contended that a right to privacy existed within American society and that this right was derived from earlier contract and property common law precedents.[8] They argued that a right to privacy should be understood as a qualified right, simply meaning "the

[5] *See generally* Milton Heumann et al., *Privacy and Surveillance: Public Attitudes on Cameras on the Street, in the Home, and in the Workplace*, 14 RUTGERS J.L. & PUB. POL'Y 37, 60–74 (2016) (examining the legal issues implicated in the increased use of surveillance).

[6] *See infra* Part III.

[7] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[8] *Id.* at 208.

right to be let alone."[9] This explicit legal right was deemed fundamentally necessary in response to a multitude of factors:

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.[10]

The notion that privacy was a fundamental necessity is one of the central themes of another important piece of the literature on privacy. Alan Westin's work, *Privacy and Freedom*, approached the issue of defining privacy and explaining its function within differing societies from a sociological perspective.[11] Westin stated that privacy was more than a personal preference, but instead, "an important functional requirement for the effective operation of a social structure."[12] Warren and Brandeis presented their conception of a right to privacy within the legal understanding that this protection was qualified, not absolute.[13] Similarly, Westin argued that each society struggles with finding "an overall equilibrium" between demands for privacy balanced with other societal demands.[14] This struggle was conceptualized based on a crucial idea: "[A]ll individuals are constantly engaged in an attempt to find sufficient privacy to serve their general social roles as well as their individual needs of the moment. Either too much or too little privacy can create imbalances which seriously jeopardize the individual's well-being."[15]

In addition to this sociological conceptualization of privacy, Westin speculated that this endless struggle for achieving a balance between privacy and other societal interests could be seriously complicated by future technological developments.[16] The first possible threat was that technological and legal developments would enable the expansion of sophisticated surveillance capabilities, which would threaten individual

---

[9] *Id.* at 193; *see also* THOMAS COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (1879) (Warren and Brandeis adopted the phrase from this treatise by Judge Thomas Cooley).

[10] Warren & Brandeis, *supra* note 7, at 196.

[11] ALAN WESTIN, PRIVACY AND FREEDOM 2 (Daniel J. Solove, ed., 2d ed. 2015).

[12] *Id*. at 64 (quoting ROBERT MERTON, SOCIAL THEORY AND SOCIAL STRUCTURE 375 (1957)).

[13] Warren & Brandeis, *supra* note 7, at 214–18.

[14] WESTIN, *supra* note 11, at 27.

[15] *Id.* at 44.

[16] *Id.* at 91–95.

and collective privacy.[17] The second was that technological developments could increasingly allow outsiders to access information that an individual desired to remain confidential.[18] Lastly, the already occurring practice of collecting data related to individuals' activities could be vastly expanded to allow government and private organizations to compile a large collection of data that could effectively lead to a dossier on every individual.[19] Westin's three predictions proved to be incredibly accurate.

Case law on privacy matters is of comparatively more recent vintage. Initially, the Court gave its attention to matters of personal autonomy—birth control,[20] abortion,[21] and then same-sex marriage.[22] Then, more recently and more significantly for this paper, the Court began examining technological issues. In *Riley v. California*, law enforcement searched the car of appellant David Leon Riley after discovering his possession of an invalid driver's license.[23] The search of his car was lawful, and led to his arrest for possession of firearms—but this was not the search Riley was appealing.[24] Upon searching his car, police confiscated his phone and searched that, as well.[25] The contents on his phone provided police with evidence of his gang affiliation, leading to separate charges, including shooting at an occupied vehicle, attempted murder, and assault with a semi-automatic firearm.[26] Riley appealed on his Fourth Amendment rights, arguing that the evidence found in his phone should not be admitted at trial.[27] The Court ruled in his favor, holding that the warrantless search exception (aimed at protecting law enforcement) did not apply, as digital data cannot possibly harm the officers, and the evidence could have easily been preserved until the officers obtained a search warrant.[28] The Court classified cell phones as "minicomputers"[29] that contain extensive

17 *Id.* at 97–143.
18 *Id.* at 145–49.
19 *Id.* at 173–84.
20 *See* Griswold v. Connecticut, 381 U.S. 479, 480 (1965).
21 *See* Roe v. Wade, 410 U.S. 113, 116 (1973).
22 *See* Obergefell v. Hodges, 576 U.S. 644, 652 (2015).
23 Riley v. California, 573 U.S. 373, 378 (2014).
24 *Id.* at 379.
25 *Id.*
26 *Id.*
27 *Id.*
28 *Id.* at 398–99.
29 *Riley*, 573 U.S. at 393.

private information and held that any information stored via "cloud computing" is not even technically on the arrestee's person.[30]

Chief Justice Roberts, in his opinion for the Court, addressed this concern by stating, "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."[31] Obtaining a warrant is necessary to search a phone, as it is a separate piece of evidence and phones are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[32] That the Chief Justice would liken cell phones to a person's anatomy is a testament to the intimacy of the data stored on these devices.

In 2018, in *Carpenter v. United States*, the Court further distinguished between cell phones and other potential sources of evidence.[33] Rather than examining the protections for information found on a cell phone, as was done in *Riley*, *Carpenter* explored the protections for information about a cell phone, including the location and movements of the cell phone (and potentially its user).[34] Called "cell site" location information (CSLI), this data provided the evidence needed to charge appellant Timothy Carpenter with aiding and abetting armed robbery involving interstate commerce, making it a federal offense.[35] Carpenter appealed, claiming that the warrantless search and seizure of this data was a violation of his Fourth Amendment rights, and the Court agreed.[36] In a separate decision, the Court held that Fourth Amendment protections not only include property interests but extend to reasonable expectations of privacy.[37] With respect to privacy rights, the Court declined to extend the "third-party doctrine"—which argues that any information disclosed to a third party carries no reasonable expectation of privacy—to CSLI, as this type of location data is more intrusive than the third-party doctrine could reasonably encompass.[38] Thus, the Court required a separate warrant for the access of location data, further bolstering privacy rights in an evolving digital age.[39]

30 *Id.* at 397–98.
31 *Id.* at 403.
32 *Id.* at 384.
33 Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).
34 *Id.* at 2214.
35 *Id.* at 2212–13.
36 *Id.* at 2220.
37 *See* Katz v. United States, 389 U.S. 347, 351–52 (1967).
38 *Carpenter*, 138 S. Ct. at 2222.
39 *Id.*

Despite the increasing number of privacy-related cases appearing before the Supreme Court, scholars have continued to wrestle with conceptualizing the function of privacy within American society. Judge Richard Posner noted that privacy is simply misunderstood and is fundamentally about concealment.[40] Posner observed that "[individuals] want to manipulate the world around them by selective disclosure of facts about themselves," and that this conception of privacy can be considered harmful rather than beneficial for society as a whole.[41] Frequently critiqued by Solove and other fellow scholars, this portrayal of privacy is more controversial than not. In his work, *Nothing to Hide: The False Tradeoff Between Privacy and Security*, Solove argues that the lack of a definitive conception of privacy has resulted in separate privacy protections being continually balanced against other societal demands.[42] Contemporary societal issues, particularly issues of national security, have resulted in individuals' forfeiture of privacy protections for a wide range of benefits.[43]

The idea that individuals have continued to trade privacy for other perceived benefits has also been addressed in the most recent notable work regarding privacy: Shoshana Zuboff's *The Age of Surveillance Capitalism*. Individual information has become the fuel driving this new form of "surveillance capitalism," which Zuboff defined as "parasitic and self-referential. It revives Karl Marx's old image of capitalism as a vampire that feeds on labor, but with an unexpected turn. Instead of labor, surveillance capitalism feeds on every aspect of human's experience."[44] Furthermore, Zuboff explains how the commodification of individual behavior has created the most valued good within this new form of capitalism at the direct expense of privacy protections within society.[45]

Finally, of importance for our work, we examined two major quantitative studies that presented a glimpse into American attitudes about the issue of privacy. The first study was published in 1981 by Alan Westin in the wake of the passage of the 1974 Federal Privacy Protection Act and the establishment of the Privacy Protection Study

---

[40] Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 393 (1978).

[41] *Id.* at *400*.

[42] DANIEL SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 24–26 (2011).

[43] *Id.* at 55–57.

[44] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 7–8 (2019).

[45] *See id.* at 99–102.

Commission.[46] Westin's study was designed to evaluate if this unprecedented federal legislation, which included the establishment of the Privacy Protection Study Commission, addressed privacy concerns highlighted in earlier published research.[47] Additionally, Westin sought to specifically identify "what degree privacy can and should be protected in an intensely service-oriented, technologically-based society—a society whose collective 'marketplace' is fundamentally fueled by the collection, storage, and use of the personal information of its citizens."[48] The second major quantitative study we examined was the 2019 Pew Privacy Study, which was designed to gauge American attitudes toward specific contemporary privacy issues and potential threats facing them.[49] Despite being separated by thirty-eight years, data from both studies presented a significant number of interesting correlations that should be further explored in a separate research project examining American attitudes toward privacy over time.

III. RESEARCH DESIGN

In our research, we aimed to collect rich *qualitative* data well beyond the constrained responses available within a survey questionnaire. Our study asks individuals to elaborate not only on their attitudes toward privacy but on why they believe they and their associates have developed such attitudes. We conducted six focus groups to collect the privacy data. A priori, we hypothesized that the age of the respondents might often be an explanatory variable, and thus we structured the design to test that theory. Specifically, we conducted six focus groups, two groups for each of three age ranges.[50] Each focus group was two hours long, and the median number of participants in each was seven. For most of the focus groups, all five of the authors participated,[51] and we each led the discussion on different sections of

[46] *Fair Fin. Info. Practices Act: Hearing on S. 1928 Before the H. Subcomm. on Consumer Affairs of the Comm. on Banking, Hous., & Urban Affairs*, 96th Cong. 480–82 (1980).

[47] *Id.*

[48] *Id.* at 576 (remarks of Dr. Alan F. Westin).

[49] *See* Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RES. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information.

[50] We used the following three age group classifications: "Young Adults," aged approximately 18–30, "Middle Age," aged approximately 31–65, and "Seniors," aged 65 and older.

[51] On occasion, one of the authors had to be absent (illness, work conflicts, etc.) from a focus group. Generally, though, all or most were present for every group session.

the interview schedule. A copy of our questions can be found in Appendix A.[52]

Our subject matter ranged over a large number of privacy matters, and we tried to balance adhering to the interview schedule with allowing discussions to flourish, even when they deviated somewhat from the questions at hand. Indeed, the inter-participant exchanges yielded some of our most intriguing results. After each of the focus groups, the authors individually wrote up the sessions, reporting on what the discussants said and reflecting on their comments. Synthesizing these focus group reports, comparing responses across the six groups, and discussing our conclusions as a research team yielded the data that we now review.

IV. FOCUS GROUP FINDINGS

A. *Age Rejected: The Dog That Didn't Bark!*

We begin by acknowledging the rejection of the hypothesis about which we were most confident in its explanatory power. Specifically, it seemed to us that the age of the respondents would matter in a rather systematic way as we explored the implications of the "right to privacy" and technological developments. Our initial intragroup discussions led us to hypothesize that younger respondents were less agonized about privacy tradeoffs and were more accepting of a wide range of technological developments that, potentially, could lead to lessened privacy. To our surprise, this hypothesis was not confirmed. As each of us studied our focus group findings, we marveled at just how wrong we were. The themes discussed below did not characterize a specific age group but instead crosscut these groups. Delving into why the "dog didn't bark" and why age was not a good explanatory variable (intriguing to speculate about) allows us a first peek into the general attitudes of the respondents—across all ages!

For instance, "consent" was one topic that we hypothesized would be particularly split by age.[53] U.S. federal law permits the recording of individual-to-individual conversations by one party without the knowledge or consent of the other party or parties involved, as long as

[52] *See infra* Appendix A.

[53] In our preliminary research discussions, there seemed to be a clear divide between older individuals, who favored two-party consent laws, and younger individuals, who were generally amicable to one-party. This anecdotal trend was not replicated in the focus groups.

at least one person is aware of the recording.[54] Thirty-eight states and the District of Columbia also have what are called "one-party consent laws."[55] Even in two-party states, certain exceptional circumstances allow only one party to be privy to the knowledge of a recording taking place. Some exceptions may include recordings made by police or law enforcement officials, emergency or first responders, or communication service providers, as well as recordings made pursuant to a court order.[56] Individual states have their own exceptions.[57]

We found that the majority of respondents, regardless of age, preferred a two-party system. While many acknowledged exceptional circumstances, such as in cases of domestic abuse or in situations with uneven power dynamics (e.g., employee-employer), the consensus was that two-party systems enabled transparency and trust, rather than the instilled sense of paranoia that they did not want to become the norm. Those exceptions, they argued, should not become the rule. The idea of "everyone going around recording each other," as one respondent said, "would set up a dangerous precedent."[58] Many others agreed that a slippery slope toward a "surveillance society" was an inherent threat to overall privacy, with one person making a principled argument that "privacy is [my] right, why should I have to give it up?"[59] In opposition, the minority that chose the one-party system claimed that if they had nothing to hide, they did not care who recorded them and why—saying that safety or protection was worth sacrificing privacy. Some

[54] *Recording Phone Calls and Conversations*, DIG. MEDIA L. PROJECT, https://www.dmlp.org/legal-guide/recording-phone-calls-and-conversations (last visited April 13, 2020) (citing 18 U.S.C. § 2511(2)(d)).

[55] *Id*. Two-party states also differ as to whether both parties must consent explicitly (i.e., "Yes, I consent to being recorded."), or whether conversing after notification of recording has been provided is sufficient for implicit consent. The eleven other states (California, Delaware, Florida, Illinois, Maryland, Massachusetts, Montana, Nevada, New Hampshire, Pennsylvania, and Washington) have "two-party consent laws" (or "all-party") in effect. *State Law: Recording*, DIG. MEDIA L. PROJECT, https://www.dmlp.org/legal-guide/state-law-recording (last visited April 19, 2021).

[56] For a lengthier exploration of recording consent laws, see Rauvin Johl, *Reassessing Wiretap and Eavesdropping Statutes: Making One-Party Consent the Default*, 12 HARV. L. & POL'Y REV. 177, 178–80 (2018).

[57] *Id*. For example, Illinois and Oregon are two-party states except in cases of electronic recording. Another example is Hawaii, which only requires all-party consent in cases where the recording device is installed in a private place. Massachusetts, for instance, is the only state without a "public location" exception, meaning that a conversation occurring in a public place still requires two party consent. States also vary as to how consent is executed, and whether such recordings are admissible in court.

[58] Member of Focus Group 3 (Young Adults), Rutgers University (Sept. 15, 2019) (on file with author).

[59] Member of Focus Group 4 (Seniors), Rutgers University (Sept. 20, 2019) (on file with author).

respondents went as far as saying the so-called surveillance society already exists; privacy in the modern day is so far eroded that, as one respondent claimed, "everything is being recorded anyway."[60] Despite preconceived notions concerning general familiarity with technology, attitudes toward recording consent laws, and privacy more broadly, participant's ages could not explain this dynamic.

B. *Protecting Privacy and Terms of Service Agreements: Reality or Illusion?*

We can further deduce the extent to which society has prioritized other interests over privacy, such as leniency with business, through close examination of Terms of Service (TOS) agreements. Upon review of focus group attitudes about this issue, three facets of the agreements emerge as potentially problematic: (1) the actual policies that permit companies to collect vast quantities of personal data; (2) the mechanism employed to obtain consent from users; and (3) the societal costs incurred from not accepting these agreements, which in turn apply pressure on users to consent irrespective of the agreement's provisions.

The first facet was only problematic for a minority of our respondents—those that viewed the mere act of data collection itself as invasive. This, however, is the most lucrative aspect of several companies' business models, and the most necessary for others. Google turns a profit by using data collected from consumers to sell targeted advertising but also needs this data to power improvements to the Google search engine and Google maps.[61] Amazon and Apple take voice recordings from Alexa[62] and Siri,[63] respectively, to improve the accuracy of their voice recognition software. Almost all companies use cookies when accessing their websites, which track consumer data as they move from webpage to webpage.[64] When viewed individually, this data seems small and innocuous. The issue is when these data are aggregated into a larger profile that tells companies more than what consumers

[60] Focus Group 2 (Middle Age), Rutgers University (Sept. 15, 2019) (on file with author).

[61] Nicole Lindsey, *Google Data Collection Is More Extensive and Intrusive Than You Ever Imagined*, CPO MAGAZINE (Nov. 14, 2018), https://www.cpomagazine.com/data-privacy/google-data-collection-is-more-extensive-and-intrusive-than-you-ever-imagined.

[62] *Alexa Terms of Use*, *Section 4.1,* AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740 (last visited Apr. 28, 2020).

[63] *Ask Siri, Dictation, & Privacy*, APPLE, https://support.apple.com/en-us/HT210657, (last updated Feb. 19, 2021).

[64] *What are Cookies?*, INDIANA UNIV., https://kb.iu.edu/d/agwm (last updated Jan. 18, 2018).

expected it would reveal. For instance, while individual facts about a person may confer little information when considered on their own, taken together, these facts may paint a more complete picture of that person than what the consumer intended to divulge.[65] One report demonstrated that merely going through normal life routines with an Android phone led Google to be able to collect enough user data to identify user interests accurately.[66] One participant was deeply troubled by this when he said, "I mean they know so much about you. They pretty much own you. I downloaded all of the data that Google had on me. I had so much data. I made the mistake of buying a Google Pixel."[67] This is often the case—a person may believe they have a reasonable expectation of privacy, only to discover that their data had been collected consistently, and without their knowledge, over an extended period.

TOS Agreements are formatted as either "opt in" or "opt out."[68] When a website prompts its users to agree, usually at the bottom of a page immediately upon opening the site, this specific site is using the opt-in style. If no such prompt appears, users must opt out of using the program entirely.[69] This may even be less clear in cases when the user interface is amorphous. While nearly all respondents understood that they had opted in to Google's TOS when they used the search engine, significantly fewer respondents were aware of Alexa's voice recordings being sent back to Amazon for analysis.[70]

We hypothesized that many respondents would not be aware that, by using Google's service, they were agreeing to the corporation's data collection policies. Most respondents did appreciate, however, that by availing themselves of this service (and others), they had acquiesced to the corporation's conditions on the ease with which the organization could aggregate data, sell data, and disseminate data.[71] They were

65 *See* Lindsey, *supra* note 61.

66 Douglas C. Schmidt, *Google Data Collection*, DIGITAL CONTENT NEXT (Aug. 15, 2018), https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf.

67 Focus Group 3 (Young Adults), Rutgers University (Sept. 15, 2019) (on file with author).

68 *See* Berkson v. GoGo, 97 F. Supp. 3d 359, 366–67 (E.D.N.Y. 2015) (discussing the legality of various methods of obtaining consent).

69 *Id.* at 376.

70 *See* Matt Day et al., *Amazon Workers Are Listening to What You Tell Alexa*, BLOOMBERG (Apr. 10, 2019), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.

71 *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1881 (2013) (discussing what individuals lay observers understand in terms of data consent laws).

aware that they had "opted in" without being given an option to "opt out." Most respondents were resigned to the fact that this is how TOS agreements functioned in practice.

Taking it one step further, we asked about situations in which the organization did ask for explicit authorization to its terms and conditions, meaning a person had to affirmatively "opt in" rather than being automatically assumed to agree to terms and conditions by using the service. The assumption was that by being given explicit statements about what they were agreeing to, respondents would have more choice and would have a better handle on what would be done with their information, effectively providing more control over the dissemination of the information they provided. A priori, this sounded more than plausible, and indeed suggested a policy for addressing privacy issues moving forward (we will turn to these in the last section of this paper).[72] But once again, what we assumed was obvious—that a choice to "opt in" with specific explanations as to what was being agreed upon would enhance an individual's control over private information—was incorrect.

Of our respondents across all six focus groups, almost no respondents claimed to read any parts of the TOS.[73] Signing these was routine; ignoring their language was universal. Some bemoaned the length of these agreement sheets; some the difficulty of reading them.[74] Even when we probed deeper and suggested altering the terms of the agreement in ways consistent with policies being adopted in Europe and some states,[75] we found at best a grudging response from a few of the respondents that maybe one change or another (i.e., highlighting key points, shorter forms) might make them give more than a mere cursory look to the documents. A few of these comments are illustrative of these themes:

[72] *See infra* Section VI.B.

[73] *See* Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 546 (2014) (discussing issues surrounding the lack of reading within the context of consumer contract law).

[74] One Focus Group Participant (from our sixth group, Middle Aged individuals), specifically noted that the determining factor behind his reasoning for not reading TOS agreements was the perceived complexity of these document's language. This participant suggested using lower Lexile levels as a standard for encouraging broader understanding of these documents.

[75] *See infra* Section VI.B.

> I skim through the TOS agreements, but that is ultimately not going to make much of a difference. If you don't sign it, you don't get to use the service. And if it is an electronic copy there even isn't an opportunity to modify it[.][76]

> There are sometimes 60 pages of TOS . . . you can't read them . . . few know what they say. You assume they are collecting data . . . if there was more of a choice to opt in, just in theory a difference, since if you don't opt in, you can't use the service. . . . The European Union efforts to change TOS [i.e., highlighting, underlining, shortening] won't matter—no one reads them.[77]

Somewhat facetiously, another respondent claimed that "all the terms and services really need to say is 'We're taking all your stuff, we're making money off it, good luck.'"[78] His point, of course, was that clients really have a sense of what they are giving away but will not change their behavior in any case.

This turns general contract theory on its head, as contracts are generally predicated on the idea of consent being given actively as an opt in. In a 1994 Yale Law Journal article, Peter Schuck wrote, "[t]o say that one cannot be bound by a promise that one did not voluntarily and knowingly make is to say that the individual should be the author of her own undertakings, that a genuine respect for her dignity requires a broad deference to her choices."[79] The issue today is that many people cannot opt out of terms such as Google's or Apple's without incurring opportunity and productivity costs. Putting together the various services and websites respondents visited that had TOS, almost no one felt that they could live today without being bound by these contracts.[80] When asked why they continued to use Google despite expressing dismay with the way Google collected their data, they replied, "Because it's convenient, and I will be left behind socially."[81] It does not matter if

[76] Focus Group 1 (Seniors), Rutgers University (Sept. 13, 2019) (on file with author).

[77] Focus Group 3 (Young Adults), Rutgers University (Sept. 15, 2019) (on file with author).

[78] Focus Group 6 (Middle Age), Rutgers University (Oct. 6, 2019) (on file with author).

[79] Peter H. Shuck, *Rethinking Informed Consent*, 103 YALE L.J. 899, 900 (1994).

[80] Focus Groups 1–6, Rutgers University (Sept. 13–Oct. 6, 2019).

[81] Focus Group 2 (Middle Age), Rutgers University (Sept. 15, 2019 (on file with author).

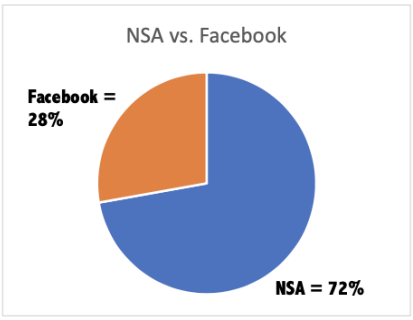
consent is questionably obtained if people do not have alternatives that allow them to "voluntarily and knowingly make" other choices.[82]

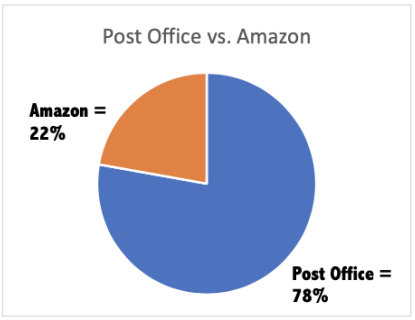
C. *The Role of Government and Corporate Giants: Trust and Tradeoffs*

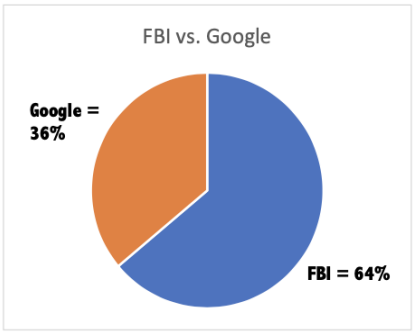
To contextualize privacy and, more importantly, how people conceive privacy, we deemed it necessary to decipher the difference between the expectations people have of public versus private entities. Since many people hold double standards, we found that it was beneficial to partake in a simple voting process, revealing the results to the group after the voting was completed. Then, we allowed people to attempt to defend their clear contradictions in their conceptions.

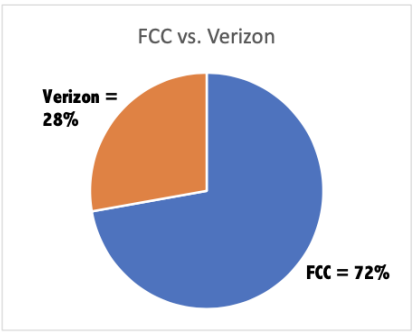
[82] *See* Joseph V. Demarco & Brian A. Fox, *Data Rights and Data Wrongs: Civil Litigation and the New Privacy Norms*, 128 YALE L.J. F. 1016, 1024–26 (2019) (discussing lawsuits involving private parties and data storage).

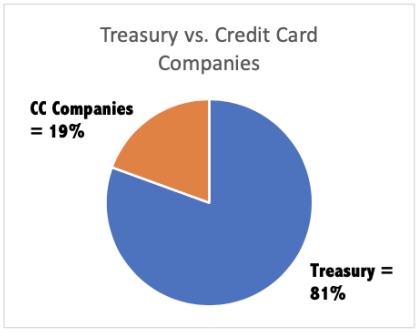
Question 1: Who do you trust more with your private information?



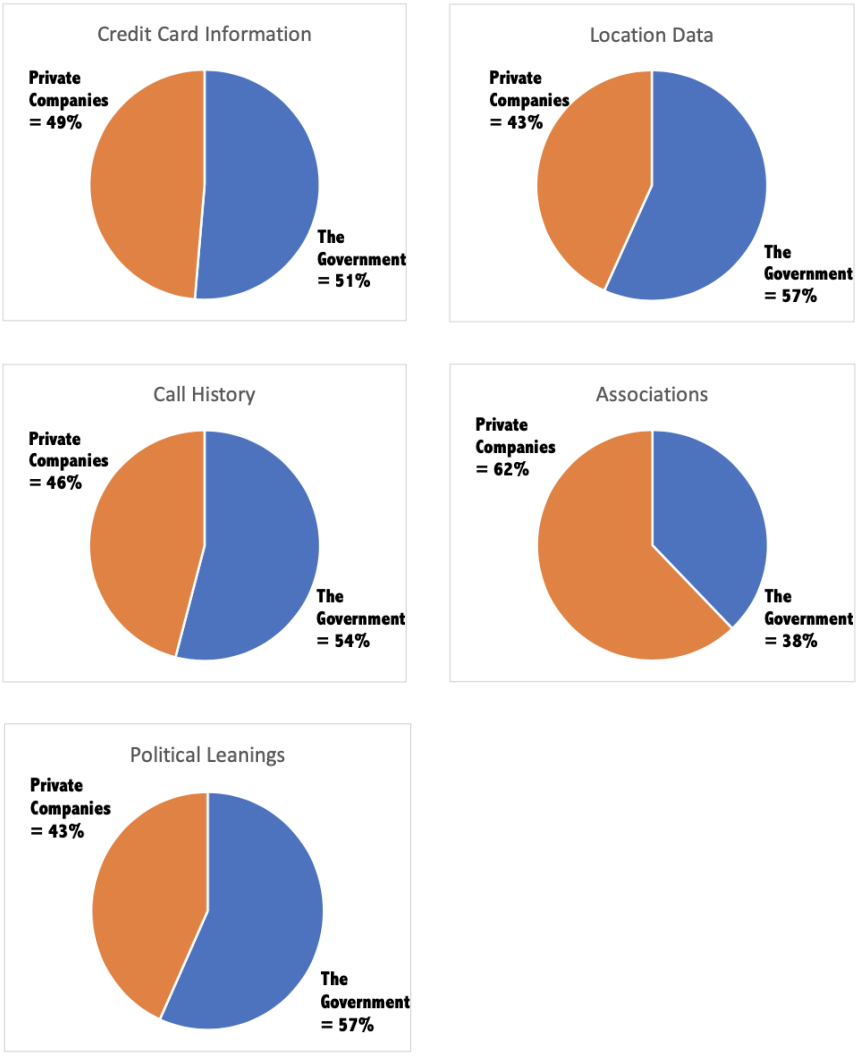








Question 2: In general, who do you trust more with the following sets of data: private companies or the government?



Consistent with our other findings,[83] responses were coherent across age groups. We found that, overall, public entities received more support, or "trust," from our focus groups. We tested this by first varying the entities (i.e., the Treasury or credit card companies), but asking about a general sense of trust, and then by varying the information obtained (i.e., your location), but asking generally "public or private." We found that when naming specific entities, an overwhelming majority selected the public option over the private option. When asking about specific information, though, "the government" either won by a very slim majority or even lost the vote. A factor that could be influencing this contradiction is the negative stigma attributed to "the government." People have always been distrusting of this ominous entity, and that is a likely reason for the voting discrepancy. When we asked about specific government agencies, though, people realized that these agencies do not warrant a sense of fear or distrust, voting in their favor. Another factor that likely influenced our participants in their voting habits is the overwhelming news coverage relating to breaches of data by private corporations. Focus group participants reported that stories about privacy issues with Facebook, Google, and Amazon influenced their decision to pick the government agency rather than the specific company. This could also explain why—in an opposite pattern to that of the government—private companies generally performed better in the collective than as individual companies.

The one noticeable outlier from the aforementioned trends was in the "Associations" question in the second round, where a majority of respondents said that they trusted private companies to know this information more than the government. During the focus groups, respondents would sometimes respond that they picked private companies when they could rationalize the private company knowing this information.[84] Given the prevalence of social media networks as a primary online interface across all generations, it is conceivable that the public has largely accepted private companies having detailed information on a person's friend and family network.

This model of analysis was designed to gauge the "trust," an often-immeasurable feeling, that participants had in various agencies, groups, etc. By seeking a justification as to why the entity would need the information we were asking about, participants unveiled their reasoning skills, ultimately seeming to draw objective conclusions. If

[83] *See supra* Section IV.A.

[84] Focus group notes, Rutgers University (Sept. 13–Oct. 6, 2019) (on file with author).

they were able to see a reason for an entity to know that information, the decision was made clearer.[85] One participant, though, articulated the true design of our questioning, stating, "[a] lot of this comes down to trust. How much do you trust the government not to abuse security cameras, how much do you trust Apple to do what they say they will do."[86] Reinforcing other theories of ours as well, this participant categorized the entire government as one entity, while distinguishing Apple from other tech giants. This participant did not pick a side in this statement but instead discussed the idea of trading off some privacy for increased security. The government, as he referred to it, is often thought of as an entity that strips the general population of privacy with a sweeping promise of safety.[87] Apple, though, promises security at its forefront.[88] The participant draws a similarity with these two, proposing that they both need to prove their efficacy and their reliability in order to gain the trust of the American people.

V. THE RESIGNATION CURVE: PROFILES IN PRIVACY

Across the landscape of themes that surfaced during our focus groups, certain patterns emerged that may offer some broader explanatory power in deciphering people's overall attitudes toward privacy. As mentioned, we initially hypothesized that a person's age might be influential in organizing individuals' opinions on privacy relative to one another. Despite the rejection of our age hypothesis, attitudes about privacy were not homogenous. They could still be roughly organized into a loose typology according to their perceived ability to control their personal privacy, and according to their overarching opinions on the current (and future) state of privacy throughout society.

---

[85] *See* Auxier et al., *supra* note 49. Our methodology for gauging the trust of focus group participants was similar to the Pew Privacy Survey's construction of survey questions for gauging the feelings of respondents as related to the sharing of information with government and private organizations. *See id.* Participants in the Pew Privacy Study responded overwhelmingly that they did not feel the benefits of sharing their personal information with the government or private companies outweighed the possible risks. In more in-depth questions, however, there was significant variation in the participants' responses when asked about their feelings toward sharing specific types of personal information with the government and private companies. *See id.* Additionally, there were also significant differences in the participants' responses when asked about their feelings toward sharing personal information with specific types of government and private organizations. *See id.*

[86] Focus Group 4 (Seniors), Rutgers University (Sept. 20, 2019) (on file with author).

[87] *Id.*

[88] *Apple Privacy Policy*, APPLE (Dec. 14, 2020), https://www.apple.com/legal/privacy/en-ww.

Throughout our various topics of discussion, one feeling guided nearly every respondent's attitude—resignation. Specifically, almost all focus group respondents agreed that the value society places on privacy today is historically lower than at any other point in history.[89] Nearly all focus group respondents also believed—for better or worse—that little could be done to change society's values as they pertain to privacy, due in large part to the various competing interests (convenience, security, etc.) for which privacy is often exchanged.

What did vary among respondents, however, was the extent to which they perceived their ability to maintain agency over their personal privacy. In other words, despite the belief that new technology has pushed society away from privacy writ large, certain respondents expressed the idea that technology could also be proactively used—if individuals chose to do so—as a safeguard in protecting privacy through such practices as private browsing, virtual private networks (VPNs), and encryption.[90] Moreover, individuals' general attitudes toward society given the current state of privacy also varied, as even certain respondents resigned to a world devoid of privacy believed that this was not necessarily problematic. Rather than being consumed with worry over the future of privacy, these individuals instead choose to enjoy the comfort of warm water, so to speak.

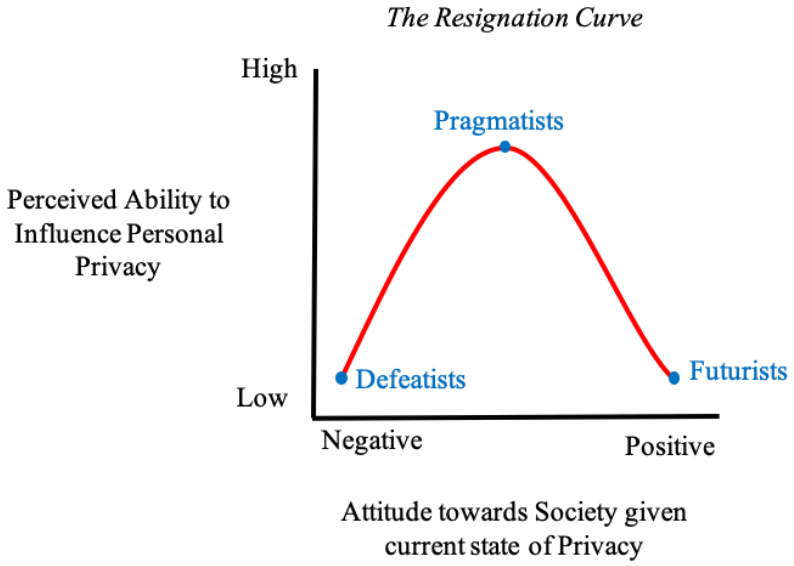
In reviewing the different attitudes among focus group respondents, each respondent could be arranged relative to one another based on both their perceived ability to influence their personal privacy and their general attitude toward society given the current state of privacy. We call this arrangement the "Resignation Curve," as respondents who possessed extremely negative attitudes or who possessed extremely positive attitudes toward society—given the current state of privacy—both generally believed there was little that could be done to safeguard personal privacy. A smaller group of respondents, who represent the center of the Resignation Curve, expressed neither extremely positive nor extremely negative views toward the state of privacy but believed there were pragmatic measures that individuals could take to safeguard their personal privacy if they chose to do so over a competing interest.

---

[89] *See* Auxier et al., *supra* note 49. Similar to this finding from our focus groups, data from the Pew Research Center's 2019 Privacy Study showed that 70 percent of participants responded that their personal information is less secure than compared to five years ago. *Id.*

[90] Focus group notes, Rutgers University (Sept. 13–Oct. 6, 2019) (on file with author).

Respondents could therefore be *loosely* placed into one of three groups along the Resignation Curve: the Defeatists, the Pragmatists, and the Futurists. Respondents do not fit neatly into only one of these groups. Instead, the groups are meant to represent sections of a spectrum. Where respondents fell on this spectrum indicates a rough approximation of their attitudes toward privacy. It is important to note that the curve depicted below does not depict the frequency with which focus group respondents could be labeled as members of each of these groups. Instead, the Resignation Curve is meant to represent a relationship between two categories of attitudes (represented by its axes), and whose extremes mark the most typical attitudes of certain typologies as outlined below.



A. *The Defeatists: Privacy Is an Illusion!*

The Defeatists' attitudes were defined by complete and total resignation—not just to an individual's inability to maintain agency over his or her privacy but also to the guaranteed negative consequences of a society that does not value privacy. Individuals on the left side of the Resignation Curve, where most focus group participants could be placed, were specifically resigned to the belief that society was now structured such that avoiding incentives to trade privacy in exchange for a variety of competing interests (security,

convenience, financial gain, etc.)[91] would impose a burden on individuals far outside what is now considered normal given the advancement of technology.

Consider visual surveillance, for example.[92] On a very basic level, it is hard to argue against the security that cameras afford over streets, university parking lots, and so many other public—and sometimes private—locales. Though one can argue about their deterrent value, few argue that the information they provide is not important to identifying culprits and so on.[93] Similarly, there is an addictive attractiveness to the use of Google's search engine. The ease, accessibility, and convenience are a brew almost impossible to resist ingesting. Related are the unbelievable efficiency rewards of technology: speed of locating accounts, storage of information, and myriad other benefits that accrue from electronic collection and storage of data.[94] Although privacy implications of different social policies have been present throughout our history,[95] the scope of the changes of the past fifty years far exceeds anything experienced in our past. The impossible has become not just possible, but a reality, and in some instances, commonplace.

Many Defeatists largely view this "new normal" as an existential threat to democracy and to the United States' ability to maintain a free and open society in which individuals retain their autonomy without the auspices of Big Brother or Big Technology watching over them.[96] Some Defeatists expressed fears that, without privacy, the country was now more vulnerable to authoritarianism, given the notion that people now fundamentally lack choice in deciding what, where, and to whom to divulge information. Any "choice" concerning whether or not to use a service or product (i.e., smartphones, search engines, mapping

---

91 *See* Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1371–78 (2017) (discussing privacy as a commodity).

92 *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1936–45 (2013) (providing a broader discussion of surveillance).

93 *See generally* Milton Heumann et al., *Privacy and Surveillance: Public Attitudes on Cameras on the Street, in the Home, and in the Workplace*, 14 RUTGERS J.L. & PUB. POL'Y 37, 60–74 (2016).

94 *See* Mike Shaw, *Why Google is the Best Search Engine (and Why Businesses Should Care)*, TOWER MARKETING (June 15, 2020), https://www.towermarketing.net/blog/google-best-search-engine.

95 *See generally* LAWRENCE CAPPELLO, NONE OF YOUR DAMN BUSINESS 6 (2019) (exploring the history of conflicts surrounding technological advancements that arguably conflicted with privacy values).

96 *See generally* Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117 (2016) (exploring the public's interest in privacy topics around the time of Edward Snowden's disclosure of National Security Agency surveillance in 2013).

applications), as one Defeatist noted, is simply an "illusion,"[97] because the cost imposed by declining to use such services places a burden on the individual outside what is now commonly deemed acceptable. While entities may not necessarily force individuals to disclose private information, the normalization of using certain technology has nevertheless forced individuals to trade their privacy.

The following is a quote from an individual near the Defeatist end of the Resignation Curve: "[N]othing I can do [about Google keeping search history] . . . . It is what it is. The individual is powerless. I'm just one person."[98] Another Defeatist summarized their feelings by asserting the following: "Privacy is an illusion. I am not sure there is a definition of privacy anymore. It is too late to make material changes in our behavior when it comes to using services like Google. We are already hooked."[99] Other Defeatists similarly reported, "I have no privacy and I can't expect it to get any better soon,"[100] and, "If you don't sign [the TOS agreement], you don't get to use the service."[101] Finally, on surveillance generally, yet another respondent stated, "There is surveillance all the time, all privacy is gone, but nothing to be done. Barring a catastrophe, there is no privacy, it's almost like a Pandora's box . . . . Get used to the new world. What can I do as an individual?"[102]

B. *The Futurists: Embrace the New World!*

Focus group respondents at both ends of the Resignation Curve shared a key characteristic: when it comes to new norms of information sharing, both Defeatists and Futurists believed that resistance is futile. Both groups are generally accepting of the "this is the way it is" mentality regarding privacy, given the advancement of technology in the 21st century. The defining difference between Defeatists and Futurists, however, is that the latter tend to believe that this new society is trending in a positive direction rather than a negative one. Futurists, unlike Defeatists, generally embrace the technology that Defeatists believe to be responsible for the decline of privacy. Of the three groups herein defined, Futurists represent the smallest number of focus group participants. They tend to not only accept the idea that society now

97 Focus Group 1 (Seniors), Rutgers University (Sept. 13, 2019) (on file with author).

98 Focus Group 3 (Young Adults), Rutgers University (Sept. 15, 2019) (on file with author).

99 Focus Group 1 (Seniors), Rutgers University (Sept. 13, 2019) (on file with author).

100 Focus Group 6 (Middle Age), Rutgers University (Oct. 6, 2019) (on file with author).

101 Focus Group 1 (Seniors), Rutgers University (Sept. 13, 2019) (on file with author).

102 Focus Group 5 (Young Adults), Rutgers University (Sept. 23, 2019) (on file with author).

values privacy less than ever before but also actively believe that the costs of trading away one's privacy are outweighed by the incentives and benefits received from doing so.

These individuals trumpeted technology's benefits, and generally believed privacy concerns were overblown, exaggerated, and more often than not theoretical musings of those far removed from reality. Futurists typically based their beliefs on the presumption that new technology brings about immense benefits for the "greater good" of society, such as heightened security, enhanced abilities to find and prosecute criminals, increased health benefits, and greater convenience in people's daily lives. Many Futurists also acknowledged that this advancement is achieved not despite the diminution of privacy but because of it. Individuals along the right side of the Resignation Curve sometimes even went as far as to champion the possibilities of mass data collection, especially in fields such as human genetics.[103] That these respondents would not only move past a general acceptance of a society dominated by information sharing but also seek to thrive in it is a testament to the wide array of opinions expressed—even by small subsections of the population—on the topic of privacy.

The more moderate of these respondents (those more toward the center-right of the Resignation Curve) felt that they had "nothing to hide," so privacy intrusions were not much of an intrusion at all. More forceful proponents said that the handwringing, dystopia-invoking voices of privacy champions were nothing more than "Chicken Littles,"[104] exaggerating the costs of technology and not crediting the enormous benefits that are associated with change. Not infrequently, these respondents threw down a challenge to the focus group: name a privacy concern that has actually materialized and affected individuals seriously and negatively. These challenges often went unanswered by other focus group respondents.[105]

The following are quotes from individuals near the Futurist end of the Resignation Curve:

> Has anyone ever suffered from these privacy concerns we are bandying about? I never did. I am happy with all that technology has given . . . . I love when the bank knows all about my accounts and alerts me to fraud. I love the fact that

103 *See generally* Natalie Ram, *Genetic Privacy After* Carpenter, 105 VA. L. REV. 1357 (2019) (analyzing privacy considerations surrounding recent advancements in genetics).

104 CHICKEN LITTLE (Walt Disney Co. 1943).

105 *See* Auxier et al., *supra* note 49. When asked if they had recently experienced three of the most common privacy harms, respondents from the Pew Study overwhelmingly answered in the negative.

> the doctor knows all about me. To be frightened is wrong . . . . Every change is for the good even if it has good and bad things . . . . What are you going to do, stay in your house the whole time?[106]

> I am not very concerned with these privacy concerns . . . by collecting more data, you get more knowledge . . . through machine learning, etc. It helps scientific progress. Every generation is faced with this [fear]. New information can be valuable . . . . We will get more benefits from AI, machine learning.[107]

Another Futurist claimed, "I have nothing to hide, so what is the problem? There are so many benefits . . . so make some concessions. I don't think we should let the negatives outweigh the positives."[108] On the topic of Google, one Futurist said, "I don't care enough to use those services [alternative to Google]. Sometimes a targeted ad is nice if it is what I am looking for."[109] Another Futurist commented, "Google is the most phenomenal thing . . . . [It is] an amazing service that adds tremendous value."[110]

C. *The Pragmatists: The Future of Privacy is . . . Different!*

The center of the Resignation Curve is occupied by a small subsection of individuals who expressed neither extremely positive nor extremely negative views toward society given the current state of privacy as they perceived it. Pragmatists, like almost all focus group respondents, also perceived societal values to be trending away from privacy. Despite perceiving this trend, however, Pragmatists themselves often still reported that they believed privacy ought to be valued and protected because of the benefits it provided—primarily those surrounding safeguarding against potential cyber-attacks that threaten an individual's financial or emotional well-being (a threat Pragmatists often took seriously). Depending on which side of the Resignation Curve members of this group fell on, Pragmatists were either cautiously optimistic or cautiously pessimistic about the direction in which society's privacy values were trending—an attitude

106 Focus Group 1 (Seniors), Rutgers University (Sept. 13, 2019) (on file with author).

107 Focus Group 2 (Middle Age), Rutgers University (Sept. 15, 2019) (on file with author).

108 Focus Group 6 (Middle Age), Rutgers University (Oct. 6, 2019) (on file with author).

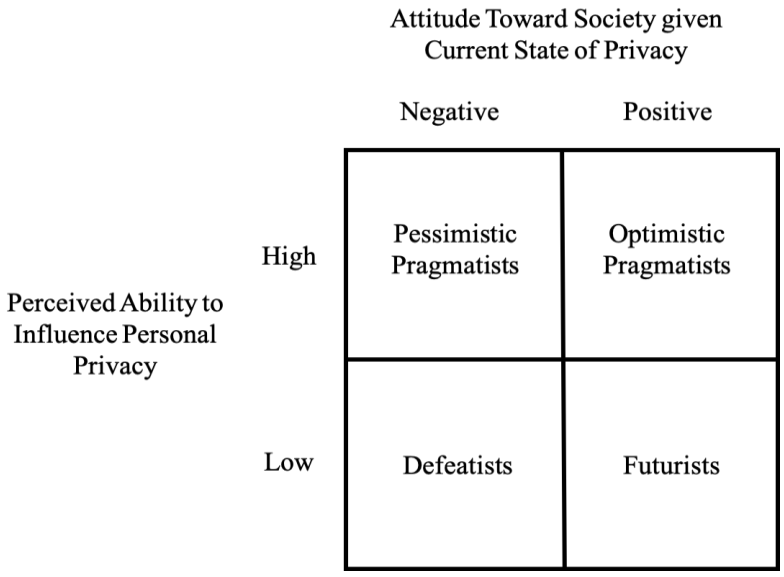
109 Focus Group 5 (Young Adults), Rutgers University (Sept. 23, 2019) (on file with author).

110 Focus Group 4 (Seniors), Rutgers University (Sept. 20, 2019) (on file with author).

that was largely tied to a Pragmatist's belief in the extent to which other individuals also realized their individual agency over protecting their personal privacy.

The following diagram illustrates how the cross section of certain attitudes affects where an individual is placed along the Resignation Curve. This depiction also distinguishes between Negative Pragmatists (those on the left side of the curve) and Positive Pragmatists (those on the right side of the curve). As previously stated, there was a subtle difference in the attitude Pragmatists took toward their general feelings about society given the current state of privacy as they perceived it. The defining characteristic within this group was an individual's perception as to whether or not others also believed that they had individual agency to affect their personal privacy. Many Pragmatists were optimistic as to the agency of their peers, while others believed that they were alone in their ability or willingness to either resist privacy tradeoffs or take certain measures, as explored below, to mitigate the collection of their data.

Resignation Curve Typologies



Unlike their peers at either end of the Resignation Curve, Pragmatists cited a variety of ways—to various extents of personal usage—that individuals could actually use technology to their benefit in protecting personal privacy. This included practices such as private browsing (a means of hiding users' cookies, the mechanism through

which websites track user traffic), VPNs (which allow individuals to create secure networks to access the internet), and encryption (a tool used to restrict information access). Knowledge of any one of these technologies varied widely among even the Pragmatist group, and many respondents—especially younger ones—reported that they were aware of such methods to protect individual privacy, but did not actively utilize these methods themselves, mostly due to a lack of technical knowledge. Despite this fact, the mere existence of such technologies suggested to the Pragmatists that perhaps a world devoid of privacy was not inevitable, although many remained skeptical that enough people cared enough, especially given tantalizing tradeoffs, or had the technical knowledge to actually use such privacy-protecting technology ("PPT"). For the Pragmatists, even among those who actively engaged with PPT, the widespread use of PPT was a necessary step if the protection of private information were to ever extend beyond small clusters of privacy-concerned individuals.

The following are quotes from Pragmatists, near the apex of the Resignation Curve: "I can choose: do I want to share [information], or do I not want to share?"[111] "I use DuckDuckGo instead of Google because they respect my information."[112] Two Pragmatists highlighted the moral duality of technology: "Every technology can be used for good and evil . . . . Encryption is a secure way of storing information."[113] "The future of privacy is different. Not bad or good necessarily—just different."[114]

VI. CONCLUSION: REFRAMING PRIVACY'S MEANING

The last question we asked focus group participants concerned the future of privacy. We tasked each group to describe, in just a few short words, what they expected from this future. While the responses varied, the most cited phrase associated with privacy's future was "meaningless." It is noteworthy that this word was used not just by Defeatists who were dismayed by a future without privacy but by the Futurists who championed the benefits of this new world as well. Across the Resignation Curve, nearly every person cast doubt on the

111 Focus Group 1 (Seniors), Rutgers University (Sept. 13, 2019) (on file with author).

112 Focus Group 5 (Young Adults), Rutgers University (Sept. 23, 2019) (on file with author).

113 Focus Group 6 (Middle Age), Rutgers University (Oct. 6, 2019) (on file with author).

114 Focus Group 6 (Middle Age), Rutgers University (Oct. 6, 2019) (on file with author).

meaning or purpose that privacy might play in an increasingly digital society.

We have already discussed literary, philosophical, and legal conceptions of privacy at length.[115] Upon reflecting over the totality of the data we gathered, however, it is worth emphasizing a phenomenon also discussed by Solove in *Nothing to Hide*: the lack of a prevailing consensus around any single conception of privacy or its alleged values.[116] This may seem strange given the final responses of our focus group participants—how could individuals lament (or even celebrate) the loss of privacy's meaning, when that meaning was never entirely clear in the first place?[117]

The notion that privacy conceptions are rather ephemeral and amorphous in practice is supported by our focus group participants, who often struggled to give coherent responses when asked what the term "privacy" meant to them.[118] It was not until these individuals were further prompted that they could even attempt to outline any values placed on privacy, and they did so primarily by identifying the types of information they sought to keep private. Even the value of privacy respondents assigned to these types of data was purpose-specific and was not generally associated with higher ideals involving privacy itself. For instance, for the most commonly cited categories—financial and health data—respondents explicitly sought to keep this information private because of fears over potential financial loss over the exposure of that data.

Among the variety of responses on this topic, however, focus group respondents constantly raised one theme, if not a clear definition. In every focus group, the theme of control over one's personal information—or more commonly, the lack thereof—was cited in discussions of respondents' conceptions of privacy.[119] Although these discussions often also boiled down to a simple "feeling," that feeling was undoubtedly the sense of being in control over one's personal information; irrespective of whether or not a respondent was accepting of his or her information being shared, he or she wished to have a say in that decision. Upon reviewing these responses and their implications within the larger context of privacy in the US and abroad, it became clear

115 *See supra* Part II.

116 *See* SOLOVE, *supra* note 42, at 24–26.

117 *See generally* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002) (discussing changing conceptions of privacy over time).

118 *See infra* APPENDIX A

119 *See* Auxier et al., *supra* note 49. Similar to our findings here, data from the Pew Privacy Study showed that respondents' conception of privacy is heavily skewed toward the idea of control over their personal information. *Id.*

that reconceptualizing privacy around a more nuanced notion of control may be a worthwhile thought experiment to conclude our exploration of privacy in the public eye.

A. *Condition vs. Choice: The Privacy Paradox*

Reconceptualizing privacy around the concept of personal choice provides a new resolution to a paradox surrounding the left half of the Resignation Curve.[120] Defeatists lament their loss of privacy while simultaneously sharing their information with Google, Facebook, Amazon, etc. Many Defeatists themselves attribute these inconsistencies to an overwhelming feeling of resignation: with privacy having "lost its meaning," many respondents have succumbed to the benefits of exchanging privacy for a variety of tradeoffs. Although nearly all respondents agreed that these tradeoffs had immense value, many—especially the Defeatists—felt as though they did not always retain control over which tradeoffs to make and the extent to which their own privacy should be exchanged for the corresponding benefits. It is quite possible that when respondents lamented their loss of privacy, they were actually lamenting their diminished control over the decision to be private (or not), rather than the actual state of being private itself.

One could argue that individuals still retain complete control over whether or not to share personal information. Our TOS agreement discussion,[121] however, serves as a counterargument to that belief. On paper, it would seem that the free market grants individuals seemingly limitless choices as to which data-collecting services to use, if any at all. Indeed, many would likely point to the ability of privacy-concerned individuals to abstain entirely from these services as justification for their claim that people still retain some level of control over their private information. Irrespective of the realistic feasibility of total abstention, the perception our focus group respondents held was clear: respondents felt as though they had no choice but to use certain products—such as Google's search engine—and to agree to its TOS contract. Respondents articulated that abstention from interfacing with any internet services would preclude them from participating in society as the average person would. It is this *feeling*—the belief that one must agree to TOS contracts or face societal ostracism—that is central to privacy's loss of meaning in the public eye.

---

120 *See supra* p. 1443.

121 *See supra* Part IV.B.

As surfaced at the beginning of each of our focus groups, respondents' relationship to privacy was defined not by privacy itself but by its competing interests. In the eyes of many respondents, the compelling nature of these tradeoffs has essentially forced their hands in a variety of situations, thereby eliminating any feeling of control over their information. Although technology has provided a new impetus for this exchange in the twenty-first century, individuals' desire to trade privacy for a competing interest is by no means a new phenomenon. In *None of Your Damn Business*, Lawrence Capello provides evidence that Americans were willing to exchange privacy for competing interests as early as the Gilded Age.[122] In his analysis, Capello argues that the current state of privacy was not the inevitable result of technological progress, outlining several key moments throughout American history in which privacy was placed against a competing interest—and lost.[123] This analysis appears to reveal an unspoken truth: maybe individuals never truly cared about the actual state of being private or anonymous.

While it may be difficult to gauge public sentiment in the past, it may very well be possible that the loss of privacy's meaning today can be attributed to the romanticization of a privacy-devoted world that never existed. In this world, everyone chose anonymity without the fear of missing out. In actuality, there were simply fewer opportunities to exchange privacy for competing interests in the past when compared to the opportunities that exist today, due in large part to the advancement of consumer technology. Previous conceptions of privacy, therefore, did not have an impetus to distinguish the state of being private with the decision to be private, for this was once a distinction without a difference. Today, however, shifting emphasis to the latter distinction could potentially provide a privacy framework that accounts for individuals' desire for agency over their personal information, while also acknowledging their desire to occasionally share that information.

To speak in terms of our frog metaphor, who could blame people for wanting warm water? For as a Futurist may claim, society has now been ushered from a technological ice age into a paradise of information enlightenment. Older conceptions of privacy, such as Westin's, which rely heavily on promoting the benefits of anonymity as a principle component of privacy, may seem somewhat tone-deaf in a world where over two billion individuals have Facebook accounts.[124] These previous

122 CAPELLO, *supra* note 95, at 5–6.

123 *Id.* at 3–4.

124 J. Clement, *Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2019*, STATISTA (Jan. 30, 2020), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide.

conceptions, which focus more on the condition of being private rather than the choice to enjoy that condition, are perhaps incompatible in a world defined not by what is withheld but by what is shared.[125] From this perspective, it is unsurprising that respondents were unable to describe what exactly privacy meant to them, largely because traditional conceptions of privacy, which emphasize anonymity, are not easily compatible with individuals' willingness and desire, in some instances, to share their information.

This inability to reconcile contemporary norms with amorphous conceptions of privacy based on anonymity may be one reason individuals feel a lack of control. Because traditional definitions of privacy emphasize the actual state of being private rather than the decision to retain that state (to whichever extent one chooses), individuals may tend to conceptualize sharing-abstinence as a more legitimate form of privacy instead of seeking out responsible ways to share information.[126] This feeling of not having control is likely furthered by the need to seek out these responsible means rather than having them implemented as a legislative standard.[127]

B. *What's the Point? The Purpose of Privacy*

Advocates who champion privacy as an important part of human dignity may criticize a conception of privacy that de-emphasizes the actual condition of being private. Political theorists such as Westin, for instance, have specifically cited the anonymity granted by privacy as a contributing factor in securing a person's dignity.[128] But fears that a model of privacy based around sharing, rather than withholding, would undermine individuals' ability to maintain their dignity are undoubtedly unfounded for two reasons: the lack of association between privacy and dignity, and the dignity that is still maintained through choice.[129]

---

125 *But see* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1906 (2013) (providing an alternative analysis that argues in favor of older conceptions of privacy).

126 For example, limiting which smartphone applications have access to certain kinds of data (i.e., location, Bluetooth, etc.), or restricting the ability of software to access data altogether.

127 For example, the European Union and California have implemented measures that may assist in granting users greater control over their data. These measures are further explored in a later section. *See infra* Section VI.B.

128 WESTIN, *supra* note 11.

129 *See* Auxier et al., *supra* note 49. A majority of participants within the Pew Privacy Study responded that the developments of new tools allowing for individuals greater control over their personal information would be a more effective way to protect their personal information. *Id.*

Throughout the focus groups, the purpose of privacy was discussed at great length. Many, but not all, respondents cited the benefits that privacy offered in terms of protecting against potential harms,[130] such as identity theft or other forms of financial loss. Hardly any respondents reported that they believed privacy was an end in and of itself. No respondents offered "human dignity" as a potential value of privacy that could compete against other interests such as convenience or security.[131] The closest the discussion came to this topic were the instances in which individuals expressed concerns of government eavesdropping, but even then, these concerns were also met with "I have nothing to hide" claims from many other respondents. Almost all respondents acknowledged, and even accepted, that today's society is defined more by a cost/benefit calculation than it is insisting on the primacy value of human dignity.

This is not to claim that rhetoric surrounding human dignity has no place in a new conception of privacy. Instead, the lack of salience of the human dignity justification for privacy provides evidence as to why privacy has been so heavily eroded in the United States. One reason privacy may have lost the battles outlined by Capello[132] could be that the human dignity element of remaining anonymous was never that compelling to Americans, and given the advent of new technology and limitless information sharing, perhaps the human dignity argument is now less compelling than ever. This is especially true given the ties between traditional conceptions of privacy, human dignity, and anonymity, or "the right to be let alone."[133] To the extent that humanity wishes to share more information than ever before, it is perhaps unsurprising that these arguments have not supported privacy throughout the history of the United States.

Instead of associating human dignity with anonymity under older conceptions of privacy, dignity ought to instead be tied to choice. It is the ability to decide whether or not to be private, and the extent thereof, that provides individuals with a sense of self-respect and worth, rather

130 An interesting point of contention from the focus groups was the extent to which these harms were actually realized. While many focus group respondents used services that, at one point, have been electronically compromised in some way, only a few respondents cited cases in which they felt personally victimized by some violation of their privacy due to a company being hacked or otherwise storing data in an unsecure fashion. The extent to which these harms are unrealized may contribute to claims that privacy concerns are often taken out of proportion.

131 *See generally* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1164–70 (2004) (comparing the United States' emphasis on liberty to European emphasis on dignity for issues involving privacy).

132 CAPELLO, *supra* note 95, at 6.

133 Warren & Brandeis, *supra* note 7, at 139.

than the actual decision itself. For instance, a person who elects to enjoy all of the competing interests of privacy at the cost of sharing their personal information retains no more or less dignity than a person who chooses to share nothing—so long as both individuals had the choice of deciding.

Of course, creating and maintaining this choice is much easier said than done. It may be tempting to identify the Pragmatist group of the Resignation Curve[134] as the set of individuals who best exemplify this new conception of privacy. After all, these were the respondents who had already begun to take measures[135] with the hope of having better control over access to their private information. Despite this observation, we would caution against turning Pragmatists into normative role models for other individuals in society if a robust conception of privacy is to be preserved. The true takeaway from the Pragmatist section is the type of behavior that flourishes due, in large part, to the absence of other privacy protections. Perhaps these individuals would be less inclined to engage with technologies that grant them greater control over their privacy if they believed that this control could be easily exerted through other means, such as legislative provisions that compel companies to implement such controls into their services.

Certain jurisdictions have actually sought to implement legislation designed to grant their constituents greater control over their personal data. The European General Data Protection Regulation (GDPR), which took effect in the European Union (EU) in May 2018, aims to protect *all* residents of the EU, meaning anyone living in the region falls under the same protective umbrella as citizens.[136] To achieve this goal, all companies with an internet presence in the EU must comply with its regulations, including American businesses that have European websites.[137] A second fundamental change resulting from this

134 *See supra* p. 1443.

135 *See supra* p. 1448.

136 Juliana De Groot, *What Is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019*, DIGITAL GUARDIAN (Sept. 30, 2020), https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection.

137 While companies may have implemented certain measures worldwide, GDPR provisions only protect EU residents. Aarti Shahani, *3 Things You Should Know About Europe's Sweeping New Data Privacy Law*, NPR (May 24, 2018), https://www.npr.org/sections/alltechconsidered/2018/05/24/613983268/a-cheat-sheet-on-europe-s-sweeping-privacy-law (stating that U.S. citizens are not necessarily entitled to the same protections afforded to EU residents: "[i]n Europe, Facebook has to get permission to do facial recognition—and it's not the default setting. But in the U.S., it is. American users have to click through screens to opt out").

legislation is an alteration in the definition of "personal data," and, accordingly, what data are included in these protections.[138] Some examples of categories of data not previously included are what you post, electronic medical records, mailing addresses, IP addresses, and GPS locations—all of which are now included as protected data.[139] These foundational alterations are crucial in understanding the legislation's greater implications, as they alter previously caste-in-stone beliefs about what "should" or "should not" be considered private.[140]

The GDPR contains several provisions designed to grant internet users greater control over their privacy. For instance, to comply with the GDPR, all companies must conform to an opt-in style of data collection for any online services that track users' information, with the goal of encouraging increased awareness of and transparency regarding the information being collected on the part of users themselves.[141] Furthermore, the GDPR empowers EU users to request that companies delete personal data they collect "without undue delay" or face potential penalties under the law.[142] Other critical components of this legislation include: "[r]equiring the consent of individuals for data processing[;] [a]nonymizing collected data to protect privacy[;] [p]roviding data breach notifications[;] [s]afely handling the transfer of data across borders[;] [and] [r]equiring certain companies to appoint a data protection officer to oversee GDPR compliance."[143] This provides consumers an enormous amount of control over their data compared to the "wild west" of the internet as it had previously existed in Europe, and as it continues to exist throughout much of the United States, with some notable exceptions.[144]

138 *Id*.

139 *Id*.

140 *See* Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2033–39 (2013) (discussing the potential implications of these new privacy classifications).

141 Shahani, *supra* note 137.

142 *Id*.

143 Juliana De Groot, *What Is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019*, DIGITAL GUARDIAN (Sept. 30, 2020), https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection.

144 *See generally* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 786–87 (2019) (comparing the GDPR with other legislative approaches taken around the world, primarily in Japan and the United States).

California presents what is likely the most notable of these exceptions. As of January 1, 2020, California's Consumer Privacy Act (CCPA) provides California residents[145] with access to enhanced knowledge and control over their personal data. Inspired by the GDPR,[146] the CCPA provides California residents with rights to the following: (1) to know what personal data is being collected about them, and by whom; (2) to know whether their personal data is being sold or otherwise disclosed, and to whom; (3) to refuse to the sale of their personal data; (4) to regain and curb access to their personal data; (5) to request businesses to delete any personal data that they may have collected; and (6) to not face discrimination for exercising their right to privacy.[147] The CCPA also provides California residents with legal standing to bring suit against any qualifying company that violates these provisions.[148]

Importantly, both the GDPR and CCPA comport with the aforementioned new conception of privacy, as they do not seek to restrict the quantity of information that companies can collect but instead aim to give individuals greater awareness and control of their personal information.[149] Given the laws' recency, it remains to be seen what effect, if any, these pieces of legislation will have on the individuals' behavior or general attitudes toward privacy. At the very least, the GDPR and CCPA illustrate the potential influence that governments can wield in safeguarding their citizens' capacity to control private information.[150] This influence, however, can work both ways.

---

145 The provisions of the CCPA apply to all residents of California, and restrict any business, nonprofit or for-profit entity that collects personal data of consumers, conducts business practices in the state of California, and is characterized by at least one of three "thresholds.". CAL. CIV. CODE § 1798.140 (2018). These thresholds include having a gross annual revenue of $25 million or more, having the ability to buy or sell the information of 50,000 or more individuals or separate households, and/or earning 51% or more of its gross annual revenue from data selling. *Id.*

146 Although they share many similarities, there are several differences between the two pieces of legislation. The most notable is that the CPPA protects data that originated from the consumer directly, while the GDPR extends protections to cover data purchased by third parties as well. Nicholas Moline, *2019 Changed the Internet Forever*, JUSTIA (Jan. 3, 2020), https://onward.justia.com/2020/01/03/2019-changed-everything.

147 *See* CAL. CIV. CODE § 1798.100 (2018).

148 For further discussion of the origins of CCPA and GDPR, see Anupam Chander et al., *Catalyzing Privacy Law*, 105 MINN. L. REV. (forthcoming 2019).

149 Nicholas Moline, *2019 Changed the Internet Forever*, JUSTIA (Jan. 3, 2020), https://onward.justia.com/2020/01/03/2019-changed-everything.

150 *Contra* Woodrow Harztog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1696–97 (2020) (providing an alternative analysis of GDPR, especially its potential shortcomings if similar legislation is applied in the United States).

The most glaring case of government influence working against privacy deserves special mention—China. Today, technology is being deployed in the Chinese mainland to increase control over the population under the guise of keeping civil order and promoting moral norms, with the most common systems being facial recognition coupled with large-scale data collection.[151] Approximately 300 million facial recognition cameras are being installed in train stations, at crosswalks, on light fixtures, traffic signals, and buildings.[152] Furthermore, pilot testing for a social credit system is already taking place, in which the government assigns credit scores to citizens based on their personal habits and the scores of their associates. The Chinese government uses those factors to indicate the presence of traits the Chinese Communist Party finds desirable in its citizens.[153] Currently, these pilots are facing technical barriers due to the sheer amount of data that must be processed,[154] but this is a limitation that may not exist one day—possibly soon.

The aforementioned developments do not stop at China's borders. Already, Chinese firms are working with foreign governments to spread facial recognition technology. Eighteen countries[155]—including Zimbabwe, Uzbekistan, Pakistan, Kenya, the United Arab Emirates, and Germany—are using Chinese-made monitoring systems.[156] Chinese technology is expanding past Chinese borders,[157] so Americans face the question of whether such a system could exist here, and what it may look like. This may boil down to cultural questions and tolerance for privacy invasions on a national level, but these are questions that people must ask while they still can.

An old adage states, "knowledge is power." We now live in an information age with nearly limitless information available—but not information all possesses equal value. Whether the end goals of companies or governments are commercial gain or societal power, the

151 *China Invents the Digital Totalitarian State*, ECONOMIST (Dec. 17, 2016).

152 *Id.*

153 Mareike Ohlberg, Shazeda Ahmed, & Bertram Lang, *Central Planning, Local Experiments: The Complex Implementation of China's Social Credit System*, MERCATOR INSTITUTE FOR CHINA STUDIES (Dec. 12, 2017).

154 *Id.*

155 Paul Mozur, Jonah M. Kessel & Melissa Chan, *Made in China, Exported to the World: The Surveillance State*, N.Y. TIMES (April 24, 2019). Thirty-six countries have received training in topics such as "public opinion guidance . . . which is typically a euphemism for censorship." *Id.*

156 *Id.*

157 Amy Hawkins, *Beijing's Big Brother Tech Needs African Faces*, FOREIGN POL'Y (July 24, 2018), https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces.

collection of personal data has proven to be among the most valuable information that exists today in achieving these ends. Understanding the value of this information and deciding for oneself what to do with it—whether to enjoy a state of privacy or the seemingly endless benefits of exchanging information (or to exist somewhere in between)—is among the greatest challenges for humanity in the age of information.

To refer once again to our Frogs analogy, the amphibians perhaps need not make the water cooler again—for that would be difficult to convince others to do, and even those that might have once preferred colder water now enjoy the warmth. Rather, the solution is to ensure that they themselves have their hands on the faucet, ever vigilant of reaching the boiling point.

APPENDIX A: GENERAL SCRIPT/QUESTIONS FOR FOCUS GROUPS

Hello all, and thank you for participating in our study! We have been exploring the idea of a "right to privacy" amongst ourselves, and we are excited to hear opinions on this topic from people outside of our team. Our goal is to be able to initiate a conversation, through which we will be able to hear each of your viewpoints about privacy and related issues. We hope that you find this conversation as intriguing as we do, and please feel free to interject with opinions, thoughts or questions at any time.

- Like (previous person) just mentioned, we'd like to start by asking very broad questions. For starters, the word privacy has many different meanings to many different people. We hear the word "privacy," but specifically what does privacy mean to you?
- Additionally, which information do you consider private?
- So let's say right now I want to know the male to female ratio at Rutgers. How would you find out this answer for me?
- So we've all used Google before, and you just did this search. Something interesting that we found was that you automatically agree to Google's terms and services agreement. Were you aware of that?
- How do you feel about it? Some people tend to feel uncomfortable; some people think it's fine. How do you feel? Why?
- There's some people who want these terms and conditions to be up front, ask permission type; some are fine with the way Google's terms are. How do you feel about this?
- How often would you say you read the terms and services agreements? Why?
- How do you feel about terms and services agreements?
- Do the terms and services agreements ever change whether or not you use that service? Like, would you stop using Google and use, say, DuckDuckGo because the TOS changed?
- What are your impressions of these documents? How would you describe them?
- Companies tend to reserve the right to change their TOS whenever they like, so they'll change it midyear and then notify you that "we have updated our Terms and Services agreement." How do you feel when this happens?
- There are sites where when you click on them, they have a popup saying "by using our website you agree to our terms and services." Do you prefer this kind of consent, or do you prefer manually clicking yes?

- What do you feel about websites that have the popup? Do you like it when that happens? Or would you rather they not bother?
- Do you have social media? So let's take social media and location services. A lot of social media will ask permission to collect location data and see where you've been. And it enables a few things, like your Lyft being able to find you or your friends being able to know where you took that photo. Do you have that enabled?
- How do you feel about companies having that information?
- What are all the ways you think companies use data? What are all the ways you think they get this data?
- Would you rather pay for services like Google or Facebook, or is the current system better in your opinion?
- Where do you think permission will go in the future? Do you think companies are going to be more or less likely to ask permission?
- Do you think you'll be giving up more or less information in the future?
- What is consent, and how/when should it be given?
    - Must it be explicit?
    - Can it be coerced?
- Next, we'd like to talk about a more specific form of consent, the type of consent that certainly occurs between companies and individuals, but also a type of consent that may commonly occur between private individuals themselves. The type of consent we would now like to discuss involves individuals being recorded.
- For individuals recording other individuals, there are mainly two schools of thought:
- Eleven states, including California, have adopted two-party consent laws for recording conversations. Two-party consent laws require both parties to agree to the recording of a conversation. How do you feel about this?
- New Jersey is one of the other thirty-eight states which requires only one party to have knowledge of a recording. Do you tend to favor this?
- If you believe in one-party consent, what are some reasons why you might see the benefits of two-party laws?
- If you believe in two-party consent, what are some situations in which one-party consent may prove beneficial?
- Even amongst our group, there is disagreement about consent in extreme cases, such as a battered woman recording her abusive husband. Do you see a conflict

between the values of, for example, safety and that of privacy?

- Should *all* recorded conversations be admissible as evidence in court? How about in order to obtain a warrant for arrest? What about to prove wrongdoing at the workplace or in an academic environment?
- Suppose the police suspect that you are plotting to commit a heinous crime. They are seeking information from your phone that may connect you to this crime. They want access to such data as your messages, your email, your photos, and your location data. We are curious about the level of difficulty that law enforcement will encounter in obtaining your data. My first two questions concern ***your belief*** about the way the world currently works in this area. The questions I will ask after concern how you believe the world ***should*** work, according to your opinion.
- Which data from your phone ***do you believe*** will be easiest for the police to obtain?
- Which data from your phone ***do you believe*** will be the most difficult for the police to obtain?
- Which data from your phone ***should be*** the easiest for police to obtain? Why?
- Which data from your phone ***should be*** the hardest for police to obtain? Why?
- Good afternoon! I've been looking into different aspects of privacy, and how the expectations of which may vary depending on the type of information and the different companies or organizations that may be collecting it. To do this, I'm going to ask you all a series of simple A or B questions, for which I ask that you choose one of the two options. We will do this anonymously, and I ask that you all close your eyes and raise your hands (yes, we're going back to elementary school voting here). I will present the two options to you, and then ask you to raise your hands for each option. Ready?
    - Who do you trust more (more comfortable with knowing):
        - NSA or Facebook
        - Post office or Amazon
        - FBI or Google
        - FCC or Verizon
        - Treasury or credit card companies
    - Would you rather have the govt or a private company knowing:
        - your credit card info
        - your location at all times

        - your call history
        - who you associate with
        - what you purchase
        - where you've been sleeping
        - your political leanings
- Quick recap/explanation of votes above
- General recap of conversation/entire group: What do you think privacy will look like in the future?
    - Why do you think so?
    - Can you describe this in one word?

APPENDIX B: RESPONDENTS' ONE-WORD DESCRIPTIONS OF PRIVACY IN THE FUTURE

Focus Group I (Seniors)

- We will get used to drinking the poison.
- We will be more aware of it, but it isn't going to get better.
- We are more aware of it. We're more careful. Is it better? Probably not, but we're more aware now.

Focus Group 2 (Middle Age)

- Scary, unknown
- Unknown but we are catching bad guys
- Uncontrolled
- Uncontrolled and concerned
- Not sure if liberal democracy will balance against authoritarian dystopia and terrible stuff
- More complex in the future; privacy means different things
- Positive about the future—we will work out the issues
- Going in a negative direction

Focus Group 3 (Young Adults)

- Will be no privacy
- Declining
- Fine
- Non-existent
- Non-existent
- Minimal
- Functional
- Regulated

Focus Group 4 (Seniors)

- Gone
- Gone
- Okay
- Unknown
- Vanishing
- Safeguards will be enlarged
- Fragile
- Precarious—"thank goodness we are of the age that it is not going to be our problem"

Focus Group 5 (Young Adults)

- Some or none
- Definition of privacy will change twenty years from now. There will be a different technological environment. We are a transitional generation. There will be ramped up technology.
- The term 'privacy' will lose its meaning. In twenty years we will say, "what is privacy?" It will just get lost, be

meaningless. With more sophisticated technology, privacy will be meaningless.

- Even though privacy is decreasing, most of the public knows this, and therefore may become more protective [with respect to government and private corporations and privacy]. The fact that people realize they are being watched/located may lead to more policies.
- Meaningless
- Meaningless but will still want privacy
- Less privacy
- Declining
- Diminishing
- Unknown

Focus Group 6 (Middle Age)

- Scary—going down slippery slope where all know about me
- Very different
- Unimaginable
- Precarious
- Interesting
- Real—more and more we'll accept the changes as they're inevitable.