2-2023

Americans Can't Consent To Companies' Use Of Their Data

Joseph Turow
University of Pennsylvania, jturow@asc.upenn.edu

Yphtach Lelkes
University of Pennsylvania, yphtach.lelkes@asc.upenn.edu

Nora A. Draper
University of New Hampshire - Main Campus

Ari Ezra Waldman
Northeastern University

Americans Can't Consent To Companies' Use Of Their Data

Abstract

Consent has aways been a central part of Americans' interactions with the commercial internet. 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, the latest Annenberg national survey finds that Americans have neither.

High percentages of Americans don't know, admit they don't know, and believe they can't do anything about basic practices and policies around companies' use of people's data.

- FACT: By law a travel site such as Expedia or Orbitz that compares prices on different airlines does not have to include the lowest airline prices. 72% don't know that; 49% of Americans admit they don't know. •
- FACT: The Federal Health Insurance and Portability Act (HIPAA) does not stop apps that provide information about health – such as exercise and fertility apps – from selling data collected about the app users to marketers. 82% of Americans don't know; 45% admit they don't know. •
- FACT: It is legal for an online store to charge people different prices depending on where they are located. 63% don't know, and 38% of Americans admit they don't know.

High levels of frustration, concern, and fear compound Americans' confusion: 80% say they have little control over how marketers can learn about them online; 80% agree that what companies know about them from their online behaviors can harm them. These and related discoveries from our survey paint a picture of an unschooled and admittedly incapable society that rejects the internet industry's insistence that people will accept tradeoffs for benefits and despairs of its inability to predictably control its digital life in the face of powerful corporate forces. 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. Our portrait of a society underprepared for the behind-the-screen pitfalls of internet commerce is drawn from a nationally representative multi-mode survey of 2,014 U.S. adults conducted during Fall 2022 for Penn's Annenberg School by the University of Chicago's National Opinion Research Center. The aim of this report is to chart the particulars of Americans' lack of knowledge about the commercial use of their data and their "dark resignation" in connection to it. Our goal is also to raise questions and suggest solutions about public policies that allow companies to gather, analyze, trade, and otherwise benefit from information they extract from large populations of people who are uninformed about how that information will be used and deeply concerned about the consequences of its use. In short, we find that informed consent at scale is a myth, and we urge policymakers to act with that in mind.

Disciplines

Communication | Social and Behavioral Sciences

AMERICANS CAN'T CONSENT TO COMPANIES' USE OF THEIR DATA

THEY ADMIT **THEY DON'T UNDERSTAND IT**, SAY THEY'RE **HELPLESS TO CONTROL IT**, AND BELIEVE THEY'RE **HARMED** WHEN FIRMS USE THEIR DATA—MAKING WHAT COMPANIES DO **ILLEGITIMATE**

JOSEPH TUROW
Robert Lewis Shayon Professor of Media Systems & Industries
University of Pennsylvania

YPHTACH LELKES
Associate Professor of Communication
University of Pennsylvania

NORA A. DRAPER
Associate Professor of Communication
University of New Hampshire

ARI EZRA WALDMAN
Professor of Law and Computer Science
Northeastern Univesity

A Report from the Annenberg School for Communication, University of Pennsylvania

Annenberg
SCHOOL FOR COMMUNICATION
UNIVERSITY of PENNSYLVANIA

Joseph Turow, Ph.D., is the Robert Lewis Shayon Professor of Media Systems & Industries at the Annenberg School for Communication. Turow is an elected Fellow of the International Communication Association and was presented with a Distinguished Scholar Award by the National Communication Association. His most recent books are *The Voice Catchers* (Yale, 2021), *Media Today: Mass Communication in a Converging World* (Routledge, 2023), and *The Aisles Have Eyes* (Yale, 2017). Since 1999 he has conducted national surveys that have moved forward public discourse on digital media, marketing, and privacy.

Yphtach Lelkes, Ph.D., is an associate professor at the Annenberg School for Communication and the Political Science department (secondary appointment) of the University of Pennsylvania. He co-directs the Polarization Research Lab, which examines the causes and consequences of polarization using surveys, experiments, and natural language processing. He teaches courses in data science and quantitative research methods. His work has appeared in major communication, political science, and psychology journals, including the *Journal of Communication*, the *American Political Science Review*, and the *Journal of Personality and Social Psychology*, as well as the *Proceedings of the National Academy of Science* and *Nature Human Behavior*.

Nora A. Draper, Ph.D., is an associate professor in the Department of Communication at the University of New Hampshire. Her research examines the complexities of authenticity, privacy, identity, and reputation in the digital era through frames of cultural theory, critical institutionalism, and public policy. She is the author of *The Identity Trade: Selling Privacy and Reputation Online* (NYU, 2019). Her work has also been published in the *International Journal of Communication*, *Critical Studies in Media Communication*, the *Journal of Children and Media*, and *Surveillance & Society*.

Ari Ezra Waldman, J.D., Ph.D. is a professor of law and computer science and faculty director of the Center for Law, Information, and Creativity at Northeastern University. He is the author of more than 35 scholarly articles in leading law reviews and peer-reviewed journals and two books. His most recent book, *Industry Unbound* (Cambridge, 2021), which focuses on the way technology companies implement and evade privacy law in practice, was named one of the top five books in privacy law. He earned his PhD in sociology from Columbia University and his JD from Harvard Law School.

February 2023

The authors thank Annenberg doctoral students Anjali DasSarma and Shane Abelard Ferrer Sheehy for their help during the creation of this report. Thanks to Kyle Cassidy and Emma Fleming for the cover art.

This survey was funded by an unsolicited, unrestricted grant from Facebook.

Overview

Consent has aways been a central part of Americans' interactions with the commercial internet. 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, the latest Annenberg national survey finds that Americans have neither.

High percentages of Americans don't know, *admit* they don't know, and believe they can't do anything about basic practices and policies around companies' use of people's data.

- FACT: By law a travel site such as Expedia or Orbitz that compares prices on different airlines does not have to include the lowest airline prices. 72% don't know that; 49% of Americans admit they don't know.
- FACT: The Federal Health Insurance and Portability Act (HIPAA) does not stop apps that provide information about health – such as exercise and fertility apps – from selling data collected about the app users to marketers. 82% of Americans don't know; 45% admit they don't know.
- FACT: It is legal for an online store to charge people different prices depending on where they are located. 63% don't know, and 38% of Americans admit they don't know.

High levels of frustration, concern, and fear compound Americans' confusion: 80% say they have little control over how marketers can learn about them online; 80% agree that what companies know about them from their online behaviors can harm them. These and related discoveries from our survey paint a picture of an unschooled and admittedly incapable society that rejects the internet industry's insistence that people will accept tradeoffs for benefits and despairs of its inability to predictably control its digital life in the face of powerful corporate forces. 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.

Our portrait of a society underprepared for the behind-the-screen pitfalls of internet commerce is drawn from a nationally representative multi-mode survey of 2,014 U.S. adults conducted during Fall 2022 for Penn's Annenberg School by the University of Chicago's National Opinion Research Center. The aim of this report is to chart the particulars of Americans' lack of knowledge about the commercial use of their data and their "dark resignation" in connection to it. Our goal is also to raise questions and suggest solutions about public policies that allow companies to gather, analyze, trade, and otherwise benefit from information they extract from large populations of people who are uninformed about how that information will be used and deeply concerned about the consequences of its use. In short, we find that informed consent at scale is a myth, and we urge policymakers to act with that in mind.

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 Housing, Education, and Welfare (HEW), entitled *Records, Computers, and the Rights of Citizens*. 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."[1]

In the decades since the HEW report, the Federal Trade Commission (FTC) has built a "common law" of privacy through consent decrees and settlement agreements with the companies it regulates.[2] These consent decrees have primarily focused on notice—notably, only one of the FIPPs—and holding companies to the promises they make in their privacy policies. Several sector-specific federal laws do the same.[3] Not waiting for federal regulation, several states have passed laws that codify versions of the FIPPs.[4] Parallel to these developments, various European privacy conventions – including those of the Organisation for Economic Cooperation and Development (OECD), the Council of Europe, and the European Union Data Protection Directive – have issued similar but more expansive guidelines for giving individuals knowledge and control over their data.[5] 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.[6] Therefore, in both the US 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 self-management: 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 U.S., by contrast, FTC oversight and state laws allow consent to be implicit in most cases. That is, as long as 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 actually quite complex. California requires internet marketers to post a clickable notice "Do Not Sell My Information" which aims to streamline the activity. Some states do require opt in for firms taking "sensitive" information such as sexual orientation and some health issues.[7] Opting in for sensitive issues has also become customary for the largest websites and apps. And Apple requires apps that track user activities across other apps and internet locations to click an opt in button affirming that is acceptable.[8] But whether emphasizing opt in or opt out, all of 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 don't 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.[9] 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.[10] In a similar vein, Solon Barocas and Helen Nissenbaum 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 that are not legible to users.[11] Neil Richards and Woodrow Hartzog suggested that existing consent models invite unwitting and coerced consent.[12] They argued that individuals cannot understand the legal agreements, technologies, or consequences of data extraction. In fact, work by Joseph Turow, Nora Draper, and Michael Hennessy showed that people even misunderstand the very meaning of the term *privacy policy*, thinking it promises the firm will protect their privacy.[13]

Arguments About Consent and Policy

Despite these concerns, the policy implications of Americans' consent to commercial data extraction remain very much 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-and-consent. When confronted with surveys that indicate people don't want to be tracked, they argue that people only claim to care about privacy in surveys; their actions say otherwise.[14] 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 in to 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 pre-school onward can be taught to manage their data online and on apps.[15] Philip Masur, for 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."[16] More specifically, Sonia Livingstone and her team studying children and online privacy in the UK find "important gaps in children's ability to foresee and navigate institutional and commercial aspects of privacy." 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." 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."[17]

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, for children 6-11, discusses privacy in terms of the need for passwords. It doesn't mention specific concerns about marketers and data.[18] "The Smart Talk," from the Norton anti-malware firm and the National Parent Teacher Association, is a "technology agreement" signed by parents and their children that formalizes their discussions about "digital safety topics." In addition to noting the importance of such actions as password use, privacy settings, and two-factor authentication with apps, the advice suggests somewhat vaguely that the child "pause to consider who I am giving my information to and how it could be used or sold."[19] Common Sense Media's multi-grade "Digital Citizenship" approach, does introduce the concept of "big data" in its seventh and eighth grade 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."[20] 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.[21] In 2020, Common Sense Education similarly suggested the idea of "Building a Better Nutrition Label for Privacy."[22] 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.[23]

Evidence suggests that the nutrition label doesn't 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.[24] 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-to-understand ways.

It is the intricate nature of these activities that leads a third group of scholars to find consent useless. Helen Nissenbaum, for example, suggests that the complexity of digital life makes securing real consent impossible.[25] Julie Cohen adds that digital networks are too powerful for consent-based approaches to privacy that center individual control.[26] Recently, Daniel Solove suggested 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.[27] And Ari Waldman has shown the consent paradigm presumes perfect rationality in decision-making that does not exist and conflates consent with actual choice.[28]

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 in connection with the ethics of clinical medical research. "Informed consent," Levine writes, "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." Levine adds 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."[29] 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 don't 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.[30] 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 far 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 NORC at the University of Chicago. A general population sample of adults (18 and over) were selected from NORC's AmeriSpeak Panel.

The survey questions included in this report focus on four related areas. First, they assess respondents' "navigational knowledge" of privacy and technology. The second set of questions relate to perceptions that respondents have control over their data and trust companies to protect them. The third set of questions assess respondents' acceptance of privacy tradeoffs—the idea that they willingly give data to companies for the benefits they receive. The final section gauges whether respondents believe that the government should protect them.

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 US 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 percent at the 95% confidence level. The margin of error is higher for smaller subgroups within the sample.[1]

Table 1 provides an introductory snapshot of the population we interviewed. As Table 1 indicates, women slightly outnumber men; 62% designate themselves as White, 12% identify themselves as Black, Asians comprise 6%, "mixed" and "other" race/ethnicity but non-Hispanic make up 2%. Hispanics (White and Black) comprise about 17% of the sample. About 45% are

[1] The total sample was balanced to match national population parameters for gender, age, education, race/ethnicity, region (U.S. Census definitions), Age x Gender, Age x Race/Ethnicity, and Race/Ethnicity x Gender. The basic weighting parameters came from the U.S. Census Bureau's Current Population Survey (February or March Supplement). NORC develops survey weights that are the product of three weights: weights that account for selection into the panel, weights that account for selection into the study, and weights that adjust survey non-response.

under age 45. Most have at least some higher education, and 28% report over $100,000 household income while 21% list it as below $30,000.

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

	%
Sex	
Male	49
Female	51
Age	
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
$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	26
Bachelor's degree	21
Post-graduate study/professional degree	15

* In this and all other tables, when the numbers don't add to 100% it is because of a 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 aren't 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 true-false statements we asked our sample to gauge what we call their

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

	True (%)	False (%)	DK (%)	Wrong (%)
When I go to a web site, it can collect information about my online behaviors even if I don't register using my name or email address.	**71**	5	24	30
A Smart TV can help advertisers send an ad to a viewer's smartphone based on the show they are watching.	**55**	7	38	45
A company can tell that I have opened its email even if I don't click on any links.	**52**	10	38	48
A website cannot track my activity across devices unless I log into the same account on those devices.	17	**46**	36	53
When 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
Facebook's user privacy settings allow me to limit the information about me that Facebook shares with advertisers.	**44**	20	36	56
All fifty states have laws requiring companies to notify individuals of security breaches involving personally identifiable information.	**43**	18	39	57
It is illegal for internet marketers to record my computer's IP address.	15	**40**	46	61
It is legal for an online store to charge people different prices depending on where they are located.	**38**	25	38	63
The doorbell company Ring has a policy of not sharing recordings with law enforcement without the homeowner's permission.	**37**	13	50	63
By 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
In the United States, the federal government regulates the types of digital information companies collect about individuals.	30	**24**	45	75
Some large American cities have banned the use of facial recognition technology by law enforcement	**30**	12	58	70
The US Federal government requires that companies ask internet users to opt-in to being tracked.	24	**30**	45	76
Section 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
The 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
Some 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

Bolded numbers indicate the correct answers. Numbers that don't add to 100 reflect rounding error.

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 don't log into the same account on those devices.

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 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 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 only one in seven knows that social media platforms do not activate users' smartphone speakers to listen to conversations and identify their interests in order 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.[31] 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 smart phones 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. 77 percent of our respondents failed the test by getting *at most* 53% of the questions (9/17) correct, and 15 percent received a D, having gotten at most a 65% score. Only 6 percent of the sample received a C, getting 71-76% of questions correct, and 1 percent got a B. One person in the entire sample received an A, and 6% got none of the answers correct.

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

	# 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%

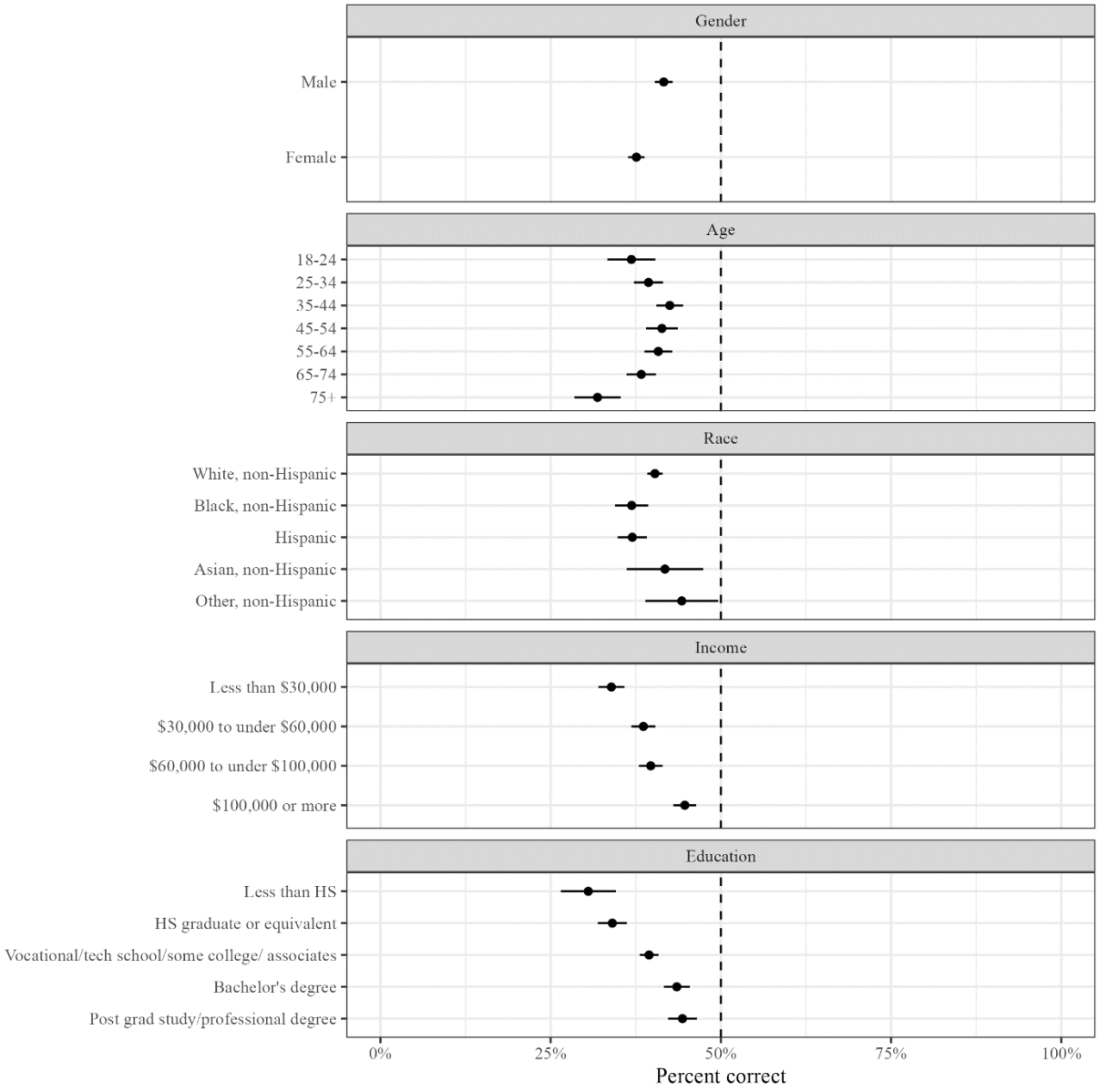
The numbers don't add to 100% because of rounding error.

There *are* statistically significant variations in navigational knowledge across U.S. society. As Figure 1 shows, scores go up substantially with income and formal education. The chart also shows that men on average get somewhat higher scores than women and that certain racial and ethnic groups differ in their scores. The age results are interestingly curvilinear: Average scores rise through 35-44-year-olds and then slide so that people aged 75 and older get the lowest grades. These differences, however, should not obscure the overriding finding: All the groups did very poorly, answering fewer than half the answers 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.

Americans Don't Believe They Can Control Their Data—Or That Companies Will Help Them.

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 don't believe they can. They also don't believe companies can be trusted to help them. We arrived at this conclusion by presenting our sample with twelve statements that plumb people's perception of their data control and company trust in nuanced ways.[32] 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

Figure 1. Average Knowledge Scores by Various Demographics



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."

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

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

	Strongly Agree (%)	Agree (%)	Disagree (%)	Strongly Disagree (%)	Neither* (%)
I want to have control over what marketers can learn about me online. **(91% agree)**	60	31	6	2	1
I would like to understand how digital marketers use the information they collect about my online activities **(87% agree)**	47	40	9	3	1
It would be naïve to think that I can reliably protect my personal data online. **(80% agree)**	36	45	14	4	1
I am not sure that I am taking the right steps to protect my digital data **(80% agree)**	28	52	16	3	2
I have come to believe that I have little control over what marketers can learn about me online. **(79% agree)**	26	53	16	5	1
I do not have the time to keep up with ways to control the information that companies have about me. **(73% agree)**	24	49	21	5	1
I trust myself to make the right decisions when it comes to handling my digital data. **(69% agree)**	22	47	25	4	2
I 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
I trust companies I visit online to handle my data the way I would want the data handled. **(28% agree)**	5	23	40	31	1
I 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

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

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 Don't 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 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

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

	Strongly Agree (%)	Agree (%)	Disagree (%)	Strongly Disagree (%)	Neither* (%)
If 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
If 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
It'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
I 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

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

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.

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 ten 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 of them*.

One statement was "I want to have control over what marketers can learn about me online." The other was "I've come to accept 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 percent 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.[2]

[2] Although there *are* variations of digital resignation across U.S. society, large percentages of all groups are resigned. There is no difference among genders when it comes to resignation. White Americans are more resigned (78%) than Asian Americans (68%) and Black Americans (62%). Those with more education are more resigned than those with less education. For example, of those that have more than a bachelor's degree, 84% report feeling resigned, and 70% of Americans with a high school education or less are resigned. The wealthier are also more likely to be resigned. Eighty-two percent of adults that earns $100,000 or more are resigned, while 65% of those who earn $30,000 or less are resigned. Younger adult Americans tend to be less resigned than older Americans. For example, 69% of Americans younger between 18 and 35 are resigned, while 80% of Americans older than 75 are resigned. In general, though, large percentages of the entire population across demographics are experiencing digital resignation.

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. Fully 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 (46%) 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.

Americans Want Congress to Act

Americans seem to understand that they have no real ability to consent to marketers' data gathering. In addition to showing that large percentages of Americans know little about key data practices and policies, we've shown that Americans acknowledge they know little, deeply mistrust companies to help them, are resigned that despite their objections firms will take and use data about them without their permission—and they believe that firms' doing that can harm them. 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?" Fully 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?

Concluding Remarks

Public Policy Toward Digital Marketers in An Age Where People Can't Consent

This study has found that overwhelmingly and to an extent not known before, Americans neither understand commercial surveillance practices and policies nor feel they are capable of doing anything about rampant data extraction. Americans also disagree with data trade-offs; that is, they don't think it is appropriate that companies should be allowed to extract data about them in return for using their platforms. The issue here is by no means merely "academic," confined to research findings. For the first time in human history, we live in a society where individuals are defined continually by data streams that circulate under the surface of everyday life. Companies have an ability to 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); to 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. Whether with first-party data, third-party data, or more, the goal is to give us tags or personas and have computers decide whether and how we ought to be the companies' targets.

Sometimes the firms know our names and sometimes they don't. Knowing our names makes it easier for the marketers to buy information about us than if they need to treat us anonymously. Don't let the claim of anonymity fool you, though. Marketers increasingly have found ways to match people who are anonymous (or who the companies make anonymous) in different places on the internet and give them single numerical identities that allow them to treat them as singular human beings wherever they are found. In that sense, it doesn't matter if person is Joseph Turow or YeshMispar70120—the ability to evaluate their worth and decide whether and how to target them remains.

Consider the patterned prejudicial discrimination these continual activities encourage. Because of the profiles marketers develop of individuals, some get better discounts than others, see different ads than others, get different offers than others. John may get low-end car ads while Jack gets high end ones. Jill may be invited to join certain marketers' clubs while Jane is left out. Jane may be among the people targeted for "depression and anxiety" based on an artificial intelligence model that links a HIPAA-compliant database to person-linked databases that identify her personally and predict her specific health conditions.[33] Her teenage daughter may be targeted with junk food commercials because firms know her above-average weight and food predilections. This kind of discrimination often overlaps with racial categorization. As Latanya Sweeney has shown, names that indicate racial identity can have a significant effect on the kinds of advertisements that appear on search platforms.[34] Just as troubling, perhaps, are the demographic, purchasing, lifestyle, and even personality categories that firms slot us in based on the data they have. 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 to advertisers in thousands of categories based on your

actions on Instagram, Facebook and elsewhere you don't know? As a result of all the pictures firms have about us, we are getting different views of the world, and different incentives to deal with that world, depending on the data streams firms collect and how they interpret them. 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.

Although informed consent is already difficult to come by, it will only become more difficult as time goes on. The downstream uses of consumer data are multiplying and diversifying. If consumers have trouble understanding how platforms use cookies to follow their online behavior in search of their preferences and interests, it seems unlikely that they will understand the vast data collection that powers machine learning or how individuals can be tracked in space in real time. Terms such as generative AI, OTT (over-the-top TV), CTV (connected television), 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? Based on that, do you want the firm to decide how long to keep you waiting or to triage you to an agent who is successful at satisfying and even "upselling" people with your emotions and purchase history? That already happens, and it indicates the rise of marketers peering into the human body for data.[35] 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.[36]

We have known about notice-and-consent's limitations for some time. This report now provides evidence that notice-and-consent may be beyond repair—and could even be harmful to individuals and society. Companies may argue they offer ways for people to stop such tracking. But as we have seen, a great percentage of the US 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.[37] 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 allows data collection for many reasons, consent is the one most used by marketers and other data collectors.[38] New state privacy laws are also based on consent. The California Consumer Privacy Act relies on opt- out consent.[39] 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.[40] 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.[41] 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.[42] These laws do little more than codify the legal structures that give data collectors dominion over consumers.

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.[43] 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 that this study calls for a paradigm shift in information-economy law and corporate practice. But consumers deserve privacy protections built into the information economy, protections that function without their need to become technology experts. We *are* seeing hints of some of these proposals in new privacy legislation. An early-stage proposal in New York as well as the Data Accountability and Transparency Act introduced by Ohio Democratic Senator Sherrod Brown nods to the idea that we cannot simply rely on individual rights and consent.[44] In one way or another, though, these bills still allow for individual consent. Lawmakers should go further by banning information-driven targeted advertisements and the sale of data about individuals for marketing use without waiting for individuals to click "Do Not Sell My Information" graphics.

We hope the findings of this study will further encourage all policymakers to flip the script so that the burden of protection from commercial surveillance is not mostly on us. The social goal must be to move us away from the emptiness of consent.

References

[1] U.S. Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems (1973), http://www.epic.org/privacy/hew1973report/.

[2] Daniel J. Solove & Woodrow Hartzog (2011), "The FTC and the New Common Law of Privacy," *Columbia Law Review* 114: 583-676.

[3] For example, the Children's Online Privacy Protection Act (COPPA) requires that websites that target minors ages 13 and under get parents' permission to collect data on children. 15 U.S.C. §§ 6501-6506 (Pub. L. 105–277, 112 Stat. 2681-728). COPPA is one of many sectoral consent-based federal privacy laws.

[4] Ari Ezra Waldman (2022), "The New Privacy Law," *University of California, Davis Law Review Online* 55: 19-41.

[5] Org. for Econ. Cooperation & Dev., OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2001),http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyan.

[6] Margot Kaminski & Meg Leta Jones (2020), "An American's Guide to the GDPR," *Denver Law Review* 98: 93-128 (p. 109)

[7] California Civil Code Sec. 1798.135.

[8] Bennett Cyphers, " How to Disable Ad ID Tracking on iOS and Android, and Why You Should Do It Now," Electronic Frontier Foundatiom, May 11, 2022, https://www.eff.org/deeplinks/2022/05/how-disable-ad-id-tracking-ios-and-android-and-why-you-should-do-it-now .

[9] Paul M. Schwartz (1999), "Privacy and Democracy in Cyberspace," *Vanderbilt Law Review* 52: 1609–1701.

[10] Jonathan A. Obar and Anne Oeldorf-Hirsch (2018), The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services, Information, Communication & Society, July 3, 1–20, https://doi.org/10.1080/1369118X.2018.1486870.

[11] Solon Barocas and Helen Nissenbaum (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, https://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf.

[12] Neil Richards and Woodrow Hartzog (2019), "The Pathologies of Digital Consent," *Washington University Law Review* 96: 1461-1503.

[13] Joseph Turow, Michael Hennessy & Nora Draper (2018) Persistent Misperceptions: Americans' Misplaced Confidence in Privacy Policies, 2003–2015, Journal of Broadcasting & Electronic Media, 62:3, 461-478, DOI: 10.1080/08838151.2018.1451867

[14] This is known as the "privacy paradox." Norberg, Patricia A., Daniel R. Horne, and David A. Horne (2007), "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors," *Journal of Consumer Affairs*, 41: 100–126.

[15] Media literacy scholars have recognized the challenges, sometimes even the limitations, of media-literacy education. See, for example, Douglas Kellner and Jeff Share (2005), "Toward Critical Media Literacy: Core Concepts, Debates, Organizations, and Policy," Discourse: Studies in the Cultural Politics of Education 26:3, 369-386, DOI: 10.1080/01596300500200169; Torres, M., & Mercado, M. (2006). The need for critical media literacy in teacher education core curricula, Educational Studies, *39:3*, 260–282. https://doi.org/10.1207/s15326993es3903_5 ; Nicole M. Lee (2018), Fake News, Phishing, And Fraud: A Call For Research On Digital Media Literacy Education Beyond The Classroom, Communication Education, 67:4, 460-466, DOI: 10.1080/03634523.2018.1503313 ; and Monica Bulger and Patrick Davison, Bulger, M., & Davison, P. (2018). The Promises, 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 .

[16] Philipp K. Masur (2019), "Reconceptualizing Online Privacy Literacy," March 28, https://philippmasur.de/2019/03/28/reconceptualizing-online-privacy-literacy/#easy-footnote-bottom-4-515 ; see also Philipp K. Masur (2020), "How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information," Media and Communication 8 (2).

[17] Sonia Livingstone, What Should We Teach Children About Online Privacy, and How? London School of Economics," June 24, 2019, https://blogs.lse.ac.uk/medialse/2019/06/24/what-should-we-teach-children-about-online-privacy-and-how/

[18] Corporation for Public Broadcasting. (2017). *Ruff Ruffman: Humble Media Genius: PBS kids*. Ruff Ruffman: Humble Media Genius | PBS KIDS. Retrieved January 17, 2023, from https://pbskids.org/fetch/ruff/

[19] National PTA and Norton. (2022, June 12). *Conversations that click*. The Smart Talk. Retrieved January 17, 2023, from https://thesmarttalk.org/

[20] Common Sense Media. (n.d.). *Digital Citizenship*. Common Sense Education. Retrieved January 17, 2023, from https://www.commonsense.org/education/digital-citizenship

[21] Patrick Gage Kelly, Joanna Bresee, Lorrie Faith Cranor, and Robert Reeder, A 'Nutrition Label' For Privacy, Symposium on Usable Privacy and Security (SOUPS), July 15-17, 2009.

[22] Girard K., Building a Better Nutrition Label for Privacy, Common Sense Media, https://www.commonsense.org/education/articles/building-a-better-nutrition-label-for-privacy , August 10, 2020, accessed on January 10, 2023.

[23] Sarah Perez (2022), Google Launches Its Own Privacy 'Nutrition Labels,' Following Similar Efforts By Apple, Techcrunch, April 26, https://techcrunch.com/2022/04/26/google-play-launches-its-own-privacy-nutrition-labels-following-similar-effort-by-apple/ .

[24] Geoffrey Fowler (2021), I Checked Apple's New Privacy 'Nutrition Labels.' Many Were False, *Washington Post*, January 29, https://www.washingtonpost.com/technology/2021/01/29/apple-privacy-nutrition-label/ .

[25] Helen Nissenbaum (2018), "Stop Thinking About Consent: It Isn't Possible and It Isn't Right," *Harvard Business Review*, September 24, https://hbr.org/2018/09/stop-thinking-about-consent-it-isnt-possible-and-it-isnt-right.

[26] Julie E. Cohen (2021), How (Not) to Write a Privacy Law, Essays and Scholarship, *Knight First Amendment Institute at Columbia University* (blog), March 23, https://knightcolumbia.org/content/how-not-to-write-a-privacy-law.

[27] Daniel J. Solove (2013), "Introduction: Privacy Self-Management and the Consent Dilemma," *Harvard Law Review* 126: 18801903.

[28] Ari Waldman (2021), *Industry Unbound*, Cambridge UK: Cambridge University Press, 52-57.

[29] This is similar to what Richards and Hartzog refer to as the "gold standard" of consent: "agreements between parties who have equal bargaining power, significant resources, and who knowingly and voluntarily agree to assume contractual or other legal obligations. Richards & Hartzog, "The Pathologies of Digital Consent," 1463.

[30] Turow, Joseph and Hennessy, Michael and Draper, Nora, The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation (June 26, 2015). Available at SSRN: https://ssrn.com/abstract=2820060 or http://dx.doi.org/10.2139/ssrn.2820060

[31] Sara Morrison (2022), "Should I Delete My Period App?" Vox, July 6, https://www.vox.com/recode/2022/7/6/23196809/period-apps-roe-dobbs-data-privacy-abortion ; Drew Harwell (2019), "Is Your Pregnancy App Sharing Your Intimate Data With Your Boss?" *Washington Post*, April 10, https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/ ; and Kashmir Hill, deleting your period tracker won't protect you, New York Times June 30, https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html

[32] These statements are adapted and adopted from other research on privacy cynicism, privacy fatigue, and digital resignation. Those sources include Hanbyul Choi, Jonghwa Park, and Yoonhyuk Jung (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; Christoph Lutz, Christian Pieter Hoffmann, and Giulia Ranzini. (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; Alice Marwick and Eszter Hargittai. (2019) Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society, 22*(12): 1697-1713. DOI: 10.1080/1369118X.2018.1450432; and Joseph Turow, Michael Hennessy, and Nora Draper. (2015). The Tradeoff Fallacy, Annenberg School for Communication.

[33] Center for Digital Democracy, "Trade Regulation Rule on Commercial Surveillance and Data Security," November 21, 2022. https://www.democraticmedia.org/sites/default/files/field/public-files/2022/cddsurveillancehealthftc112122.pdf

[34] Latanya Sweeney (2013), Discrimination in Online Ad Delivery: Google ads, black names and white names, racial discrimination, and click advertising, acmqueue, https://dl.acm.org/doi/pdf/10.1145/2460276.2460278

[35] See Joseph Turow (2021), *The Voice Catchers*, New Haven: Yale University Press.

[36] Michael Kearns and Aaron Roth (2019), *The Ethical Algorithm*. Oxford UK and New York: Oxford University Press.

[37] Adam Bear & Joshua Knobe (2017), *Normality: Part Descriptive, Part Prescriptive*, 167 COGNITION 25.

[38] GDPR, *supra* note 6, at art. 6(1).

[39] Cal. Civil Code § 1798.135(a)(5).

[40] Arizona S.B. 1614 §18-701(H); Arizona H.B. 2729 §§18-574(B), 18-577(G)(3).

[41] Illinois S.B. 2263 §30(3); Illinois S.B. 2330 §35(l)(3).

[42] Maine Rev. Stat. Ann. §9301(3) (2020).

[43] Ari Ezra Waldman (2022), "Privacy's Rights Trap," *Northwestern University Law Review Online* 117: 88-106.

[44] S. 2277, N.Y. Senate, 2023-2024 legis. sess.; S. ___, "Data Accountability and Transparency Act." 116th Cong. 2d sess., https://www.banking.senate.gov/imo/media/doc/Brown%20-%20DATA%202020%20Discussion%20Draft.pdf.