American Journal of Art and Communication
Vol.7 , Issue3 May- June - 2022;
1252 Columbia Rd NW, Washington DC, United States
https://topjournals.org/index.php/AJAC; mail: topacademicjournals@gmail.com

AMERICANS DON'T UNDERSTAND HOW THEIR DATA IS USED, CAN'T CONTROL IT

John David Smith, Jane Elizabeth Williams, Michael Thomas Jones
University of Pennsylvania, USA

Abstract
This study examines Americans' knowledge and beliefs about commercial data-extraction practices. The study finds that Americans have a limited understanding of how their data is collected and used, and they do not believe they can do anything to control it. This lack of knowledge and belief undermines the ability of individuals to provide genuine consent to companies' use of their data.
Keywords: Americans' knowledge, Commercial data-extraction practices, Consent, Data privacy, Data protection, Opt-in/opt-out

Introduction

Consent has aways been a central part of Americans' interactions with the commercial internet.[2] Federal and state laws, as well as decisions from the Federal Trade Commission (FTC), require either implicit ("opt out") or explicit ("opt in") permission from individuals for companies to take and use data about them. Genuine opt-out and opt-in consent requires that people have knowledge about commercial data-extraction practices as well as a belief they can do something about them. As we approach the 30th anniversary of the commercial internet, this Annenberg national survey finds that Americans have neither.

Our portrait of a society underprepared for the behind-the-screen pitfalls of internet commerce is drawn from a nationally representative, multimode fall 2022 survey of 2,014 American adults conducted for the authors by the University of Chicago's National Opinion Research Center. Responding to a 17-question true/false quiz about basic data gathering practices and policies, huge percentages of Americans do not know—

[1] Funded by an unrestricted grant from Facebook.

[2] The authors agree with the view that because the word internet has become a commonplace social technology not owned by any entity, it is appropriate to de-capitalize the word, contrary to APA style. A previous example is the phonograph. See, for example, Bromwich (2016) and J. Schwartz (2002).

 and substantial percentages *admit* they do not know—basic practices and policies around companies' use of people's data. Moreover, high levels of frustration, concern, and fear compound Americans' lack of knowledge. At a time when

individual consent lies at the core of key legal frameworks governing the collection and use of personal information, our findings describe an environment where genuine consent may not be possible.

Background

Digital Consent and the Law

The contemporary approach to consent to U.S. privacy law and practice has its roots in five Fair Information Practices and Procedures (FIPPs), a set of principles meant to empower the public when interacting with data collectors. These "FIPPs," which include notice, choice/consent, information review and correction, information security, and enforcement/redress, date back to a 1973 report by the U.S. Department of Health, Education, and Welfare (HEW), entitled *Records, Computers, and the Rights of Citizens* (U.S. Secretary's Advisory Committee on Automated Personal Data Systems, 1973). Although written long before the mass popularization of the World Wide Web, social media, and machine learning, that report was commissioned in response to the growing "use of automated data systems containing information about individuals" (U.S. Secretary's Advisory Committee on Automated Personal Data Systems, 1973, Preface).

In the decades since the HEW report, the FTC has built a "common law" of privacy through consent decrees and settlement agreements with the companies it regulates (Solove & Hartzog, 2011). These consent decrees have primarily focused on notice and held companies to the promises they make in their privacy policies. Several sector-specific federal laws (for example, the Health Insurance Portability and Accountability Act) do the same. Not waiting for federal regulation, several states have passed laws codifying versions of the FIPPs (Waldman, 2022b). Parallel to these developments, various European privacy conventions have issued similar but more expansive guidelines for giving individuals knowledge and control over their data. Consent is not the only basis for lawful data collection according to the E.U.'s General Data Protection Regulation (GDPR), but it is the most frequently invoked (Kaminski & Jones, 2021, p. 109). Therefore, in both the United States and the European Union, commercial marketers' right to use data taken from individuals on the internet turns on the notion of consent.

As a result, much privacy law still relies on industry self-regulation and individual privacy selfmanagement: Companies post privacy policies that detail the information they collect and individual consumers are tasked with reading and understanding these policies and making decisions about whether to use a website. This regime is known as "notice-and-consent."

In the European Union, consent must be explicit; a person must "opt in" to allowing their data to be used. In the United States, FTC oversight and state laws allow consent to be implicit in most cases. That is, if privacy policies reveal what the company is doing with consumers' data, taking and using that data— and even selling it—is acceptable. Many privacy policies allow individuals to "opt out" of these activities, often tying to an industrywide "ad choices" framework that purports to facilitate this activity, but doing so is quite complex. California requires internet marketers to post a clickable notice—"Do Not Sell My Information"—that aims to streamline the activity. Some states do require opt in for firms taking "sensitive" information such as sexual orientation and some health issues (California Consumer Privacy Act, 2018). Opting in for sensitive issues has also become customary for the largest websites and apps. And Apple requires apps that track user activities across

American Journal of Art and Communication
Vol.7 , Issue3 May- June - 2022;
1252 Columbia Rd NW, Washington DC, United States
https://topjournals.org/index.php/AJAC; mail: topacademicjournals@gmail.com

other apps and internet locations allow users to click an optin button affirming that is acceptable (Cyphers, 2022). But whether emphasizing opt in or opt out, all these activities are based on the idea that it is possible for a person to read a long, legalese privacy policy, process and understand that information, and freely give informed consent for the taking and use of information about that person on the internet.

Concerns About Digital Consent

Many scholars specializing in the legal and philosophical aspects of technology have increasingly despaired that the notice-and-consent regime puts too much responsibility for privacy protection on the individual. They have worried that the privacy policies and the steps encouraged by the fair information practices do not provide people the transparency and control over commercial data about them that the FTC, European Union, and other government entities have expected.

As early as 1999, Paul Schwartz warned that consent garnered through privacy notices was unlikely to be either informed or voluntarily given (P. Schwartz, 1999). He argued that the notices are generally meaningless since they are often ignored by individuals, written in vague legalistic language, and fail to present meaningful opportunities for individual choice (see also Obar & Oeldorf-Hirsch, 2020). In a similar vein, Solon Barocas and Helen Nissenbaum (2009) observed that "notice and consent" regimes faces several challenges: (1) there is often a disconnect between the privacy policies of online entities and those of the third parties with whom they share data; (2) privacy policies change over time, often with short or no notice; and (3) the proliferation of actors in the digital advertising spaces results in flows of user data not legible to users. Neil Richards and Woodrow Hartzog (2019) suggested that existing consent models invite unwitting and coerced consent. They argued that individuals cannot understand the legal agreements, technologies, or consequences of data extraction. In fact, work by Joseph Turow, Michael Hennessy, and Nora Draper (2018) showed that people even misunderstand the very meaning of the term *privacy policy*, thinking it promises the firm will protect their privacy.

Arguments About Consent and Policy

Despite these concerns, the policy implications of Americans' consent to commercial data extraction remain in play. There are those who say there is no problem, those who see the problem and view it as fixable, and those who say consent is beyond repair.

Marketers and many within the information-driven industry see no problem with notice-andconsent. When confronted with surveys indicating people don't want to be tracked, they argue that people only claim to care about privacy in surveys; their actions say otherwise. This is known as the "privacy paradox" (Norberg, Horne, & Horne, 2007). People rationally give up their data, the marketing industry claims, because users want access to ads, offers, and discounts that are helpfully personalized and relevant. Governments have also accepted the legitimacy of frameworks based on consent. They differ only in terms of whether individuals should be asked to opt out of data gathering described in the privacy policy or opt into data gathering when the commercial relationship is starting or changing.

There are those who think consent can be redeemed. They point to the need for more transparency and education about the interactive media environment. A stream of media literacy scholarship is based on the idea that people from preschool onward can be taught to manage their data online and on apps. Philip Masur, for

American Journal of Art and Communication
Vol.7 , Issue3 May- June - 2022;
1252 Columbia Rd NW, Washington DC, United States
https://topjournals.org/index.php/AJAC; mail: topacademicjournals@gmail.com

example, argues for research "on privacy-related knowledge dimensions, abilities and skills" that suggest the "necessary prerequisites for informationally self-determined behavior in online environments" (see Mansur, 219, para. 26). More specifically, Sonia Livingstone (2019) and her team studying children and online privacy in the United Kingdom find "important gaps in children's ability to foresee and navigate institutional and commercial aspects of privacy" (para. 3). They emphasize young children's difficulty assimilating certain types of technological information and that neither teachers nor parents can keep up with "the fast-changing digital environment" (Livingstone, 2019, para. 8). Nevertheless, they add, efforts need to be made to create a learning environment which allows children to develop not only the necessary technical skills but also a broader understanding of how media and data are created, recorded, tracked, aggregated, analysed, distributed, applied, used and commercialized. (Livingstone, 2019, para. 6)

Education organizations have been trying to do some of that, with varied attention to commerce and personal information. For example, PBS Kids' Humble Media Genius (2017), for children 6–11, discusses privacy in terms of the need for passwords. It doesn't mention specific concerns about marketers and data. "The Smart Talk," from the Norton antimalware firm and the National Parent Teacher Association (2022), is a "technology agreement" signed by parents and their children that formalizes their discussions about "digital safety topics" (p. 3). In addition to noting the importance of such actions as password use, privacy settings, and two-factor authentication with apps, the agreement suggests somewhat vaguely that the child "pause to consider who I am giving my information to and how it could be used or sold" (National Parent Teacher Association & Norton, 2022, "Preface to Questions," pp. 15–18). Common Sense Media's (n.d.) multigrade "Digital Citizenship" approach does introduce the concept of "big data" in its seventh- and eighthgrade curricula. The seventh- and eighth-grade curricula explain "why information about [students] and their behaviors is valuable to companies[,] analyze how certain types of data are used by companies[, and] . . . [explore] strategies to limit individual data collection by companies" (Common Sense Media, n.d., para. 2). In the eighth grade, that includes how to turn cookies off in their browser settings if the student is uncomfortable with tracking. While these programs have different approaches, they all emphasize individual autonomy and ignore government regulations and oversights. .

An extension of this individual literacy approach for adults is the notion of a "privacy label." In 2009, researchers from Carnegie Mellon University created "a clear, uniform, single-page summary of a company's privacy policy" so people could decide whether to use a particular website or another (Kelly,
Bresee, Cranor, & Reeder, 2009, p. 1). In 2020, Common Sense Education similarly suggested the idea of "Building a Better Nutrition Label for Privacy" (Girard, 2020). Commercially, both Apple's App Store (in 2021) and the Google Play app emporium (in 2022) initiated versions of privacy "nutrition labels" for the apps they carry. Both require app developers to present their data use practices in the same format as every other app (Perez, 2022).

Evidence suggests that the nutrition label does not work. In a January 2021 spot check of app labels on the App Store, the *Washington Post* found inaccuracies in labels' claims and suggested they gave users a false sense of security about how their data are used. Google also acknowledged the difficulty of ferreting out false information. Both companies said they would try to ensure the accuracy of apps' assertions about their tracking

practices (Fowler, 2021). Yet it is hard to see how a standardized, necessarily oversimplified "nutrition label" can give people meaningful insights into the complicated world of data collection that companies allude to in their privacy policies and that they practice in even more difficult-tounderstand ways.

It is the intricate nature of these activities that leads a third group of scholars to find consent useless. Helen Nissenbaum (2018), for example, suggests that the complexity of digital life makes securing real consent impossible. Julie Cohen (2021) adds that digital networks are too powerful for consent-based approaches to privacy that center on individual control. Daniel Solove (2013) suggests that the rights companies extend to individuals regarding the collection and use of their personal information are undermined by a lack of public understanding about how that information is used. Solove argues that technology companies "take refuge" in consent; they rely on a click-to-agree button to give them permission to do whatever they want with user data. And Ari Waldman (2021) has shown the consent paradigm presumes perfect rationality in decision making that does not exist and conflates consent with actual choice (pp. 52–67).

This debate between those who support the notice-and-consent model and those who recognize its dangers led us to carry out a major inquiry into the extent to which adult Americans can navigate notice and whether knowledgeable, or informed, consent is even possible. We adapt our notion of informed consent from the formulation expressed by Robert J. Levine (1988) in connection with the ethics of clinical medical research. As summarized by Cottrell and McKenzie (2011),

Informed consent is "the voluntary agreement of an individual, or his or her authorized representative, who has the legal capacity to give consent, and who exercises free power of choice, without undue inducement or any other form of constraint or coercion to participate." (p. 106)

They add that "the individual must have sufficient knowledge and understanding of the nature of the proposed research, the anticipated risks and potential benefits, and the requirements of the research to be able to make an informed decision" (Cottrell & McKenzie, 2011, p. 106).

From the standpoint of the use of people's data by commercial entities, Levine's formulation points to two elements of consent, both of which are necessary to make an informed decision: understanding and autonomy. A person must understand the corporate practices and policies—and the extent of legal protections, if any—related to the data companies try to take about them. A person must also believe that technology companies will give the person the independence to decide whether and when to give up the data. If people do not fit either or both elements, it indicates that their consent to companies' data collection is involuntary, not free, and illegitimate.

Our research task, then, involved investigating Americans' knowledge of essential facts about marketing practices and policies in the digital environment as well as their belief that they have the autonomy to control the extent to which marketers take and use data about them. To explore Americans' sense of autonomy, we used the idea of digital resignation, a concept Turow, Draper, and Hennessey introduced in 2015. It measures the extent to which Americans say they would like to control the data firms have about them but believe they cannot. Since the term was coined, marketers' command of internet data has become more far reaching, cross media, and location specific. What we find now definitively negates the idea that Americans feel that they can adequately understand and consent to marketers' data-gathering regime. It also indicates that Americans do not have even the basic

knowledge to benefit from such a regime. At this point in the development of the internet, individual consent is unworkable.

The Study and Its Population

Our findings come from a survey we carried out regarding Americans' opinions about and understanding of questions related to privacy, surveillance, and technology. The survey was conducted from August 8, 2022, to September 8, 2022, by the National Opinion Research Center (NORC) at the University of Chicago. A general population sample of adults (18 and over) was selected from NORC's AmeriSpeak Panel. NORC conducted Web and telephone interviews with a nationally representative, English (N = 1963) or Spanish (N = 51) speaking sample of 2,014 adult internet users living in the continental United States. The survey used a mixed-mode design, and respondents could opt to take the survey via a self-administered Web survey (N = 1919) or by talking to a live telephone interviewer (N = 95). Respondents were sampled using area probability and address-based sampling from NORC's National Sample Frame, and fully represented the U.S. population. The median survey duration was 13 minutes. The Weighted Household Recruitment Rate (RR3) was 20.3%. 7,141 panelists were invited to take the survey, yielding a completion rate of 28.2%. The Weighted Cumulative Response Rate was 4.5%, a good result for national surveys. Statistical results are weighted to correct known demographic discrepancies. The margin of sampling error for the complete set of weighted data is ±2.95% at the 95% confidence level. The error margin is higher for smaller subgroups within the sample. Table 1 provides an introductory snapshot of the population we interviewed.

Table 1. Characteristics of U.S. Adults in Sample (N = 2,014).

Trait	%
Sex	
Male	49
Female	51
ge 18–24	
	11
25–34	17
35–44	17
45–54	14
55–64	18
65–74	14
75+	8
Race/Ethnicity	
White, non-Hispanic	62
Black, non-Hispanic	12
Asian, non-Hispanic	6
Hispanic	17
Mixed, other non-Hispanic	3
Income	
Under $30,000	21
$30,000 to under $60,000	27

American Journal of Art and Communication
Vol.7 , Issue3 May- June - 2022;
1252 Columbia Rd NW, Washington DC, United States
https://topjournals.org/index.php/AJAC; mail: topacademicjournals@gmail.com

$60,000 to under $100,000	24
$100,000 and Over	28
Highest Education Level	
Less than high school graduate	9
High school or equivalent	29
Vocational/tech school/some college/associates Bachelor's degree	26
	21
Postgraduate study/professional degree	15

Note. When numbers in this and other tables don't add to 100%, it is due to rounding error.

Findings

Americans Overwhelmingly Lack the Basic Knowledge About Internet Privacy Necessary to Grant Consent

A primary element of consent is sufficient understanding of risks and benefits. Strikingly large percentages of adult Americans are not alert to basic practices and policies by companies and governments that can help them navigate the commercial internet in ways that benefit them. Table 2 contains 17 truefalse statements we asked our sample to gauge what we call their internet navigational knowledge— important facts that can help them use the digital commercial world to their benefit. It shows that large percentages of Americans—71%—do know that when they go to a website, it can "collect information about [their] online behaviors even if [they] don't register using [their] name or email address." Beyond that, awareness of types of company tracking drops considerably: 55% know a smart TV can help advertisers send an ad to a viewer's smartphone based on the show they are watching; 52% are correct that a company can tell that a person has opened its email even the person doesn't click on any links; and 46% know that a website can track people's activity across devices even if they do not log into the same account on those devices.

Table 2. True-False Statements About Basic Corporate and Governmental Internet Practices and Policies (N = 2,014).

Statement	True (%)	False (%)	DK (%)	Wrong (%)
	71		24	
When I go to a website, it can collect information about my online behaviors even if I don't register using my name or email address.	5			30
mart TV can help advertisers send an ad to a viewer's smartphone based on the show they are watching.	**55**	7	38	45
ompany can tell that I have opened its email even if I don't click on any links.	**52**	10	38	48
ebsite cannot track my activity across devices unless I log into the same account on those devices.	17	**46**	36	53

en a website has a privacy policy, it means the site will not share my information with other websites or companies without my permission.	33	**44**	23	56
ebook's user privacy settings allow me to limit the information about me that Facebook shares with advertisers.	**44**	20	36	56
fifty states have laws requiring companies to notify individuals of security breaches involving personally identifiable information.	**43**	18	39	57
illegal for internet marketers to record my computer's IP address.	15	**40**	46	61
legal for an online store to charge people different prices depending on where they are located.	**38**	25	38	63
doorbell company Ring has a policy of not sharing recordings with law enforcement without the homeowner's permission.	**37**	13	50	63
law, a travel site such as Expedia or Orbitz that compares prices on different airlines must include the lowest airline prices.	23	**28**	49	72
ıe United States, the federal government regulates the types of digital information companies collect about individuals.	30	**24**	45	75
ıe large American cities have banned the use of facial recognition technology by law enforcement.	**30**	12	58	70
U.S. federal government requires that companies ask internet users to opt in to being tracked.	**24**	30	45	76
tion 230 of the Communication Decency Act ensures that digital platforms like Facebook, Twitter, and YouTube can be held responsible for illegal content posted on their platforms.	33	**19**	48	81
Health Insurance Portability and Accountability Act (HIPAA) prevents apps that provide information about health . . . from selling data collected about app users to marketers.	37	**18**	45	82
ıe social media platforms activate users' smartphone speakers to listen to conversations and identify their interests in order to sell them ads.	44	**16**	40	85

Note. Bolded numbers indicate the correct answers.

Even lower percentages of Americans can correctly identify when corporate and government policies give them control over information. Less than half of the adult population (44%) understands that the phrase privacy policy does not indicate a site won't share a person's information with other sites without the person's permission (many privacy policies state that they do share, in fact, and even sell such information).

From there the table shows a slide toward increasing collective ignorance. For example, just a bit more than one in three (38%) knows it is legal for an online store to charge people different prices depending on where

American Journal of Art and Communication
Vol.7 , Issue3 May- June - 2022;
1252 Columbia Rd NW, Washington DC, United States
https://topjournals.org/index.php/AJAC; mail: topacademicjournals@gmail.com

they are located. Fewer than one in three (28%) knows that a travel site such as Expedia or Orbitz that compares prices on different airlines need not include the lowest airline prices. Only about one in six knows that the federal Health Insurance Portability and Accountability Act (HIPAA) does not prevent apps that provide information about health from selling data collected about app users to marketers. And one in seven thinks some social media platforms activate users' smartphone speakers to listen to conversations and identify their interests to sell them ads.

Being wrong about such facts can have real consequences. Think of a person who believes a travel site such as Expedia or Orbitz that compares prices on different airlines must include the lowest airline prices. That may lead him not to check other sites or apps and so not get the best deal. Or consider a person who uses a fertility app to facilitate family planning. In the wake of the Dobbs decision that gave individual states the right to regulate abortion, privacy experts encouraged people to delete fertility apps. The fear was that some fertility apps share data about users' attempts to get pregnant, leaving users open not just to advertisements about sales on diapers but also intrusions by employers and health insurers, erosion of autonomy, concerns about abortion rights, and the loss of dignity that comes with unwanted sharing of personal information (Harwell, 2019; Hill, 2022; Morrison, 2022). Moreover, retailers such as Target are under no HIPAA obligation to keep the purchases of fertility related purchases private. At the same time, people who think social media platforms like Instagram cause their smartphones to listen to them may be paying attention to the wrong kinds of concerns, or they may be worried about everything digital, which can make it difficult to focus on commercial surveillance activities that really count.

Another insight the table presents is the large percentage of Americans who admit to not knowing the answer to the true-false questions. The *don't knows* range from 23% regarding the meaning of privacy policy (and one of only two statements where the percentage of *don't know* is lower than the of incorrect answers) to the statement about travel sites where a full 49% of respondents selected that choice. They didn't try to guess, implying that they directly acknowledge the digital world's confusing nature.

Table 3 assigns letter grades to the navigational knowledge test. Seventy-seven percent of our respondents failed the test by getting *at most* 53% of the questions (9/17) correct.

Table 3. Americans' Grades on the Navigational Knowledge (N = 2,014).

Letter Grade	¦ correct for that group	Percent of the population
F (53% or less correct)	0–9	77%
D (59–65% correct)	10–11	15%
C (71–76% correct)	12–13	6%
B (82–88% correct)	14–15	1%
A (94% correct)	16	.03%

American Journal of Art and Communication
Vol.7 , Issue3 May- June - 2022;
1252 Columbia Rd NW, Washington DC, United States
https://topjournals.org/index.php/AJAC; mail: topacademicjournals@gmail.com

Note. Fifteen percent received a D, having gotten at most a 65% score. Only 6% of the sample received a C, getting 71–76% of questions correct, and 1% got a B. One person in the entire sample received an A, and 6% got none of the answers correct.

There *are* statistically significant variations in navigational knowledge across U.S. society. Figure 1 shows typically small differences in knowledge based on gender, age, race, income, and education. These distinctions, however, should not obscure the overriding finding: All the groups did very poorly, answering fewer than half the questions correctly. When it comes to navigating the commercial internet, our findings indicate Americans overall are sorely lacking knowledge to navigate it in ways that protect their interests.

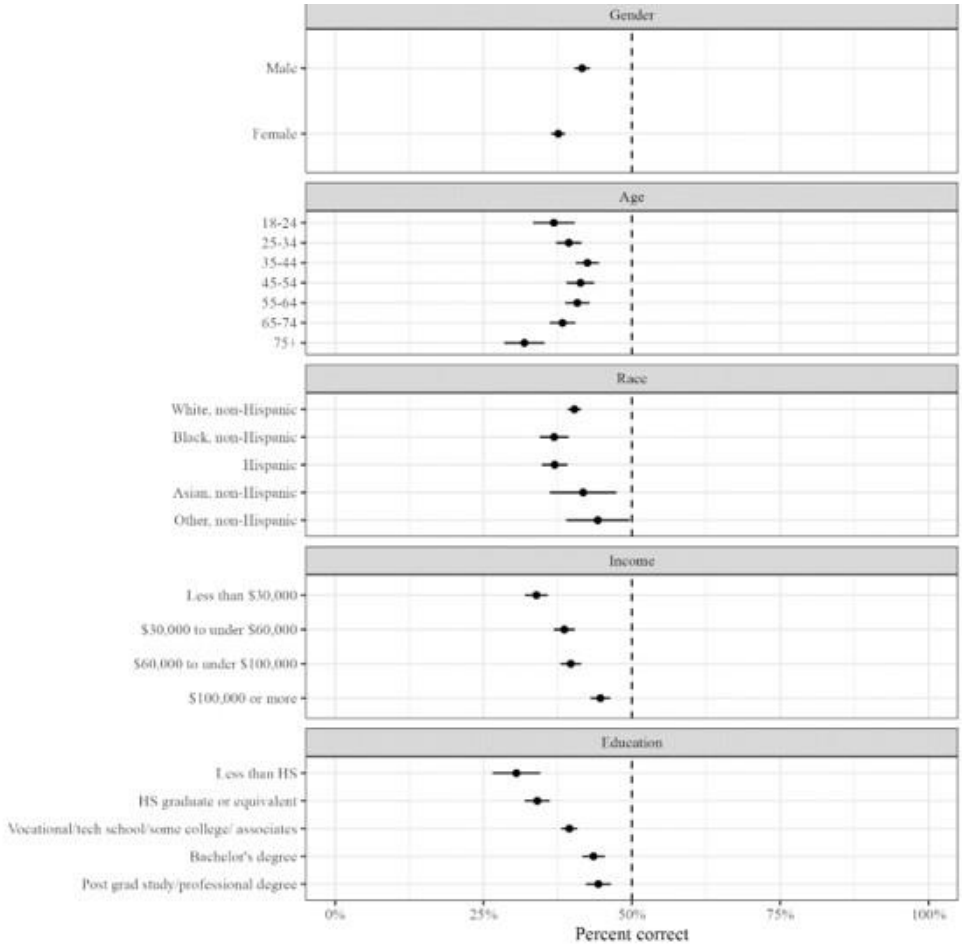

Figure 1. Average knowledge by various demographics.

Americans Do Not Believe They Can Control Their Data or That Companies Will Help Them

American Journal of Art and Communication
Vol.7 , Issue3 May- June - 2022;
1252 Columbia Rd NW, Washington DC, United States
https://topjournals.org/index.php/AJAC; mail: topacademicjournals@gmail.com

Consent must also be given voluntarily, and consumers must believe they can relinquish consent. In this environment of (often admitted) lack of knowledge, Americans say they want to control the data companies get about them but do not believe they can. They also do not believe companies can be trusted to help them. We arrived at this conclusion by presenting our sample with 12 statements adapted from prior studies (Choi, Park & Jung, 2018, Lutz, Hoffmann, & Ranzini, 2020, Marwick & Hargittai, 2019; Turow, Hennessy, & Draper, 2015) that plumb people's perception of their data control and company trust in nuanced ways. As Table 4 shows, virtually all Americans (91%) agree they want to have control over what marketers can learn about them online. At the same time, around 80% say they are naïve to believe they can do so, that they aren't confident they are taking the right steps to protect their digital data, and that they have little control over what marketers can learn about them online. Further, 73% say that they don't have the time to keep up with ways to control what companies can learn about them online, and 60% agree with the blunt statement "I do not understand how digital marketers learn about me."

Table 4. Americans' Responses to Statements About Control Over Their Data (N = 2,014).

Response	Strongly Agree (%)	Agree (%)	Disagree (%)	Strongly Disagree (%)	Neither* (%)
want to have control over what marketers can learn about me online. (91% agree)	60	31	6	2	1
would like to understand how digital marketers use the information they collect about my online activities. (87% agree)	47	40	9	3	1
would be naïve to think that I can reliably protect my personal data online. (80% agree)	36	45	14	4	1
am not sure that I am taking the right steps to protect my digital data. (80% agree)	28	52	16	3	2
have come to believe that I have little control over what marketers can learn about me online. (79% agree)	26	53	16	5	1
do not have the time to keep up with ways to control the information that	24	49	21	5	1

companies have about me. (73% agree)					
trust myself to make the right decisions when it comes to handling my digital data. (69% agree)	22	47	25	4	2
do not understand how digital marketers learn about me. (60% agree)	19	41	31	8	1
It doesn't make a difference whether I try to protect my personal data online or not.(46% agree)	11	35	31	22	1
trust companies I visit online to handle my data the way I would want the data handled. (28% agree)	5	23	40	31	1
don't care what companies learn about me online. (18% agree)	4	14	29	52	1
I believe companies can be trusted to use my personal data with my best interests in mind. (14% agree)	3	11	34	51	1

Note. **Neither* was a volunteered, *don't know* or a skipped question on the Web version.

Trust in marketers is very low when it comes to this topic. Only 28% of Americans agree that they trust companies they visit online to handle their data in ways the individuals would want. An even lower number—14%—agrees that "companies can be trusted to use my personal data with my best interest in mind." As opposed to marketers, 69% agree that they trust *themselves* to make the right decisions when it comes to handling their digital data. Based on other answers, it seems people mean they trust themselves rather than marketers to try to make the right data-control decisions even if they are unsure the steps they are taking are effective. They acknowledge it's tough to succeed. Table 4 indicates that 46% of Americans don't believe it makes "a difference whether I try to protect to protect my data online or not." But recall that a much higher 80% (including, it turns out, 73% of those who say it makes a difference to keep trying) nevertheless agree it is naïve to believe they can protect their online data. And 79% agree "I have come to believe that I have little control over what marketers can learn about me online."

Americans Do Not Accept the Idea of Data Tradeoffs

Americans' lack of trust in marketers extends to situations in which marketers offer them value in exchange for their data. Table 5 lists the four statements we presented that reflect this idea of reciprocity. Three of the tradeoff propositions depict an everyday data-collection approach as well as a common privilege (discount, improved service, or use of a store's wireless internet) marketers claim to present in return. The table shows that

American Journal of Art and Communication
Vol.7 , Issue3 May- June - 2022;
1252 Columbia Rd NW, Washington DC, United States
https://topjournals.org/index.php/AJAC; mail: topacademicjournals@gmail.com

over 60% of respondents disagree with the acceptability of specific common tradeoff activities. A huge 88% don't agree that that if companies give them a discount, it is fair for these companies to collect information about them without their knowledge. A smaller but still large 68% disagree that if a store lets them log into its Wi-Fi, it's fair for the store to monitor their online actions. In direct contrast to marketers' claims that Americans want personalized service and understand that this requires the collection and analysis of personal information, 61% disagree that it is okay if a store where they shop uses information it has about them to create a picture of them that improves the services they provide for them. Table 5 also indicates that 52% of Americans agree that they sometimes feel marketers hold discounts hostage for data. An example would be a store's requirement that shoppers log in to its website or app to reveal personal data if they want to enjoy the benefits of special prices.

Table 5. Americans' Responses to Marketers' Information Collection Activities (N = 2,014).

Statement	Strongly Agree (%)	Agree (%)	Disagree (%)	Strongly Disagree (%)	Neither* (%)
companies give me a discount, it is a fair exchange for them to collect information about me without my knowing it. (88% disagree)	3	8	24	64	1
I log onto a store's Wi-Fi, it is fair for them to monitor what I'm doing online while I am in the store. (68% disagree)	7	24	26	42	1
's okay if a store where I shop uses information it has about me to create a picture of me that improves the services they provide for me. (61% disagree)	5	34	32	29	1
sometimes feel that if I don't let companies take my data, I won't get the discounts I want. (52% agree)	12	40	25	22	1

Note. **Neither* was a volunteered *don't know* on the phone or a skipped question on the web version.

Americans Are Resigned to Marketers' Ability to Use Data About Them

While Americans don't accept the idea of tradeoffs, a large proportion is still willing to give up their data in actual situations. For example, when we gave people a scenario that offered them discounts for providing a supermarket they frequent personal information for discounts, about half—47%—did say yes. But less than half of people who were willing to accept discounts also accepted the notion of tradeoffs. And only 40% of the people

who said yes to the supermarket scenario were the same people who thought it's fine for a store where they shop to create a picture about them in return for benefits. Why are people giving up their data if not because they support tradeoffs? Our data shows that these people are simply resigned.

Resignation occurs when a person believes an undesirable outcome is inevitable but feels powerless to stop it. Asking our respondents whether they agree or disagree with two statements in Table 2, we investigated what percentage of the population can be described as resigned to marketers' imbibing data about them. We presented these statements in random order among the 10 other agree/disagree propositions so that the respondents wouldn't see the relationship between the two or suspect our intention. *To be identified as resigned, a person had to agree with both*.

One statement was "I want to have control over what marketers can learn about me online." The other was "I've come to believe that I have little control over what marketers can learn about me." As Table 4 shows, 91% of Americans agree that "I want to have control over what marketers can learn about me online," and 79% agree that "I have come to believe that I have little control over what marketers can learn about me online." When we investigated the overlap that designates resignation, we found that a large majority of the population—74%—is resigned. They believe they live in a world where marketers taking and using their data is inevitable.

Our findings also indicate the Americans who are willing to give up their data in the supermarket scenario are far more likely to be resigned than to accept the notion of tradeoffs: 81% of the people who said yes to the supermarket scenario are resigned. Conversely, 50% of those who said yes to the supermarket scenario believe in tradeoffs. So, when we see someone giving up data to marketers, it is far more likely they are doing it because they are resigned rather than believe in tradeoffs.

Importantly, huge percentages of American are either resigned, have extremely low knowledge (that is, score 53% or below on the true-false questions), or both. We found that 57% are resigned with extremely low knowledge; 20% have extremely low knowledge and aren't resigned; and 17% do not fail the knowledge test (they score above 53%) but are resigned. Only 5% of the population has neither low knowledge nor resignation. That is a stunningly low number for an "information society" centered around the commercialization of data.

Most Americans Believe That Marketers' Use of Using Their Data Can Harm Them, and They Are Resigned to That Happening

We found that marketers' data capture and resignation come with another combined cost in Americans' mind: individual harm they are powerless to prevent. A full 80% of the population agrees that what companies know about them from their online behaviors can hurt them. Moreover, 62% of Americans believe they can be harmed and are resigned. Put differently, about 6 in 10 Americans believe that what companies know about them can hurt them, *and* that they are powerless to stop it. Roughly 5 in 10 Americans also have extremely low knowledge (fail the navigational knowledge test), are resigned, and believe firms can harm them. In fact, of the 77% of Americans who clearly fail the test (get below 53% on it), 80% believe what companies know about them can harm them. In this context, the idea of consent becomes especially nonsensical.

American Journal of Art and Communication
Vol.7 , Issue3 May- June - 2022;
1252 Columbia Rd NW, Washington DC, United States
https://topjournals.org/index.php/AJAC; mail: topacademicjournals@gmail.com

Americans Want Congress to Act

Americans seem to understand that they have no real ability to consent to marketers' data gathering. It's not surprising, then, that Americans see federal government help as necessary now. We asked, "How urgent is it for Congress to regulate how digital companies' use personal information?" A full 79% of Americans say it is urgent, with 53% saying it is very urgent. Only 6% of people said it was not at all urgent—the rest said they didn't know. In a society where people's consent to marketers' use of their data inherently illegitimate, what directions should public policy take?

Conclusion

For the first time in human history, we live in a society where individuals are defined continually by data streams circulating under the surface of everyday life. Companies can see what we do on our websites and apps (through first-party cookies and other such trackers) to follow us across the media content we visit (via third-party cookies and emerging versions) and view our activities as we move from one media technology to another—for example, from the Web to our smartphone to our tablet to our "connected" TV to the in-store trackers we pass in the aisles to outdoor message boards we stop to view. The goal is to give us tags or personas and have computers decide whether and how we ought to be the companies' targets.

This study has found that overwhelmingly and to an extent not known before, Americans neither understand the basics of such commercial surveillance practices and policies nor feel they can do anything about rampant data extraction. Yet consider the patterned prejudicial discrimination the continual marketing activities encourage. John may get low-end car ads while Jack gets high-end ones. Jane may be among the people targeted for "depression and anxiety" based on an artificial intelligence model that links a HIPAAcompliant database to person-linked databases that identify her personally and predict her specific health conditions (Center for Digital Democracy, 2022). Her teenage daughter may be targeted with junk food commercials because firms know her above-average weight and food predilections. Do you want your retailer to know you as a 35-year-old female who is newly pregnant? Do you feel comfortable that your supermarket is continually analyzing what you've bought? Or that Meta is offering you up advertisers in thousands of categories based on your actions on Instagram, Facebook, and elsewhere you don't know? As Latanya Sweeney (2013) has shown, even names that indicate racial identity can have a significant effect on the kinds of advertisements that appear on search platforms. Apart from the potential discriminatory deals such a world propels, it also encourages a loss of dignity: a sense that unseen forces are defining us and we really can't do anything about it.

If consumers have trouble understanding today's tracking activities, it seems unlikely they will understand—and be capable of giving informed consent to—the vast data collection that powers machine learning. Terms such as generative artificial intelligence (AI), over-the-top TV (OTT), connected television (CTV), the metaverse, and biometrics reflect a new world of interconnected technologies marketers are entering that will follow and define people in new ways. When you phone an 800 number to complain, do you want the company to infer your emotional state by the sound of your voice and to triage you to an agent who is successful at satisfying and even "upselling" people with your putative emotions and purchase history? That already happens, and it indicates the rise of marketers peering into the human body for data (Turow, 2021). Biometric data cannot

be changed like email addresses. Yet people already give opt-out or opt-in "consent" to the collection of their bodily data every day. Understanding how those data feed automated decision-making systems, geolocation tracking, and biometric analyses, among other high-tech tools, requires individuals to read about, process, and make decisions based on algorithmic information even many experts do not comprehend (Kearns & Roth, 2019).

Companies may argue that they offer ways for people to stop such tracking. But as we have seen, a great percentage of the U.S. population has no understanding of how the basics of the commercial internet work. Expecting Americans to learn how to continually keep track of how and when to opt out, opt in, and expunge their data is folly. Moreover, the more people accept that data will be taken about them, the more that activity will become normalized. Normalization is a psychological concept that associates frequency with acceptability (Bear & Knobe, 2017). People a generation from now will take for granted that giving up personal data is the way to get along in the 21st century. And they won't complain when the techniques commercial marketers use are picked up by political campaigns, police, and governments in their avowedly democratic societies.

Recent proposals for comprehensive privacy legislation retain consent as a primary vehicle for extracting data from individuals. Although the GDPR (2018) allows data collection for many reasons, consent is the one most used by marketers and other data collectors. New state privacy laws are also based on consent. The California Consumer Privacy Act (2018) relies on opt-out consent. Two proposals recently introduced in Arizona would let technology companies sell customer data, avoid all restrictions on processing data about adults, and make decisions based on consumer profiling if they obtain consent (Arizona S.B. 1614, 2020; Arizona H.B. 2729, 2020). Two proposals introduced in the Illinois Senate would allow companies to skirt limits on processing sensitive data, even processing that posed a significant risk to privacy, if they obtain consent (Data Privacy Act, 2019; Data Transparency and Privacy Act, 2020). And Maine's privacy law, which took effect in 2019, lifts all restrictions on use, disclosure, sale, and third-party access to personal information if companies obtain consent (An Act To Protect the Privacy of Online Customer Information, 2019).

Based on our findings and their relation to deep discussions among scholars regarding this issue, we believe that consent, whether opt in or opt out, should no longer be allowed to trigger data collection. That means companies shouldn't be able to use first-party or third-party data collected pursuant to a consent button to create definitions or personas of people that they offer up to customers. Our data indicate that large proportions of Americans don't distinguish between first party and other data trackers; they don't want *any* data taken from them as they try to eke benefits from the internet.

Our findings also call into question the value of many of the "rights-based" privacy laws proposed and enacted by several U.S. states over the past several years. These laws, which attempt to regulate data extraction by providing consumers with rights to access the information companies have about them, rights to request deletion of that data, rights to move the data to other companies, and rights to correct inadequate data, still require individuals to understand and process information in privacy policies and terms of service at scale (Waldman, 2022a). They require knowledge and a belief that companies will genuinely listen to their requests—that is, the opposite of the confusion and resignation we have found across the U.S. population. We recognize that some shoppers derive benefits from ad targeting in the form of sales, coupons, and information. If policymakers would

like to retain an advertising-based business model based on consumer interests, we suggest that they restrict it to contextual advertising. Policymakers could permit a system where companies can target people based only on the context in which advertisers find customers in the moment—on a website for cars, an app about travel, a supermarket aisle with diapers, or a video closely associated with a set of interests—without allowing the marketers to share or keep any history of consumer connections to those contexts.

We realize we are calling for regulations that include a paradigm shift in information-economy law and corporate practice. To encourage lawmakers to implement these major changes undoubtedly requires a politically engaged public that is angry about the contemporary situation—just the opposite of the resigned public our study has found. Figuring out how to best do that presents a new challenge for researchers. One way to move citizens from resignation to anger and action regarding commercial surveillance may involve pointing out how the discriminatory tracking and targeting that takes place in marketing realms has begun to migrate to other sectors of society—for example, political campaigning, policing, incarceration, and migrant interrogation (see Crain & Nadler, 2019; Turow, 2021, pp. 234–243)—where harm from digital discrimination is easier to imagine and angry indignation perhaps easier to ignite. Further, tying these developments to the rise of biometric profiling in and outside of marketing—emphasizing the profound implications of allowing firms to interrogate typically unchangeable aspects of the body—may raise worries about future generations and provide even more catalysts to turn public resignation into anger and, ultimately, action.

References

An Act To Protect the Privacy of Online Customer Information, Maine Rev. Stat. Ann. §9301(3). (2019). Retrieved from https://legislature.maine.gov/legis/bills/bills_129th/chapters/PUBLIC216.asp#:~:text=Privacy%20of%20customer%20personal%20information,United%20States%20Code%2C%20Section%202703

Arizona H.B. 2729 §§18-574(B), 18-577(G)(3). (2020). Retrieved from https://azleg.gov/legtext/54leg/2R/bills/HB2729P.pdf

Arizona S.B. 1614 §18-701(H). (2020). Retrieved from https://www.azleg.gov/legtext/54leg/2R/bills/SB1614P.pdf

Baracos, S., & Nissenbaum, H. (2009). On notice: The trouble with notice and consent. In *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information.* Retrieved from https://ssrn.com/abstracts=2567409

Bear, A., & Knobe, K. (2017). Normality: Part descriptive, part prescriptive. *Cognition, 167,* 25–37. https://doi.org/10.1016/j.cognition.2016.10.024

Bromwich, J. E. (2016, May 24). Goodbye, Internet. Hello, internet. *New York Times*. Retrieved from https://www.nytimes.com/2016/05/25/business/media/internet-to-be-lowercase-in-new-yorktimes-and-associated-press.html?_r=0

Bulger, M., & Davison, P. (2018). The promise, challenges, and futures of media literacy. *Journal of Media Literacy Education, 10*(1), 1–21. https://doi.org/10.23860/JMLE-2018-10-1-1

California Consumer Privacy Act, Cal. Civ. Code § 1798.135. (2018). Retrieved from https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.135

Center for Digital Democracy. (2022, November 21). *Trade regulation rule on commercial surveillance and data security.* Retrieved from https://www.democraticmedia.org/sites/default/files/field/publicfiles/2022/cddsurveillancehealthftc112122.pdf

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior, 8,* 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Cohen, J. E. (2021, March 23). *How (not) to write a privacy law*. Retrieved from https://knightcolumbia.org/content/how-not-to-write-a-privacy-law

Common Sense Media. (n.d.). *Digital citizenship*. Retrieved from https://www.commonsense.org/education/digital-citizenship

Cottrell, R., & McKenzie, J. (2011). *Health promotion* (2nd ed.). Sudbury, MA: Jones and Bartlett.

Crain, M., & Nadler, A. (2019). Political manipulation and internet advertising infrastructure. *Journal of Information Policy, 9*, 370–410. https://doi.org/10.5325/jinfopoli.9.2019.0370

Cyphers, B. (2022, May). *How to disable ad ID tracking on iOS and Android, and why you should do it now*. Retrieved from https://www.eff.org/deeplinks/2022/05/how-disable-ad-id-tracking-ios-andandroid-and-why-you-should-do-it-now

Data Privacy Act, Illinois S.B. 2263 §30(3). (2019). Retrieved from https://www.ilga.gov/legislation/BillStatus.asp?GA=101&DocTypeID=SB&DocNum=2263&GAID=15&SessionID=108&LegID=121653

Data Transparency and Privacy Act, Illinois S.B. 2330 §35(l)(3). (2020). Retrieved from https://www.ilga.gov/legislation/BillStatus.asp?DocNum=2330&GAID=15&DocTypeID=SB&LegId=122685&SessionID=108&GA=101

Fowler, G. (2021, January 29). I checked Apple's new privacy "nutrition labels." Many were false. *Washington Post.* Retrieved from https://www.washingtonpost.com/technology/2021/01/29/apple-privacy-nutrition-label/

General Data Protection Regulation, Regulation (EU) 2016/679 *supra* note **Error! Bookmark not defined.**, at art. 6(1). (2018). Retrieved from https://gdpr-info.eu/art-6-gdpr/

Girard, K. (2020, August 10). *Building a better nutrition label for privacy*. Retrieved from https://www.commonsense.org/education/articles/building-a-better-nutrition-label-for-privacy

Harwell, D. (2019, April 10). Is your pregnancy app sharing your intimate data with your boss? *Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2019/04/10/tracking-yourpregnancy-an-app-may-be-more-public-than-you-think/

Hill, K. (2022, June 30). Deleting your period tracker won't protect you. *The New York Times*. Retrieved from https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html

Kaminski, M., & Jones, M. L. (2021). An American's guide to the GDPR. *Denver Law Review, 98*(1), 93–128. Retrieved from https://www.denverlawreview.org/print-archive459f/volume98-issue1

Kearns, M., & Roth, A. (2019). *The ethical algorithm: The science of socially aware algorithm design.* Oxford, UK: Oxford University Press.

Kellner, D., & Share, J. (2005). Toward critical media literacy: Core concepts, debates, organizations, and policy. *Discourse: Studies in the Cultural Politics of Education, 26*(3), 369–386.

Kelly, P. G., Bresee, J., Cranor, L.F., & Reeder, R. (2009). Cranor. In *SOUPS '09: Proceedings of the 5th Symposium on Usable Privacy and Security* (pp. 1–12). https://doi.org/10.1145/1572532.1572538

Lee, N. M. (2018). Fake news, phishing and fraud: A call for research on digital media literacy education beyond the classroom. *Communication Education, 67*(4), 360–466. https://doi.org/10.1080/03634523.2018.1503313

Levine, R. J. (1988). *Ethics and regulation of clinical research*. New Haven, CT: Yale University Press.

Livingstone, S. (2019, June 14). *What should we teach children about online privacy, and how?* Retrieved from https://blogs.lse.ac.uk/medialse/2019/06/24/what-should-we-teach-children-about-onlineprivacy-and-how/

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society*, *22*(7), 1168–1187. https://doi.org/10.1177/1461444820912544

Mansur, P. K. (2019, March 28). *Reconceptualizing online privacy literacy*. Retrieved from https://philippmasur.de/2019/03/28/reconceptualizing-online-privacy-literacy/

Marwick, A., & Hargittai, E. (2019). Nothing to hide, nothing to lose? Incentive and disincentives to sharing information with institutions online. *Information, Communication & Society, 22*(12), 1697–1713. https://doi.org/10.1080/1369118X.2018.1450432

Morrison, S. (2022, July 6). *Should I delete my period app?* Retrieved from https://www.vox.com/recode/2022/7/6/23196809/period-apps-roe-dobbs-data-privacy-abortion

National PTA & Norton. (2022, June 12). *Conversations that click*. Retrieved from https://thesmarttalk.org/

Nissenbaum, H. (2018, September 24). Stop thinking about consent: It isn't possible and it isn't right. *Harvard Business Review*. Retrieved from https://hbr.org/2018/09/stop-thinking-about-consentit-isnt-possible-and-it-isnt-right.

Norberg, P., Horne, D. R., & Horne D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070

Obar, J., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society, 23*(1), 128–147. https://doi.org/10.1080/1369118X.2018.1486870

Perez, S. (2022, April 26). *Google launches its own privacy "nutrition labels," following similar effort by Apple*. Retrieved from https://techcrunch.com/2022/04/26/google-play-launches-its-ownprivacy-nutrition-labels-following-similar-effort-by-apple/

Public Broadcasting Service. (2017). Ruff Ruffman: Humble media genius. Retrieved from https://pbskids.org/fetch/ruff/

Richards, N., & Hartzog, W. (2019). The pathologies of digital consent. *Washington University Law Review, 96*(6), 1461–1503. Retrieved from https://openscholarship.wustl.edu/law_lawreview/vol96/iss6/11

Schwartz, J. (2002, December 29). The Nation: Case-sensitive crusader. *New York Times*. Retrieved from https://www.nytimes.com/2002/12/29/weekinreview/the-nation-case-sensitive-crusader-who-ownsthe-internet-you-and-i-do.html

Schwartz, P. (1999). Privacy and democracy in cyberspace. *Vanderbilt Law Review, 52*(6), 1607–1701. Retrieved from https://scholarship.law.vanderbilt.edu/vlr/vol52/iss6/2

Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review, 126*(7), 1880–1903. Retrieved from https://harvardlawreview.org/print/vol126/introduction-privacy-self-management-and-the-consent-dilemma/

Solove, D. J., & Hartzog, W. (2011). The FTC and the new common law of privacy. *Columbia Law Review, 114*(3), 583–676. Retrieved from https://columbialawreview.org/content/the-ftc-and-the-newcommon-law-of-privacy/

Sweeney, L. (2013). Discrimination in online ad delivery: Google ads, Black names and White names, racial discrimination, and click advertising. *Acmqueue, 11*(3), 10–29.

Torres, M., & Mercado, M. (2006). The need for critical media literacy in teacher education core curricula. *Educational Studies, 39*(3), 250–282.

Turow, J. (2021). *The voice catchers: How marketers listen in to exploit your feelings, your privacy, and your wallet.* New Haven, CT: Yale University Press.

Turow, J., Hennessy, M., & Draper, N. (2015). *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation.* Retrieved from https://repository.upenn.edu/cgi/viewcontent.cgi?article=1554&context=asc_papers

Turow, J., Hennessy, M., & Draper, N. (2018). Persistent misperceptions: American's misplaced confidence in privacy policies, 2003–2015. *Journal of Broadcasting & Electronic Media, 62*(3), 461–478.

U.S. Secretary's Advisory Committee on Automated Personal Data Systems. (1973). *Records, computers, and the rights of citizens* (OHEW Publication NO. (OS)73-94). U.S. Department of Health, Education & Welfare. Retrieved from https://archive.epic.org/privacy/hew1973report/

Waldman, A. E. (2021). *Industry unbound: The inside story of privacy, data, and corporate power.* Cambridge, UK: Cambridge University Press.

Waldman, A. E. (2022a). Privacy rights trap. *Northwestern University Law Review Online, 117,* 88–106. Retrieved from https://northwesternlawreview.org/articles/privacys-rights-trap/

Waldman, A. E. (2022b). The new privacy law. *UC Davis Law Review Online, 55,* 19–41. Retrieved from https://lawreview.law.ucdavis.edu/online/55/waldman.html