The Evolution of Consumer Attitudes Toward Online Tracking, 1995-2019

May 2020

Katie McInnis

Consumer Reports | Digital Lab

Investments from our members and philanthropic organizations including the Alfred P. Sloan Foundation, the Ford Foundation, and Craig Newmark Philanthropies support CR's efforts to promote consumer interests in relation to privacy, security, and data practices. This report was made possible by a grant from the Alfred P. Sloan Foundation.

Table of Contents

Executive Summary

Although consumers have been using the internet since the mid-1990s and have gained more technical literacy over time, consumers' increased understanding of the web could not and did not keep track with the increasingly sophisticated methods companies use to track consumers for advertising. The first large-scale consumer engagement with tracking technology came with the advent of tools for identifying and removing cookies in web browsers. Over time consumers have become more aware of advanced tracking methods—such as cross-device tracking and the correlation/combination of offline and online data.

Through an evaluation of over two decades of survey research regarding consumer adoption of new technology and understanding of tracking technologies, and the public's feeling towards the internet, we demonstrate that despite growing technical literacy consumers are unable to fully control when and how often they are tracked online. The period covered in this report, 1995-2019, is split into four periods based on attitudes: Cautious Users, Confident Users, Savvy Users, and Critical Users. Early internet users (1995-2004) exhibited a lot of caution in their use of the internet and had correspondingly strong feelings about the importance of their privacy. In the mid- to late-aughts (2005-2010), internet users were confidently taking advantage of new conveniences and features of the web. During the first-half of the 2010s (2011-2015), American consumers become more savvy users of the net and engage in more privacy-protecting activities like changing the default settings of their accounts. Finally, consumers of the late 2010s (2016-2019) exhibit more critical attitudes toward technology, yet also allow technology that collects sensitive information around the clock into their homes like smart speakers, TVs, and toys. In order to present how consumers currently feel about tracking techniques, Consumer Reports conducted a nationwide survey in July 2019.

During all four periods, the onus has been on the consumer to control their digital footprint. And since 1995, only a handful of legal protections have passed to aid consumers with this burden. Meanwhile (as shown by articles on, public discussion of, and controversy around whether or not Facebook is listening to users), tracking technology has progressed to the point that consumers are unable to keep pace with the ways advertisers, data brokers, and edge providers invade their privacy by collecting, using, and sharing their data. Therefore, in order to put the consumer back in control of their data, they do not need better advice on how to protect themselves online; they need a federal law that puts limits on collection and use of their data, and tools to aid that process or bridge the gaps that law is not able to fill.

I. Introduction

Consumers use the internet to fulfill and facilitate myriad tasks throughout their day, from navigating around town to keeping in touch with friends and family. However, in the course of these activities, consumers are, largely unwittingly, sharing a lot of personal information with entities both known and unknown to them. While consumers may understand that by using Gmail or Facebook they are sharing personal information with Google and Facebook, they are less aware that there are numerous trackers following them around the web and between devices collecting their personal information in order to better predict their behaviors and sell products or services to them. Consumers lack a deep understanding of this pervasive tracking because it has been obfuscated from the end user by design, and largely outsourced to vague, hard to find, read, and understand, and (at times) incorrect Privacy Policies and Terms of Service documentation. While the internet was created to be an "open and democratic platform for all,"[1] consumers now interact with a web that is no longer as open or transparent as its founders envisioned.

This paper seeks to chart consumers' understanding of tracking technologies in order to understand what barriers consumers face when trying to control how collects information about them. Pursuant to our grant from the Alfred P. Sloan Foundation, Consumer Reports[2] conducted a review of research into consumer perceptions of online tracking from the period of 1995 to 2019, using journal-published articles and studies and survey results from Consumer Reports, the Pew Research Center, and other studies on consumer privacy and tracking technologies. For the sake of completeness, this review also included survey results about other aspects of online life, including consumers' use and trust of online resources and consumers' assessment of the usefulness of the internet. The results have been divided into four segments: Cautious Users, 1995-2004; Confident Users 2005-2010; Concerned Users 2011-2015; and Critical Users, 2016-2019. These time periods have been chosen based on temporal differences in users' behaviors and attitudes with respect to the internet.

Although many individuals in the US have been using the internet since the mid-1990s, generally, consumers still struggle to understand the myriad ways they are tracked. In the late 1990s and early 2000s, consumer awareness of tracking began with the identification of phishing and spam emails, learning what a "cookie" is, and being aware that personal data is being gathered when they visit a website or open an email from them. Although more than half (56 percent) of adult internet users

[1] Katrina Brooker, *"I Was Devastated": Tim Berners-Lee, The Man who Created the World Wide Web, Has Some Regrets*, VANITY FAIR (July 1, 2018), https://www.vanityfair.com/news/2018/07/the-man-who-created-the-world-wide-web-has-some-regrets.

[2] Consumer Reports is the world's largest independent product-testing organization. It conducts its advocacy work in the areas of privacy, telecommunications, financial services, food and product safety, health care, among other areas. Using its dozens of labs, auto test center, and survey research department, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

in 2000 could not identify the primary online tracking tool (an HTTP cookie),[3] consumers still worried about their online privacy. For instance, more than half (54%) of adult internet users in that same survey thought that websites' tracking of users is harmful because "it invades their privacy."[4]

Consumers' increased use of the internet over time leads to greater awareness of advanced tracking practices like cross-device tracking. However, this increased understanding does not sufficiently empower consumers to control who collects their data due to the fact that most of these tracking methods are obscured and decentralized by design. Moments like the consumer backlash against the Facebook Beacon program in 2007, the reveal of Target's ability to predict pregnancy through purchase history in 2012, and the Cambridge-Analytica scandal in 2017 have taught advertising companies that consumers are more accepting of tracking they cannot see. The resulting environment is one in which consumers remain highly concerned about their privacy but lack knowledge about how tracking technologies are employed and their ability to effectively control online tracking. For example, most consumer tracking is currently so obscured from the user that individuals conclude that devices and apps published by large online companies (like Facebook) must be listening to their conversations in order to generate them. However, this environment is also the result of years of successful industry pressure and lobbying efforts[5] to prevent the passage of privacy laws and the abandonment of any self-regulatory[6] schemes[7] that were put forward.

Through an evaluation of surveys on consumers' understanding of tracking technologies, individuals' feelings toward and adoption of internet-enabled products and services, and concerns for their digital privacy and security, this report demonstrates the multitude of challenges consumers face when trying to control how much and how often they are tracked online. Consumers are concerned about their digital privacy but have few mechanisms that are easy and strong enough to stem the pervasive and intransparent tracking of their activities. And although consumers gain tech literacy over time, they are being told to do more and more to protect their privacy and the security of their data in order to keep pace with industries that work to prevent such consumer control over their information. In order to fully control who knows what about them, consumers must be given policy solutions (like mandated effective controls and data minimization by default) to accord industry practices with consumers' reasonable expectations.

---

[3] Susannah Fox, *Trust and Privacy Online*, PEW RESEARCH CTR. (Aug. 20, 2000), http://www.pewinternet.org/2000/08/20/trust-and-privacy-online/.

[4] *Id*.

[5] Carole Cadwalladr & Duncan Campbell, *Revealed: Facebook's Global Lobbying Against Privacy Laws*, THE GUARDIAN (Mar. 2, 2019, 9:00 AM), https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment; *Google, Facebook Hit Lobbying Highs as Privacy Heat Grows*, LAW 360 (Jan. 24, 2019, 10:17 PM), https://www.law360.com/competition/articles/1121861/google-facebook-hit-lobbying-highs-as-privacy-heat-grows.

[6] *See*, *e.g.*, Chris Hoffman, *RIP "Do Not Track," The Privacy Standard Everyone Ignored*, HOW-TO GEEK (Feb. 7, 2019, 4:04 AM), https://www.howtogeek.com/fyi/rip-do-not-track-the-privacy-standard-everyone-ignored/.

[7] *Online @ds*, CONSUMER WATCHDOG (2012), https://consumerwatchdog.org/newsrelease/consumer-watchdog-says-online-ad-industry-self-regulation-fails-protect-privacy-calls-co.

These policy solutions would therefore allow consumers to understand the ways in which they are tracked and how this information is used, in addition to giving them more control over the collection, use, and sharing of their data.

II. Cautious Users, 1995-2004

The first decade of consumer use of the web is marked by the public's concern about the security of their online transactions combined with growing adoption of internet-enabled services like email. During this time period consumers became more connected and grew more confident in their use of the web. People began to use the web to connect with friends, shop online, download music, and find health information. Consumers' trust in disclosing personal information and conducting financial transactions online increased during this time. Despite this increased trust in the infrastructure of the internet, consumers did not gain a correlative greater understanding of how their traffic was being monetized through user tracking. Although consumers understood they were being tracked across the web, many did not know how this tracking was conducted. For example, consumers expressed strong negative opinions about online tracking of their activities as early as 2000. However, more than half of all internet users in that year could not identify the HTTP cookie as the main mode of online tracking. Awareness of cookies grew only slightly by the early 2000s, but those who did know about this tracking technology took steps to protect their information.

A. Early Internet Adopters

While the creation of the world wide web dates back to 1989, the first browser was not launched until 1991[8] when Tim Berners-Lee introduced his WorldWideWeb browser (later termed Nexus).[9] Although the first image was uploaded to the net in 1992,[10] it was not until 1995 that a significant portion of the global population (44.4 million people, mostly in America) began using the internet and robust web-centered corporations, like eBay, Amazon, and Yahoo,[11] opened for business. In addition, the browser that the majority of the web would come to use, Internet Explorer, was not released until 1995. In the winter of 1994, five million Americans,[12] or 1.92 percent of the total US

[8] Martin Bryant, *20 Years Ago Today, the World Wide Web Opened to the Public*, THE NEXT WEB (Aug. 6, 2011), https://thenextweb.com/insider/2011/08/06/20-years-ago-today-the-world-wide-web-opened-to-the-public/ [hereinafter *20 Years Ago Today*].

[9] Tim Berners-Lee, *The WorldWideWeb Browser*, W3, https://www.w3.org/People/Berners-Lee/WorldWideWeb.html (last visited Aug. 26, 2019).

[10] *20 Years Ago Today*, *supra* note 8.

[11] Max Roser, *The Internet's History Has Just Begun*, OUR WORLD IN DATA (Oct. 3, 2018), https://ourworldindata.org/internet-history-just-begun

[12] Andrew Kohut et al., *Technology in the American Household: Americans Going Online...Explosive Growth, Uncertain Destinations*, TIMES MIRROR CTR. FOR THE PEOPLE & THE PRESS (Oct. 16, 1995), http://assets.pewresearch.org/wp-content/uploads/sites/5/legacy-pdf/136.pdf.

population,[13] subscribed to an online service. However, by 1995 4.5 percent of the US population were subscribers.[14]

Even in 1995, when the internet was young, consumers were worried about the privacy impacts of this new technology:

> A major fear of Americans about technology is the potential loss of privacy amid the powerful array of interconnected databases holding information about them. Half of all respondents expressed at least some uneasiness about privacy in the computer age: one-fifth (20%) said they worry "a lot" about this, while 30% worry "some." Online users were somewhat less concerned, with 12% expressing "a lot" of worry and 32% saying they worry "some" about it. People who go online from home are, in turn, less concerned than those who do so only at school or work (10% vs.16% worry "a lot").[15]

This concern was reflected in the federal government as well. In 1995, President Clinton's task force on privacy rules for these new communication services observed that "many people may be reluctant" to use the internet if they are "afraid that the personal information transmitted over it can be used in ways that are unexpected or inappropriate."[16]The task force's white paper continued, stating: "Thus, if government and the private sector want to encourage the vigorous consumer activity needed to unlock the full potential of the information infrastructure, they must acknowledge and safeguard the legitimate privacy interests of […] users."[17] However, the task force concluded that what the US needed was not an omnibus privacy law, but rather a voluntary framework predicated on a notice and consent model where companies would disclose information about their data practices to consumers prior to obtaining their consent to collect data about them.[18] This model allowed companies to "set the terms for user privacy, subject only to public acceptance of those terms rather than regulatory constraints."[19]

---

[13] This proportion was calculated by comparing the number of online Americans with the current population estimate for the U.S. at the time. *Historical National Population Estimates: July 1, 1900 to July 1, 1999*, U.S. CENSUS, https://www.census.gov/population/estimates/nation/popclockest.txt (last visited Aug. 26, 2019).

[14] This proportion was calculated by comparing the number of online Americans (Andrew Kohut et al., *supra* note 12) with the current population estimate for the U.S. at the time (*Historical National Population Estimates: July 1, 1900 to July 1, 1999*, U.S. CENSUS, https://www.census.gov/population/estimates/nation/popclockest.txt (last visited Aug. 26, 2019)).

[15] Andrew Kohut et al., *supra* note 12.

[16] *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information*, U.S. DEP'T OF COMMERCE, NAT'L TELECOMM. & INFO. ADMIN. (Oct. 1995), https://www.ntia.doc.gov/legacy/ntiahome/privwhitepaper.html.

[17] *Id*.

[18] "As stated above, NTIA's proposed framework draws upon the IITF's Principles and has two fundamental elements—provider notice and customer consent. Under NTIA's proposed framework, each provider of telecommunications and information services would inform its customers about what TRPI it intends to collect and how that data will be used. A service provider would be free to use the information collected for the stated purposes once it has obtained consent from the relevant customer. Affirmative consent would be required with respect to sensitive personal information. Tacit customer consent would be sufficient to authorize the use of all other information." *Id*.

[19] Anupam Chandler, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 666 (2014), *available at* http://law.emory.edu/elj/content/volume-63/issue-3/articles/how-law-made-silicon-valley.html.

In the late 90s, consumers began to be more concerned about the computerization of their medical records and the subsequent loss of privacy. In 1999, more than half of all US adults (54 percent) said that "the shift from paper record keeping systems to electronic or computer-based systems makes it more difficult to keep personal medical information private and confidential."[20] This concern about a lack of privacy for health information was due to worry about the actions of bad actors and hackers, rather than the disclosure of medical information by an authorized individual.[21] Although the Health Information Privacy and Portability Act (HIPAA) was passed in 1996,[22] this legislation did not fully assuage consumers' concerns about even authorized access to their private health information.

While the majority of consumers (60 percent) trusted their health care providers to keep their health information private all or most of the time, the same could not be said for health insurers: just over a third of US adults say they trust their health plan (35 percent) and government programs like Medicare (33 percent) to keep their information private all or most of the time.[23] Although improper disclosures generally decreased from 1993 to 1999,[24] 15 percent of US adults reported that they have taken an extraordinary step to keep their personal medical information confidential, like paying out-of-pocket to avoid disclosure, or asking a doctor not to record a health problem or record a less serious or embarrassing condition.[25]

The period of 1995-1999 also featured the introduction of a new kind of service for consumers: social networking sites. Sites like Classmates and[26] Six Degrees[27] were launched during this time period. However, while sites like Six Degrees had millions of users,[28] the site's growth was

---

[20] *Medical Privacy and Confidentiality Survey*, CALIF. HEALTH CARE FOUND. (Jan. 30, 1999), https://www.chcf.org/publication/medical-privacy-and-confidentiality-survey/.

[21] "Nationally, 55% say they worry more about computer hackers breaking into a system, while only 30% worry more about authorized users leaking information." *Id.*

[22] *HIPAA for Professionals*, U.S. DEP'T OF HEALTH & HUMAN SERV. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/index.html.

[23] *Id.*

[24] "A comparison of the new survey results with those of a 1993 Louis Harris survey for Equifax shows no evidence that violations of medical privacy have become more common over the past five years. In fact, reports of improper disclosure by health insurance companies (15% vs. 8%), public health agencies (10% vs. 4%), and hospitals (11% vs. 6%) are down significantly, compared to the 1993 results." *Id.*

[25] *Id.*

[26] Classmates was originally introduced as a site that hosted people's school affiliations. However, Classmates later evolved to allow users to create their own profiles and connect with friends. *Then and Now: A History of Social Networking Sites*, CBS NEWS, https://www.cbsnews.com/pictures/then-and-now-a-history-of-social-networking-sites/ (last visited Aug. 26, 2019).

[27] Six Degrees "is widely considered to be the very first social networking site. Founded by Andrew Weinreich in May 1996, the site launched the following year and combined popular features such as profiles, friends lists and school affiliations in one service. While the site had millions of registered users, due to the lack of people connected to the Internet, networks were limited. It would be a few years before the Internet's infrastructure could catch up with the concept of social networks." *Id.*

[28] *Id.*

hindered by the consumers' lack of a home internet connection.

B. New Users Expected Strong Privacy Protections Online, Demonstrate Low Technological Literacy

By the time the web was 11 years old, the average consumer had only been using it for around five years. Internet users at this time said they "overwhelmingly want the presumption of privacy when they go online."[29] However, these strong attitudes were not matched by consumer understanding of tracking techniques or use of privacy-protective tools.

By 2000, 19.5 percent of Americans reported being online.[30] And accordingly, "Americans' attachment to the internet [grew] along with the size of the online population," with 43 percent of online users reporting that they would miss going online "a lot" and half of internet users stating that they would miss email "a lot."[31] A Business Week Harris Poll found that the overwhelming majority of individuals disliked tracking and the creation of detailed profiles about them as consumers.[32] The majority of Americans wanted companies to seek their opt-in consent before sharing or collecting personal information: 86 percent of users wanted a website to obtain opt-in consent before collecting users' names, addresses, phone numbers, or financial information; 88 percent of users supported opt-in as the standard before a web site shares personal information with others; 89 percent of respondents were uncomfortable with web tracking schemes where data was combined with an individual's identity; and 91 percent were uncomfortable with information sharing that allowed tracking users across multiple web sites.[33] In addition, whether a site monetized the transfer or not, the vast majority of users did not want their information shared: 92 percent were uncomfortable with web sites that shared user information with other organizations; and 93 percent were uncomfortable with web sites that sold user information to other organizations.[34]

Even at this early date in the history of the internet, users had already demonstrated sensitivity for the kind of data they reveal. But this sensitivity skewed slightly more protective for physical information (address) than for digital (email, browsing habits). For instance, the vast majority (85 percent) of polled users expressed a strong desire for a website to get their permission every time before the site can use personal information like name, address, phone number or financial

---

[29] Susannah Fox, *supra* note 3.
[30] This statistic was calculated by comparing the total population in the U.S. (*The Population of the United States on April 1, 2000*, U.S. CENSUS, https://www.census.gov/census2000/states/us.html (last visited Aug. 26, 2019)) to the number of people who were online at that time (Lee Rainie et al., *Tracking Online Life*, PEW RESEARCH CTR. (May 10, 2000), http://www.pewinternet.org/2000/05/10/tracking-online-life/ [hereinafter *Tracking Online Life*].
[31] *Tracking Online Life*, *supra* note 30.
[32] *Business Week/Harris Poll: A Growing Threat*, BUS. WEEK (Mar. 2000), https://www.bloomberg.com/news/articles/2000-03-20/business-week-harris-poll-a-growing-threat.
[33] *Id*.
[34] *Id*.

information.[35] By comparison, users felt more comfortable with websites using digital information like their email address (78 percent wanted a website to get their permission every time), browsing habits, or shopping patterns (76 percent wanted a website to get their permission every time).[36] In addition, users reported a willingness to "punish firms and their executives when they violate users' privacy."[37] And 54 percent of internet users believed that websites' tracking of users is harmful because "it invades their privacy."[38]

Despite these strong feelings about the use of their private information, consumers lacked the corresponding knowledge of present tracking techniques and the availability of privacy-protecting tools. For instance, over half (56 percent) of US internet users could not identify the primary online tracking tool: an HTTP cookie.[39] And although the use and awareness of privacy protective tools was low (only nine percent of internet users used encrypted email, only five percent had used anonymizing software for browsing the web), consumers were more comfortable with giving false information online (24 percent of internet users had provided fake personal information in order to avoid giving a site their real information).[40]

By 2001, 56 percent of all Americans were online,[41] and the web was not only a place where people connect with their friends and family, but to shop,[42] find health information,[43] download music,[44] access news, conduct work-related research, and find information about their hobbies.[45] In addition, after the World Trade Center attacks on September 11, 2001, Americans used their access to the web for expressing their anger and sorrow[46] and reaching out to their family and friends.[47] Increasingly, the web was a place where individual users found communities and social connections.[48] Despite the growing prominence of the internet, most users did not feel comfortable

---

[35] A similar proportion of users (84 percent) also wanted a website to get their information before using their health information. *Id*.
[36] *Id*.
[37] Susannah Fox, *supra* note 3.
[38] *Id*.
[39] *Id*.
[40] *Id*.
[41] *Id*.
[42] John B. Horrigan, *The Holidays Online 2000*, PEW RESEARCH CTR. (Dec. 31, 2000), http://www.pewinternet.org/2000/12/31/the-holidays-online-2000/.
[43] Lee Rainie & Susannah Fox, *The Online Health Care Revolution*, PEW RESEARCH CTR. (Nov. 26, 2000), http://www.pewinternet.org/2000/11/26/the-online-health-care-revolution/.
[44] Amanda Lenhart & Susannah Fox, *Downloading Free Music*, PEW RESEARCH CTR. (Sept. 28, 2000), http://www.pewinternet.org/2000/09/28/downloading-free-music/.
[45] Dan Packel & Lee Rainie, *More Online, Doing More*, PEW RESEARCH CTR. (Feb. 18, 2001), http://www.pewinternet.org/2001/02/18/more-online-doing-more/.
[46] Lee Rainie, *How Americans Used the Internet After the Terror Attack*, PEW RESEARCH CTR. (Sept. 15, 2001), http://www.pewinternet.org/2001/09/15/how-americans-used-the-internet-after-the-terror-attack/.
[47] Lee Rainie & Bente Kalsnes, *The Commons of the Tragedy: How the Internet was Used by Millions After the Terror Attacks*, PEW RESEARCH CTR. (Oct. 10, 2001), http://www.pewinternet.org/2001/10/10/the-commons-of-the-tragedy-how-the-internet-was-used-by-millions-after-the-terror-attacks/.
[48] John B. Horrigan, *Online Communities*, PEW RESEARCH CTR. (Oct. 31, 2001), http://www.pewinternet.org/2001/10/31/online-communities/.

giving out their credit card or personal information over the internet,[49] and consumers seeking health information still valued the ability to get such information "anonymously" and worried about the storage of medical records online, even if the site was secured and password protected.[50]

By 2002, consumer knowledge of cookies as a device for online tracking rose from 43 percent in 2000[51] to 49 percent.[52] The knowledge of cookies grew with maturity of internet use (63 percent of those online for three or more years had heard of cookies, compared to 23 percent of those online for six months or less).[53] Despite their knowledge of cookies, 72 percent of mature users allowed for their browsers to accept these cookies, while only 56 percent of novice users changed their browser's default settings. Individuals who did not change their browser settings to block these cookies also appeared to trust the web more, since 90 percent of those users provided personal information over the web, while only 65 percent of people who changed their default settings (or were unsure) shared such information online.[54] Finally, 76 percent of all participants in a survey conducted by Peter Han and Angus Mclaurin stated that they were uncomfortable or very

---

[49] 72% of Internet users say they don't like giving out their credit card information or personal information over the Internet; and 41% say some Web sites make shopping online too confusing." Lee Rainie, *Holidays Online 2001*, PEW RESEARCH CTR. (Jan. 1, 2002), http://www.pewinternet.org/2002/01/01/holidays-online-2001/.

[50] "An overwhelming majority of Internet users who seek health information online are worried that others will find out about their activities: 89% of "health seekers" are worried that Internet companies might sell or give away information, and 85% fear that insurance companies might change their coverage after finding out what online information they accessed...63% of Internet health seekers and 60% of all Internet users oppose the idea of keeping medical records online, even at a secure, password-protected site, because they fear other people will see those records....80% of health seekers say it is important to them that they can get information anonymously. For the most part, users have not shared personal information at health Web sites: only 21% have provided their e-mail address; only 17% have provided their name or other identifying information; and only 9% have participated in an online support group about a health condition...81% of Internet health seekers want the right to sue a Web company if it violates its own privacy policy." Susannah Fox et al., *Exposed Online: The Federal Health Privacy Regulation and Internet User Impacts*, PEW RESEARCH CTR. (Nov. 19, 2001), http://www.pewinternet.org/2001/11/19/exposed-online-the-federal-health-privacy-regulation-and-internet-user-impacts/.

[51] "56% of Internet users cannot identify the primary online tracking tool. It is called a "cookie," and it is a text file that is placed on a user's computer by a Web site to help track that user's browsing activities. Despite Americans' high anxiety about being monitored online, only 10% of Internet users have set their browsers to reject cookies." Susannah Fox, *Trust and Privacy Online,* PEW RESEARCH CTR. (Aug. 20, 2000), http://www.pewinternet.org/2000/08/20/trust-and-privacy-online/.

[52] "Online users split on their knowledge of cookies: about half (49%) know what they are and half (49%) do not. A strong relationship exists between the knowledge of cookies and a user's experience online. A solid majority (63%) of those online for three or more years have heard of cookies, compared to 23 percent of the most novice users (online six months or less)." *A Matter of Trust: What Users Want from Web Sites*, CONSUMER WEBWATCH (a project of Consumer Reports) (Apr. 16, 2002), https://consumersunion.org/wp-content/uploads/2013/05/a-matter-of-trust.pdf [hereinafter *A Matter of Trust*].

[53] *A Matter of Trust*, *supra* note 52.

[54] "Those who know what a cookie is and have cookies enabled on their browser have a significantly different view on privacy and credit card protection than those who don't have them enabled or do not know about cookies. More than eight in ten (84%) of those who have cookies enabled use a credit card online compared to slightly more than half (55%) of those who don't allow cookies. More than nine in ten (90%) have provided personal information to Web sites, while just 65% of those who don't have cookies enabled have done the same. Those with cookies enabled are more likely to look at all of credit card protection policies compared with those whose browsers do not accept cookies (40% vs. 30%). The difference on privacy policies is not as great, but slightly more of those who have cookies enabled look at some of these policies compared with those not using cookies (53% vs. 46%)." *Id.*

uncomfortable with a company connecting user patterns (data made possible by cookies) on the internet to email addresses for a targeted email campaign.[55]

2002 also marked the year when search engines became "an indispensable utility for Internet users"[56] with the Google search engine securing the most-used search engine spot.[57] In addition, email had become an integral part of the American workplace, with studies showing that "about 62% of all employed Americans have Internet access and virtually all of those (98%) use email on the job." In 2002, the internet was also host to a new social media site: Friendster. Although "there were social networks that existed before Friendster, none of them engaged the mainstream with the same success."[58] Over its lifetime, the site experienced a number of technical issues that eventually pushed users away from the platform and towards another social network, Myspace. However, this website is credited as "giving birth to the modern social media movement."[59] Although social media was just beginning on the web, users continued to turn to the internet for a variety of tasks, such as playing video games,[60] downloading music,[61] and finding health information.[62]

Despite the increased use of the internet, consumers still fundamentally misunderstood what rights they had online and the realities of online tracking. For instance, most consumers (94 percent) agreed with this statement: "I have a legal right to know everything that a web site knows about me.," and 40 percent expressed distrust that major advertisers would protect their information and

[55] Peter Han & Angus Maclaurin, *Do Consumers Really Care About Online Privacy?*, 11 MARKETING MGMT. 35 (2002).

[56] Susannah Fox, *Search Engines*, PEW RESEARCH CTR. (July 2, 2002), http://www.pewinternet.org/2002/07/03/search-engines/.

[57] "According to comScore Media Metrix, Google is currently the most-used general search engine based on average minutes spent per usage month. Google garnered an average of 25.9 minutes per user in May 2002, an increase from 23.4 minutes in October 2001. Yahoo's average for May 2002 was 10.8 minutes per user and MSN averaged 5.9 minutes per user." *Id*.

[58] *Then and Now*, *supra* note 26.

[59] *Id*.

[60] "Seventy percent (70%) of college students reported playing video, computer or online games at least once in a while. Some 65% of college students reported being regular or occasional game players." Steve Jones, *Let the Games Begin: Gaming Technology and College Students*, PEW RESEARCH CTR. (July 6, 2003), http://www.pewinternet.org/2003/07/06/let-the-games-begin-gaming-technology-and-college-students/.

[61] "Two-thirds of those who download music files or share files online say they don't care whether the files are copyrighted or not; 35 million U.S. adults download music files online, 26 million share files online." Amanda Lenhart & Mary Madden, *Music Downloading, File-sharing and Copyright*, PEW RESEARCH CTR. (July 31, 2003), http://www.pewinternet.org/2003/07/31/music-downloading-file-sharing-and-copyright/.

[62] "Fully 80% of adult Internet users, or about 93 million Americans, have searched for at least one of 16 major health topics online. This makes the act of looking for health or medical information one of the most popular activities online, after email (93%) and researching a product or service before buying it (83%)." Susannah Fox & Deborah Fallows, *Internet Health Resources,* PEW RESEARCH CTR. (July 16, 2003), http://www.pewinternet.org/2003/07/16/internet-health-resources/.

not release it without the user's notice and consent.[63] However, no such legal framework existed to support rights over access to private data. Moreover, 57 percent believed that if a company has a privacy policy, the company will not share information with other entities[64] and yet 47 percent of internet users said website privacy policies were easy to understand.[65] Despite consumers' assertion that privacy policies are easy to understand, 59 percent did not know that websites collected information about them even without a registration requirement on the site.[66] However, most users thought a privacy law would be a good solution: 85 percent thought that a law that gave individuals the right to control how websites use and share information would either be very or somewhat effective in protecting privacy.[67]

C. Rise of Spam Posed Obstacles to Users

The prevalence of spam[68] continued to deter users from wider adoption and use of email: 60 percent of email users said "the ever-increasing volume of spam has reduced their email use in a big way" and 70 percent of email users said spam has made being online "unpleasant or annoying."[69] Their experience with spam emails led many users to use defensive tactics such as avoiding giving out their email address,[70] creating and using their own email filters,[71] or immediately deleting spam emails.[72] While spam presented both work and personal emailers with a growing problem,[73] consumers still had positive experiences online.[74]

---

[63] Joseph Turow, *Americans and Online Privacy: The System is Broken*, ANNENBERG SCHOOL OF COMMC'NS (June 2003), https://repository.upenn.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1411&context=asc_papers [hereinafter *The System is Broken*].

[64] *Id*.

[65] *Id*.

[66] *Id*.

[67] *Id*.

[68] "92% of email users agree that spam is "unsolicited commercial email from a sender they do not know or cannot identify." Deborah Fallows, *Spam: How it is Hurting Email and Degrading Life on the Internet*, PEW RESEARCH CTR. (Oct. 22, 2003), http://www.pewinternet.org/2003/10/22/spam-how-it-is-hurting-email-and-degrading-life-on-the-internet/.

[69] *Id*.

[70] "73% of email users avoid giving out their email addresses; 69% avoid posting their email addresses on the Web." *Id*.

[71] 37% of those who have a personal email account apply their own filters to their email system; 21% of those with filters say less than a tenth of the email they receive is spam." *Id*.

[72] "86% of email users report that usually they "immediately click to delete" their incoming spam." *Id*.

[73] Deborah Fallows, *Email at Work*, PEW RESEARCH CTR. (Dec. 8, 2002), http://www.pewinternet.org/2002/12/08/email-at-work/.

[74] "Internet users are very likely to say that they expect the Web to be a source of information on health care, government agencies, news, and shopping. About 80% of Internet users say they expect the Web to have information in these topic areas. These high expectations are driven by experience. Of Internet users who have sought information from the Web on these topics, about three-fourths have had positive experiences in finding what they need." Lee Rainie & John B. Horrigan, *Counting on the Internet: Most Find the Information they Seek, Expect*, PEW RESEARCH CTR. (Dec. 29, 2002), http://www.pewinternet.org/2002/12/29/counting-on-the-internet-most-find-the-information-they-seek-expect/; ""More than three quarters of the nation's Internet users (78%) did some form of holiday activity via email and the Web this holiday season. They used email to socialize and arrange holiday gatherings, reconnect with old friends, and plan religious activities. They browsed online malls and bought gifts in higher numbers than last

In 2003, LinkedIn launched and gained 4,500 members in its first month.[75] Although the site started as a place to post resumes, it soon evolved into a business networking site.[76]

By 2004, a significant number of users had created and uploaded content to the web, including building or posting to web sites, sharing files, and creating blogs.[77] Unfortunately, spam continued to plague users, even after the passage and enactment of the CAN-SPAM Act: 29 percent of users said that they used email less due to spam, and 63 percent of all users said that spam has eroded their trust in email.[78] Also in 2004, while interest in downloading music files began to fall (possibly due to an increase in suits against peer-to-peer music sharing[79]),[80] wireless internet usage was on the rise, as 17 percent of users reported logging on using a wireless device.[81] In addition, using online search engines was "a top online activity" and users "increasingly feel they get the information they want when they perform search queries."[82] Users also moved past email for online communications and increasingly turned to instant messages.[83] While individuals also began to use the internet to rate products or services,[84] those that did so were also more skeptical of the information they found on the web.[85]

---

year." John B. Horrigan & Lee Rainie, *Holidays Online 2002*, PEW RESEARCH CTR. (Jan. 7, 2003), http://www.pewinternet.org/2003/01/07/holidays-online-2002/.

[75] *Then and Now*, *supra* note 26.

[76] *Id*.

[77] "44% of Internet users have created content for the online world through building or posting to Web sites, creating blogs, and sharing files." Amanda Lenhart et al., *Content Creation Online*, PEW RESEARCH CTR. (Feb. 29, 2004), http://www.pewinternet.org/2004/02/29/content-creation-online/.

[78] Lee Rainie & Deborah Fallows, *The CAN-SPAM Act Has Not Helped Most Email Users So Far*, PEW RESEARCH CTR. (Mar. 17, 2004), http://www.pewinternet.org/2004/03/17/the-can-spam-act-has-not-helped-most-email-users-so-far/.

[79] Abhimanyu Ghoshal, A Nostalgic Look Back at Digital Music Piracy in the 2000s, THE NET WEB (Jan. 2019), https://thenextweb.com/insights/2018/12/28/a-nostalgic-look-back-at-digital-music-piracy-in-the-2000s/.

[80] "One in seven Internet users say they no longer download music files; The number of American Internet users who say they download music or share files online has increased slightly, but continues to sag well below peak levels." Lee Rainie et al., *14% of Internet Users Say They No Longer Download Music Files*, PEW RESEARCH CTR. (Apr. 25, 2004), http://www.pewinternet.org/2004/04/25/14-of-internet-users-say-they-no-longer-download-music-files/ [hereinafter *14% of Internet Users*].

[81] Lee Rainie, *The Rise of Wireless Connectivity and PIP's Latest Findings*, PEW RESEARCH CTR. (Apr. 13, 2004), http://www.pewinternet.org/2004/04/13/the-rise-of-wireless-connectivity-and-pips-latest-findings/.

[82] *14% of Internet Users*, *supra* note 80.

[83] "53 million adults trade instant messages and 24% of them swap IMs more frequently than email. IM also gains a following in U.S. workplaces" Eulynn Shiu & Amanda Lenhart, *How Americans Use Instant Messaging*, PEW RESEARCH CTR. (Sept. 1, 2004), http://www.pewinternet.org/2004/09/01/how-americans-use-instant-messaging/.

[84] "...26% of adult internet users in the U.S., more than 33 million people, have rated a product, service, or person using an online rating system." Lee Rainie & Paul Hitlin, *Use of Online Rating Systems*, PEW RESEARCH CTR. (Oct. 20, 2004), http://www.pewinternet.org/2004/10/20/use-of-online-rating-systems/.

[85] "Thirty-nine percent of those who believe that search engines are not fair and unbiased have participated in an online rating system as compared to 28% of those who do believe search engines are fair. Additionally, those who are "very confident" in their own internet searching abilities are more likely to have posted a rating compared to those who are either "not too confident" or "not at all confident" in their own abilities, 35% to 11%." *Id*.

Although Myspace was founded in 2003, the site did not launch until January 2004.[86] The site grew quickly, reaching one million users in February 2004, five million users in November 2004, and grabbing the number one most visited website in July 2006.[87]

D. Cautious Users Period

Although consumers during this time period began to use the web to fulfill a growing number of tasks, from expressing themselves to conducting their business online, concerns about privacy, security, and spam continued to worry users. Despite these issues, Americans engaged in new services, such as email, search engines, instant messaging, and social networks during this period. As more consumers became connected and grew confident using the internet, trust in disclosing personal information and conducting financial transactions online increased but an understanding of what tracking was or how to control tracking did not. Further complicating this environment, many users thought they had more privacy protections online by law than they did. In addition, the low level of internet adoption across the country during this time could have contributed to consumers' inability to understand how tracking worked since only a small proportion of the US was able to access the internet. In 2001, only 9.1 percent of US households had broadband internet connections.[88] By October 2003, this number had increased to 19.9 percent.[89] Although a significant number of Americans were using the internet by the close of this period, consumers as a whole had not gained sufficient technical literacy to understand what rights they had online and how they were being tracked. In subsequent years, more consumers would have access to the web, become more confident in their use of internet-enabled services, and correspondingly gain a greater understanding of how extensively they were tracked and how to prevent such tracking.

II. Confident Users, 2005-2010

During the second half of the aughts, the public was more confident in their ability to use the net and, correspondingly, had a better understanding of cybersecurity threats like malware and viruses. However, spam remained a chief issue for many users. Although the number of individuals using social media continued to increase, the social network providers were the focus of one of the first "tech-lashes" in the US following the release of the Facebook Beacon program. Despite the pushback Facebook received during this period, the company grew dynamically. Throughout this period, consumers became more aware of tracking technologies during this time period amid continued dislike for such tracking. Although consumers signaled their interest in a Do Not Track registry and desired more tools to protect their privacy, they still did not understand what terms

---

[86] *Myspace History: A Timeline of the Social Network's Biggest Moments*, HUFFPOST https://www.huffpost.com/entry/myspace-history-timeline_n_887059?slideshow=true#gallery/5bb385dce4b0fa920b9b4ab1/6 (last visited Aug. 26, 2019).

[87] *Id.*

[88] *A Nation Online: Entering the Broadband Age*, U.S. DEP'T OF COMMERCE, NAT'L TELECOMM. & INFO. ADMIN. (Sept. 2004), https://www.ntia.doc.gov/files/ntia/editor_uploads/NationOnlineBroadband04_files/NationOnlineBroadband04.pdf.

[89] *Id.*

are typically in a privacy policy and lack a complete understanding of tracking technologies. In addition, many consumers had false confidence in their ability to understand what a privacy policy signals to users and what terms are contained within.

A. Consumers Have Misplaced Confidence in their Knowledge of, and Ability to Defend Against, Tracking Methods

In 2005, the use of search engines continued to rise, with 84 percent reported usage across all internet users, of whom 92 percent said that they are "confident about their searching abilities."[90] Sixty-eight percent of all users stated that search engines are a fair and unbiased source of information.[91] Meanwhile, adoption of instant messaging capabilities grew likewise, with 42 percent reported usage among adults.[92] Spam messages also pervaded this service, with 30 percent of users reporting they have received unsolicited commercial instant messages.[93] Unsurprisingly, the adoption of wireless devices, like cell phones, continues to increase. Approximately 50 percent of all US adults were using cell phones, of whom 27 percent were using the text message feature.[94]

Even though it had been a full year since the enactment of the CAN-SPAM act, spam messages continued to frustrate users on all platforms, including 28 percent of those using text messaging (SMS) on their phone. [95] Despite the fact that fewer email users said that spam was undermining their email use, 52 percent of users said that spam was a "big problem" while a decreasing number (53 percent in 2005, compared to 62 percent in 2004) said that spam had made them less trusting of email.[96]

With greater adoption of internet-enabled services and products, survey research also started to delve deeper into consumers' understanding of tracking techniques. Even though consumers had a misplaced and inflated sense of knowledge, most consumers remained unaware of online tracking and how little protected their information had been online. While by 2005, 80 percent of adults knew that marketers "have the ability" to track them across the web and 62 percent knew

---

[90] Deborah Fallows, *Search Engine Users*, PEW RESEARCH CTR. (Jan. 23, 2005), http://www.pewinternet.org/2005/01/23/search-engine-users/.

[91] *Id*.

[92] Lee Rainie, *The Advent of Spim*, PEW RESEARCH CTR. (Feb. 21, 2005), http://www.pewinternet.org/2005/02/21/the-advent-of-spim/.

[93] *Id*.

[94] This proportion was reached through a comparison with the current population in the US (*United States of America Population, 2005*, PopulationPyramid.net, https://www.populationpyramid.net/united-states-of-america/2005/ (last visited Aug. 26, 2019)) with the population that used cell phones during this time (Lee Rainie, *The Rise of Cell Phone Text Messaging*, PEW RESEARCH CTR. (Mar. 14, 2005), http://www.pewinternet.org/2005/03/14/the-rise-of-cell-phone-text-messaging/).

[95] Lee Rainie, *The Rise of Cell Phone Text Messaging*, PEW RESEARCH CTR. (Mar. 14, 2005), http://www.pewinternet.org/2005/03/14/the-rise-of-cell-phone-text-messaging/.

[96] Deborah Fallows, *Spam and Phishing*, PEW RESEARCH CTR. (Apr. 10, 2005), http://www.pewinternet.org/2005/04/10/spam-and-phishing/.

that a company "can tell" if they have opened their marketing emails,[97] most are not similarly aware of profiling, behavioral targeting, and price discrimination tactics:

> Large majorities of internet-using U.S. do not understand key laws and practices relating to profiling, behavioral targeting and price discrimination. About half of the population does know some basics. About 50% recognize that most online merchants are allowed to share information with "affiliates" without the consumers' permission; that magazines can sell information about them without permission; and that merchants do not (and need not) allow consumers the opportunity to see or erase the information they gather about them. Moreover, about half seem to have caught the description of "phishing" and so answer it is false that banks "often send their customers emails that ask them to click on a link wanting them to verify their account."[98]

Despite this awareness of tracking methods, 75 percent of those surveyed did not realize that the presence of a privacy policy does not prohibit a site from sharing a visitor's information.[99] The majority of consumers also lacked knowledge about where to turn in the event that their information was used illegally.[100] Correspondingly, only 35 percent say they "trust(s) the U.S. government to protect consumers from marketers who misuse their information."[101] Consumers also lacked awareness of online and offline price discrimination[102] and yet disliked the practice and objected to most forms of behavioral targeting.[103] And although consumers were generally unaware of data sharing arrangements between common retailers,[104] they had strong feelings about the

---

[97] Joseph Turow et al., *Open to Exploitation: America's Shoppers Online and Offline*, ANNENBERG PUB. POLICY CENTER U. PENN. (June 1, 2005), https://repository.upenn.edu/cgi/viewcontent.cgi?article=1035&context=asc_papers [hereinafter *Open to Exploitation*].

[98] *Id*. at 17-18.

[99] *Id*.

[100] "Large majorities of internet-using U.S. adults do not know basic places to turn for help if their marketplace information is used illegally. The lack of understanding regarding marketplace laws and practices carries over to their understanding of where they can go for recourse if things do go wrong. Fully 76% agree incorrectly that "The Federal Trade Commission will correct errors in credit reports if it is shown proof of the errors." The FTC suggests that consumers contact one of the three national credit reporting agencies, Equifax, Experian, or TransUnion. Yet when asked "Can you give me the name of national Credit Reporting Agencies that can give you a copy of your credit report?" 66% of the respondents could not name any of them." *Id*. at 19.

[101] *Open to Exploitation, supra* note 97.

[102] "68% of American adults who have used the internet in the past month believe incorrectly that "a site such as Expedia or Orbitz that compares prices on different airlines must include the lowest airline prices...64% of American adults who have used the internet recently do not know it is legal for "an online store to charge different people different prices at the same time of day." "71% don't know it is legal for an offline store to do that." *Id*. at 3.

[103] "76% agree that "it would bother me to learn that other people pay less than I do for the same products. 64% agree that "it would bother me to learn that other people get better discount coupons than I do for the same products."66% disagree that "it's OK with me if the supermarket I shop at keeps detailed records of my buying behavior." 87% disagree that "it's OK if an online store I use charges people different prices for the same products during the same hour."72% disagree that "if a store I shop at frequently charges me lower prices than it charges other people because it wants to keep me as a custmer (sic) more than it wants to keep them, that's OK." *Id*. at 4.

[104] "72% do not know that charities are allowed to sell their names to other charities even without permission...64% do not know that a supermarket is allowed to sell other companies information about what they buy." *Id*. at 3.

potential dangers of this personal data being collected and shared.[105] In addition, the majority of users (66 percent) could not detect a phishing attempt.[106] However, consumers did practice some defensive techniques to avoid viruses or other unwanted software programs, like ceasing opening email attachments or not navigating to suspect sites.[107] Despite all of these indicators of consumers' lack of awareness of their rights and vulnerabilities online, the majority (65 percent) of internet users said they "know what I have to do to protect myself from being taken advantage of by sellers on the web."[108] Meanwhile, some online users had begun to use this new technology for selling products themselves.[109]

As a strong indication that users remained unaware of websites' and online services' data collection, consumers in 2003 and 2005 showed a clear lack of knowledge of what a privacy policy means for users. In both years, the majority of respondents (57 percent in 2003,[110] 59 percent in 2005[111]) agreed that the following statement is true: "When a web site has a privacy policy, I know that the site will not share my information with other websites or companies."

By this time, consumers had started using webcams[112] and viewing the web as an important source of news.[113] However, the top three activities on the web were still email, search engine use, and

---

[105] "Only 17% agree with the statement that "what companies know about me won't hurt me" (81% disagree), 70% disagree that "privacy policies are easy to understand," and 79% agree that "I am nervous about websites having information about me."" *Id. at* 4.

[106] "49% could not detect illegal "phishing"—the activity where crooks posing as banks send emails to consumers that ask them to click on a link wanting them to verify their account." *Id.* at 3.

[107] "81% of internet users say they have stopped opening email attachments unless they are sure these documents are safe. 48% of internet users say they have stopped visiting particular Web sites that they fear might deposit unwanted programs on their computers. 25% of internet users say they have stopped downloading music or video files from peer-to-peer networks to avoid getting unwanted software programs on their computers. 18% of internet users say they have started using a different Web browser to avoid software intrusions.
Tens of millions of Americans have been affected in the past year by software intrusions and many more have begun to take precautions by changing the way they use the internet. Overall, 91% of internet users say they have made at least one change in their online behavior to avoid unwanted software programs." Susannah Fox, *Spyware*, Pew Research Ctr. (July 6, 2005), http://www.pewinternet.org/2005/07/06/spyware/.

[108] *Open to Exploitation*, *supra* note 97.

[109] "17% of internet users – about 23 million people – have sold something online; Visits to classified ad web sites have grown 80% in the past year" Amanda Lenhart, *About 25 Million People Have Used the Internet to Sell Something*, PEW RESEARCH CTR. (Nov. 27, 2005), http://www.pewinternet.org/2005/11/27/about-25-million-people-have-used-the-internet-to-sell-something/.

[110] *The System is Broken*, *supra* note 63.

[111] *Open to Exploitation*, *supra* note 97.

[112] "One out of six American adult internet users (16%) have gone online to view another person or a place via a web cam. That translates into roughly 21 million people who have viewed material on web cams. And on any given day, about two million internet users are checking out remote places or people by using webcams." Lee Rainie, *Use of Web Cams*, PEW RESEARCH CTR. (June 20, 2005), http://www.pewinternet.org/2005/06/20/use-of-web-cams/.

[113] "The internet continues to grow as a source of news for Americans. One-in-four (24%) list the internet as a main source of news. Roughly the same number (23%) say they go online for news every day, up from 15% in 2000; the percentage checking the web for news at least once a week has grown from 33% to 44% over the same time period." Lee Rainie, *Online Newspapers Gain a Foothold*, PEW RESEARCH CTR. (June 27, 2005), http://www.pewinternet.org/2005/06/27/online-newspapers-gain-a-foothold/.

newsgathering, in that order.[114] Despite the fact that social media did not make it to one of the top three activities on the web, by 2006, Myspace was the number one most visited website.

B. Tech-lash Against Facebook

In September 2006, Facebook.com became accessible to users without an affiliated .edu email account.[115] By July 2007, the social networking site reached 30 million users, "making it the largest social-networking site with an education focus."[116] More than half of all teens aged 12-17 had a social media profile, and the majority of these teens (66 percent) limited access to their profile in some way.[117] Teen users who allowed their profiles to be viewed publicly used fake information as a defensive tactic with 46 percent of teen social media users reporting posting fake or false information on their profiles, both for protection and "to be playful or silly."[118] Although public posting on a friend's page was popular (84 percent of teen social media users had posted on a friend's page), the private messaging abilities of these sites was also very popular with 82 percent using this more private method of communication.[119]

The findings that teens care about their privacy is in accord with the reaction of students to the introduction of the Facebook News Feed. Facebook introduced this feature, which tracks and displays the online activities of a user's friends, on September 5, 2006. Although the updates from the user's friends were never private in the first place, "their aggregated public display on the start pages of all friends outraged Facebook users, who felt exposed and deprived of their sense of control over their information."[120] In response, one student created the Facebook group "Students Against Facebook News Feed (Official Petition to Facebook)," which attracted over 700,000 members.[121] Three days after releasing the feature, Facebook introduced privacy controls that allowed users to limit the audience for their activities on the site in response to public outcry.[122]

---

[114] Lee Rainie, *Big Jump in Search Engine Use*, PEW RESEARCH CTR. (Nov. 20, 2005), http://www.pewinternet.org/2005/11/20/big-jump-in-search-engine-use/.

[115] Sarah Phillips, *A Brief History of Facebook*, THE GUARDIAN (July 25, 2007, 5:29 PM), https://www.theguardian.com/technology/2007/jul/25/media.newmedia.

[116] *Id*.

[117] Amanda Lenhart & Mary Madden, *Social Networking Websites and Teens*, PEW RESEARCH CTR. (Jan. 7, 2007), http://www.pewinternet.org/2007/01/07/social-networking-websites-and-teens/ [hereinafter *Social Networking Websites*].

[118] Amanda Lenhart & Mary Madden, *Teens, Privacy, and Online Social Networks*, PEW RESEARCH CTR. (Apr. 18, 2007), http://www.pewinternet.org/2007/04/18/teens-privacy-and-online-social-networks/.

[119] *Social Networking Websites*, *supra* note 117.

[120] Bernhard Debatin et al., *Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences*, 15 J. OF COMPUTER-MEDIATED COMMC'N 83, 83–108 (Oct. 2009), *available at* https://doi.org/10.1111/j.1083-6101.2009.01494.x; *and*, *see*, danah boyd, *Facebook's Privacy Trainwreck*, 14 CONVERGENCE 13, 13-20 (Feb. 1, 2008), *available at* https://doi.org/10.1177/1354856507084416; https://www.newsweek.com/facebooks-news-feed-109521.

[121] Andrew Romano, *Facebook's 'News Feed'*, NEWSWEEK (Sept. 24, 20016 8:00 PM), https://www.newsweek.com/facebooks-news-feed-109521.

[122] danah boyd, *supra* note 120.

In November 2007, Facebook introduced its "Facebook Beacon" program which was built to send data from external sites to Facebook for the purpose of targeting advertisements and allowing users to share their online activities from these sites with their friends on Facebook via updates published in the News Feed.[123] Earlier in 2007, Facebook changed their privacy policy to allow the company to collect information about users without their consent and removed the opt-out option on their site.[124] This Beacon operated through the use of 1x1 pixel web beacon[125] published on a third-party sites which leveraged cookies from Facebook. Although users could block the publication of their activities to other users on Facebook, they could not opt-out of the information being sent to Facebook in the first place. (Users could clear their cookies after logging out of Facebook in order to prevent the third-party site from being able to communicate to Facebook that a specific user accessed their site.)

Despite Facebook's affirmations to the contrary, external sites still sent information to Facebook even if the user declined to share their activity with their friends and were logged out of Facebook due to the fact that the tools Facebook promised did not function as described.[126] The program was mired in controversy since its introduction. A Facebook group entitled "Petition: Facebook, Stop Invading My Privacy!" was launched and reached over 70,000 members within a few weeks.[127] By the end of November, MoveOn.org created a Facebook group which garnered 50,000 members in a little over a week and included a petition demanding that Facebook make the program opt-in rather than opt-out.[128]

In response to public pressure, Coca-Cola,[129] publicly dropped their use of the Beacon program and Facebook reversed their settings for the tool, changing it to an opt-in system.[130] In less than two years, Facebook would shut down this program entirely and create a $9.5 million foundation[131] to

---

[123] Vauhini Vara, *Facebook's Tracking of User Activity Riles Privacy Advocates, Members*, WALL ST. J. (Nov. 21, 2007, 12:01 AM), https://www.wsj.com/articles/SB119560466428899897?mod=technology_main_whats_news.
[124] Bernhard Debatin et al., *supra* note 120.
[125] "A Web beacon is an often-transparent graphic image, usually no larger than 1 pixel x 1 pixel, that is placed on a website or in an email that is used to monitor the behavior of the user visiting the Web site or sending the email. It is often used in combination with cookies." Vangie Beal, *Web Beacon*, WEBOPEDIA, https://www.webopedia.com/TERM/W/Web_beacon.html (last visited Aug. 26, 2019).
[126] Juan Carlos Perez, *Facebook's Beacon More Intrusive Than Previously Thought*, PC WORLD (Nov. 30, 2007, 4:10 PM), https://www.pcworld.com/article/140182/article.html.
[127] Bernhard Debatin et al., *supra* note 120.
[128] Caroline McCarthy, *MoveOn.org Takes on Facebook's 'Beacon' Ads*, CNET (Nov. 20, 2007, 12:00 PM), https://www.cnet.com/news/moveon-org-takes-on-facebooks-beacon-ads/
[129] Louise Story, *Coke is Holding Off on Sipping Facebook's Beacon*, N.Y. Times (Nov. 20, 2007, 3:53 PM), https://bits.blogs.nytimes.com/2007/11/30/coke-is-holding-off-on-sipping-facebooks-beacon/.
[130] Mark Zuckerberg, *Thoughts on Beacon*, THE FACEBOOK BLOG (Dec. 5, 2007 7:00 AM), http://blog.facebook.com/blog.php?post=7584397130 [*retrieved via* THE WEB ARCHIVE on May 22, 2019].
[131] This organization became known as the Digital Trust Foundation and operated from 2014-2019 in order to fund projects to promote online safety, security, and privacy. DIGITAL TRUST FOUND., https://www.digitaltrustfoundation.org/ (last visited Aug. 26, 2019).

promote online privacy[132] as part of a settlement of a class action lawsuit,[133] alleging the company had broken the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and the Video Privacy Protection Act, among others.[134] Beacon, which Facebook introduced as service for users that would be like receiving a "recommendation from a trusted friend,"[135] damaged Facebook's reputation. In addition, the Beacon program led many to be skeptical of the motives of companies like Facebook and raised worries "that Facebook and other profit-oriented social networking sites are large Internet-based surveillance machines."[136] However, it appears that a takeaway from the Beacon experiment for companies was to lean into surveillance while removing the transparency of pervasive data collection and subsequent monetization of this collection:

> The *Facebook* Beacon was quickly met with resistance because of privacy concerns and was changed to an opt-in system rather than a set feature of the website. This software change could be interpreted as a victory against the alienation of users from the information they provide, yet this is far from being the case. The Beacon, after all, was a visual representation of processes of commercialization that are still taking place on the *Facebook* platform. These processes, however, increasingly take place at the back-end level and because they are invisible to users, they meet with less resistance.[137] [Citation omitted.]

Online tracking by other companies is more obscured from the end user, perhaps in part to ensure that the following statement from an article in 2007 remains true: "the average American consumer is largely unaware that such tracking goes on, the extent to which it is happening or how exactly information is being used."[138] Furthermore, the transparency of such tracking was likely a mistake on behalf of Facebook:

> For the average user, however, Facebook-based invasion of privacy and aggregation of data, as well as its potential commercial exploitation by third parties, tend to remain invisible. In this respect, the Beacon scandal was an accident, because it made the users aware of Facebook's vast data-gathering and behavior surveillance system. Facebook's owners quickly learned their lesson: The visible part of

---

[132] Cade Metz, *Facebook Turns Out the Light on Beacon*, THE REGISTER (Sept. 23, 2009, 12:18 AM), https://www.theregister.co.uk/2009/09/23/facebook_beacon_dies/.

[133] John Oates, *Facebook Sued for Beacon Blunder*, THE REGISTER (Aug. 15, 2008, 8:17 AM), https://www.theregister.co.uk/2008/08/15/faceboo_beacon_sued/.

[134] Chloe Albanesius, *Facebook Hit by Class Action Suit over 'Beacon,'* PCMAG (Aug. 14, 2008, 2:47 PM), https://www.pcmag.com/news/230913/facebook-hit-by-class-action-suit-over-beacon.

[135] Louise Story & Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES (Nov. 30, 2007), https://www.nytimes.com/2007/11/30/technology/30face.html.

[136] Christian Fuchs, FOUNDATIONS OF CRITICAL MEDIA AND INFORMATION STUDIES, p. 1 (2011) New York: Routledge. ISBN 978-0-415-58881-2.

[137] Ganaele Langlois et al., *FCJ-095 Mapping Commercial Web 2.0 Worlds: Towards a New Critical Ontogenesis*, 14 FIBRECULTURE J. (2009), http://fourteen.fibreculturejournal.org/fcj-095-mapping-commercial-web-2-0-worlds-towards-a-new-critical-ontogenesis/.

[138] Jaikumar Vijayan, *Most Consumers Clueless about Online Tracking, Behavior Profiling*, COMPUTERWORLD (Nov. 1, 2007), https://www.computerworld.com/article/2539890/data-privacy/most-consumers-clueless-about-online-tracking--behavior-profiling.html.

> Facebook, innocent-looking user profiles and social interactions, must be neatly separated from the invisible parts. As in the case of an iceberg, the visible part makes up only a small amount of the whole.[139]

Beacon was Facebook's first effort to connect the walled garden of the social media site to the user's activities off the site. Beacon was one of the company's first forays into tracking both users and non-users for the purposes of advertising. In 2008, Facebook needed to create "an enduring stream of advertising revenue."[140] Indeed, at that time it was unclear how Facebook or another social media platform could create this opportunity for advertising revenue:

> A survey last week from the research firm IDC suggested that social networks were a miserable place for advertisers: just 57 percent of all users of social networks clicked on an ad in the last year, and only 11 percent of those clicks led to a purchase, IDC said. And it turns out that marketers are not so interested in advertising on pages filled with personal trivia and relationship updates.[141]

Following the Beacon experiment, Facebook introduced another feature for consumers: Facebook Connect.[142] Facebook Connect allows users to sign onto third-party websites or applications using their Facebook identity.[143] Once logged in, users can then connect with Facebook friends on those platforms and post updates to their Facebook profile.[144]And although Facebook stated at the time that it "had no plans to explore any other advertising potential with Connect,"[145] this service enabled Facebook to combine data it already had about its users (like their real identities, who they associate with, and what they like and dislike) with information from third-parties websites about what those users do on their sites. The combination of these data sets set Facebook up to better serve targeted ads to their 120 million members worldwide.[146]

C. Wider Adoption of Social Media, with Many Changing Default Settings

In 2008, Facebook secured the spot of the number one social network. Although competitor

---

[139] Bernhard Debatin et al., *supra* note 120.
[140] Brad Stone, *Facebook Aims to Extend Its Reach Across the Web*, N.Y. TIMES (Nov. 30, 2008), https://www.nytimes.com/2008/12/01/technology/internet/01facebook.html.
[141] *Id*.
[142] Josh Cantone, *Facebook Connect is Beacon Done Right*, SITEPOINT (July 24, 2008), https://www.sitepoint.com/facebook-connect-is-beacon-done-right/
[143] Dave Morin, *Announcing Facebook Connect*, FACEBOOK DEVELOPERS (May 9, 2008), https://developers.facebook.com/blog/post/2008/05/09/announcing-facebook-connect/ [*retrieved via* THE INTERNET ARCHIVE on May 21, 2019 https://web.archive.org/web/20120910000405/https://developers.facebook.com/blog/post/2008/05/09/announcing-facebook-connect/].
[144] *Id*.
[145] *Id*.
[146] *Id*.

Myspace attempted several re-designs, Myspace never regained its dominance.[147] A 2008 survey demonstrated that consumers' knowledge of online tracking techniques had increased, with 71 percent of online consumers being aware that their browsing information may be collected by a third party for advertising purposes.[148] However, consumers were largely unfamiliar with the term "behavioral targeting."[149] In general, the results from this survey indicated that US consumers were aware of being tracked for targeted advertising purposes and disliked such tracking. For instance, 57 percent stated that they were not comfortable with advertising using their browsing history to tailor ads, even if the information could not be tied to their identity. Furthermore, almost all of those surveyed (91 percent) said they would be willing to take steps to protect their privacy online.[150] Finally, the majority of consumers (64 percent) expressed a desire to see ads only from the brands they know and trust.[151]

In 2009, with social media use still on the rise, 35 percent of American adults had created a profile on a social media site.[152] This level of engagement was four times the rate of adult social media participation just four years prior.[153] In spite of this growth, more teens were using social media sites, with 65 percent of all US teens using social networks.[154] While newer to this kind of site, adult users largely restricted access to their profile, with 60 percent of adult social network users using their privacy settings to ensure that only their friends could see their profile.[155]

Further proving that both teens and adults value the ability to limit who accesses their online information, a survey conducted in the same year showed that "younger adults have as strong an aversion to being followed across websites and offline...as do older adults."[156] Most Americans (66 percent) do not want marketers to tailor advertisements to their interests.[157] Once the participants were informed about how these marketers gather the information they use to target advertisements to users, the percentage of people who did not want such advertising increased.[158]

By 2010, users had developed a sense of an "online identity" or a digital self: 57% of adults have used search engines to find information about themselves online; 56% of social media users have

---

[147] *Then and Now*, *supra* note 26.
[148] *TRUSTe Report Reveals Consumer Awareness and Attitudes About Behavioral Targeting*, TRUSTE (Mar. 28, 2008), https://danskprivacynet.files.wordpress.com/2009/02/truste2008_tns_bt_study_summary1.pdf.
[149] *Id*.
[150] *Id*.
[151] *Id*.
[152] Amanda Lenhart, *Adults and Social Network Websites*, PEW RESEARCH CTR. (Jan. 14, 2009), http://www.pewinternet.org/2009/01/14/adults-and-social-network-websites/.
[153] *Id*.
[154] *Id*.
[155] *Id*.
[156] Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It*, ANNENBERG PUB. POLICY CENTER U. PENN. (Sept. 29, 2009), https://ssrn.com/abstract=1478214 [hereinafter *Americans Reject Tailored Advertising*].
[157] *Id*.
[158] *Id*.

"unfriended" others; 65% of social media users had limited what they share with others online; and 33 percent of all users had worried about what information is available about them online.[159] Two-thirds of all adults reported sleeping with their cell phones by their side,[160] and seven percent of all users who accessed the internet via their phones had started using location-based services.[161] Social media use continued to rise, with 62% of internet-connected adults active on social media sites like Facebook, Myspace, or LinkedIn and 24 percent of connected adults using Twitter or another site to share updates about themselves.[162]

D. Concerns about Online Tracking Persist

A 2010 study found that the vast majority of their participants associate the word "pop-ups" with "internet advertising,"[163] and many participants described banner ads and other ads on websites they visit as "pop ups."[164] Individuals also associated "internet advertising" with spam and expressed dislike for any form of ad.[165]

Most of the participants could identify that Google's main business was advertising and understood where and when Google search displays ads.[166] However, there was continuing confusion around what a cookie is and what it does. In addition, consumers could not identify which parts of a New York Times page were advertisements.[167] Eighty-six percent of the study participants believed advertisements were tailored based on websites visited in the past, but only 39 percent believed that advertisements were also based on email content via Gmail. Even though these participants did not exhibit a full understanding of tracking technology, the majority (64 percent) found the practice of tailoring advertisements to be invasive.[168]

E. Confident Users Period

Despite consumers' confident adoption of new services like social media, most Americans continued to have a lot of trepidation about tracking and their online privacy. Although angst over tracking ebbs and flows over this period, this time also featured another wide-scale engagement with tracking technology through consumers' use of social media platforms. Individuals engaged

---

[159] Mary Madden & Aaron Smith, *Reputation Management and Social Media*, PEW RESEARCH CTR. (May 26, 2010), http://www.pewinternet.org/2010/05/26/reputation-management-and-social-media/.
[160] Amanda Lenhart, *Cell Phones and American Adults*, PEW RESEARCH CTR. (Sept. 2, 2010), http://www.pewinternet.org/2010/09/02/cell-phones-and-american-adults/.
[161] Kathryn Zickuhr & Aaron Smith, *4% of Online Americans Use Location-Based Services*, PEW RESEARCH CTR. (Nov. 4, 2010), http://www.pewinternet.org/2010/11/04/4-of-online-americans-use-location-based-services/.
[162] *Id*.
[163] Aleecia McDonald & Lorrie Cranor, *Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising*, TPRC (Aug. 16, 2010), http://aleecia.com/authors-drafts/tprc-behav-AV.pdf.
[164] *Id*.
[165] *Id*.
[166] *Id*.
[167] *Id*.
[168] *Id*.

in tracking technology not by identifying and blocking cookies but rather through controlling who views their private information, either at the settings or company policy level. Social media users often changed their default settings, used defensive tactics like posting false information about themselves, and pushed back against platform decisions that negatively impacted their personal privacy. Despite this higher level of engagement, individuals also had a lot of misplaced confidence about their ability to understand privacy policies and their understanding of what rights they had online. Consumers did, however, gain a greater awareness that they were being tracked and continued to find such tracking invasive.

IV. Concerned Users, 2011-2015

By 2011, consumers were confident and enthusiastic users of the web. However, privacy concerns continued to pervade their adoption and use of new technologies and services. Consumers showed a greater understanding that their information is not as private as previously thought and that their actions were being tracked online through revelations such as Target's ability to predict a shopper's pregnancy and the Snowden disclosures of 2013. Although Facebook had become the dominant social network in 2013, users also reported taking breaks regularly post-Snowden in 2014. In addition, concerns over access and collection of personal information had hit an all-time high. In this period, consumers also made more use of privacy-protective settings as evolution of the smartphone brought with it increased tracking capability.

A. Growing Awareness of Tracking, Persistent Concerns about Privacy

In 2011, the majority of consumers (74 percent) said they were aware of programs on their computer that tracked their behavior and personal details, but even more consumers (80 percent) desired an end to such tracking.[169] However, awareness of tracking technologies also corresponded with income levels, as found in a poll conducted the same year: "Among people who earn less than $20,000 a year, 60% understand tracking. Awareness soared to 84% among people earning over $75,000."[170] The finding of this study was backed up by another survey in that year which found that 70 percent of participants were "aware of the concept of online behavioral advertising."[171] With half of all US adults using social media sites,[172] many more people (68 percent) reported using location-based services by either "checking in" at a physical location or using a location-based information service.[173] Some social media users (14%) even allowed their online accounts to

[169] Christopher Ming, *Poll: Americans Understand Online Tracking. And They Don't Like It*, CREDIT (Feb. 15, 2011), https://www.credit.com/blog/2011/02/poll-americans-understand-online-tracking-and-they-dont-like-it/.
[170] *Id.*
[171] *2011 Consumer Research Results: Privacy and Online Behavioral Advertising*, TRUSTE (July 25, 2011), https://www.eff.org/files/truste-2011-consumer-behavioral-advertising-survey-results.pdf.
[172] Mary Madden & Kathryn Zickuhr, *65% of Online Adults Use Social Networking Sites*, PEW RESEARCH CTR. (Aug, 26, 2011), http://www.pewinternet.org/2011/08/26/65-of-online-adults-use-social-networking-sites/ [hereinafter *65% of Online Adults*].
[173] Kathryn Zickuhr & Aaron Smith, *28% of American Adults Use Mobile and Social Location-Based Services*, PEW RESEARCH CTR. (Sept. 6, 2011), http://www.pewinternet.org/2011/09/06/28-of-american-adults-use-mobile-and-social-location-based-services/.

automatically include their current location when they posted on sites.[174] These permissive sharing practices, despite the growing awareness of online tracking, may have stemmed from people's attitudes towards social media platforms, with users overwhelmingly describing their experiences on these platforms with positive adjectives.[175]

During this period, researchers Avi Goldfarb and Catherine Tucker conducted an eight-year longitudinal study that showed that refusals to reveal information had risen over time.[176] This trend was due in part to a growing awareness of the various contexts in which privacy is relevant,[177] but also due to the fact that traditional data collection schemes can alert consumers to the vast amounts of personal data companies collect, control, and infer about them. For instance, in 2012, the retailer Target was able to guess correctly that a teenager in Minnesota was likely pregnant by combining her customer data (purchasing history) with demographic data the company collected or purchased from other sources, and comparing this data with historical buying data for customers who had signed up for Target baby registries in the past. Target's powerful ad targeting system was able to ascertain the girl's pregnancy before she was even able to tell her family.[178]

Not only was this a radicalizing moment for the public, who is generally alarmed a company has this ability, it is also a moment of change for Target. The company, realizing that highly accurate ads can make people uneasy, started to mix in unrelated ads into their targeted coupon booklets: "And we found out that as long as a pregnant woman thinks she hasn't been spied on, she'll use the coupons...As long as we don't spook her, it works."[179] Consumers have interacted with algorithms in the past, but for many, this served as the first realization of a retailer's ability to predict an individual's purchasing behavior.

In this year, a majority of all social media users, 58 percent, restricted access to their social media profiles[180] and 68 percent of internet users disapproved of targeted advertising because they did not want their online behavior to be tracked and analyzed.[181] Reinforcing this finding, a study by Carnegie Mellon University reported that consumers found behavioral advertising to be privacy

---

[174] *Id*.

[175] "When social networking users were asked for one word to describe their experiences using social networking sites, "good" was the most common response. Overall, positive responses far outweighed the negative and neutral words that were associated with social networking sites (more than half of the respondents used positive terms). Users repeatedly described their experiences as "fun," "great," "interesting" and "convenient." Less common were superlatives such as "astounding," "necessity," and "empowering."" *65% of Online Adults, supra* note 172.

[176] Avi Goldfarb & Catherine Tucker, *Shifts in Privacy Concerns*, 102(3) AMER. ECON. REV. 349, 349-53 (2012), https://www.aeaweb.org/articles?id=10.1257/aer.102.3.349.

[177] *Id*.

[178] Charles Dihigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=6&_r=1&hp.

[179] *Id*.

[180] Mary Madden, *Privacy Management on Social Media Sites*, PEW RESEARCH CTR. (Feb. 24, 2012), http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/.

[181] Kristen Purcell et al., *Search Engine Use 2012*, PEW RESEARCH CTR. (Mar. 9, 2012), http://www.pewinternet.org/2012/03/09/search-engine-use-2012/.

invasive as well as useful.[182] The individuals in their study were "surprised to learn that browsing history is currently used to tailor advertisements, yet were aware of contextual advertising."[183] Furthermore, the participants in this study misinterpreted the very disclosures and icons that were meant to notify them about online behavioral advertising.[184] This study concluded that if consumers were provided with effective notice about the practice of tailoring ads, they would not need to understand the technologies used to target consumers with ads—which is normally a significant complicating factor for consumer understanding.[185] However, notice and choice mechanisms have been "ineffective" and consumers have not been provided with context-dependent preferences for the privacy of their data; instead, each company only provides individuals with the mechanism to opt out of targeting by that company alone—there had been and is not a universal opt-out setting.[186] Although the majority (90 percent) of those surveyed in a different study reported that they had never heard of the Federal Trade Commission's (FTC) Do Not Track mechanism, most consumers favored this approach.[187]

Regardless of the fact that consumers had been consistently eager to take advantage of the features afforded to them by new technology, such as the ability to use location-based services on their phones (75 percent of smartphone users either location-based services or check into locations using their phone[188]), privacy concerns affected their adoption of new services, with more than half of all app users (57 percent) reporting that they had uninstalled or decided not to install an app due to concerns about their data privacy.[189]

In 2013, almost three quarters of adults online use a social networking site,[190] and the majority of US adults (67 percent) are on the dominant social network site, Facebook.[191]And although users report taking breaks from the site, these breaks are largely sparked by a need to focus on other demands or a lack of interest in the site[192] rather than a concern about their privacy. With the growing use of smartphones and other connected products, consumers also were becoming more

---

[182] Blase Ur et al., *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising*, CYLAB (Apr. 2, 2012), https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab12007.pdf.
[183] *Id*.
[184] *Id*.
[185] *Id*.
[186] *Id*.
[187] Chris Hoofnagle et al., *Privacy and Modern Advertising: Most US Internet Users Want 'Do Not Track' to Stop Collection of Data about their Online Activities*, BERKELEY CONSUMER PRIVACY SURVEY (Oct. 8, 2012), https://ssrn.com/abstract=2152135.
[188] Kathryn Zickuhr, *Three-quarters of Smartphone Owners Use Location-Based Services*, PEW RESEARCH CTR. (May 11, 2012), http://www.pewinternet.org/2012/05/11/three-quarters-of-smartphone-owners-use-location-based-services/.
[189] Jan Lauren Boyles et al., *Privacy and Data Management on Mobile Devices*, PEW RESEARCH CTR. (Sept. 5, 2012), http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/.
[190] Joanna Brenner & Aaron Smith, *72% of Online Adults are Social Networking Site Users*, PEW RESEARCH CTR. (Aug. 5, 2013), http://www.pewinternet.org/2013/08/05/72-of-online-adults-are-social-networking-site-users/.
[191] Lee Rainie et al., *Coming and Going on Facebook*, PEW RESEARCH CTR. (Feb. 5, 2013), http://www.pewinternet.org/2013/02/05/coming-and-going-on-facebook/.
[192] *Id*.

aware of tracking techniques and the means to thwart them. For example, a 2013 survey found that the majority, of internet users (86 percent) had taken steps to mask or remove their digital footprints through methods like avoiding using their name and employing virtual private networks (VPNs) and 55 percent of users had taken steps to avoid observation by the government or specific people or organizations.[193] In addition, a Pew Study on Anonymity, Privacy, and Security Online found that a growing number of users (50 percent) "are worried about the amount of personal information about them that is online—a figure that has jumped from 33% who expressed such worry in 2009."[194] Despite these concerns, more and more individuals were allowing their social media accounts to automatically include their location in their posts, from 14 percent in 2011[195] to 30 percent in 2013.[196]

In 2014, the vast majority of users (90 percent) said that the internet had been good for them personally and most thought it has also been a benefit to society (76 percent).[197] Despite these positive attitudes toward the internet as a whole, consumers still disliked being tracked while online. A Consumer Reports survey found that 86 percent of online users were "unwilling to trade their personal data, even anonymously, for the sake of being served ads that online advertisers think are more relevant to them."[198] Additionally, our survey found that the majority of consumers (78 percent) said personalized advertisements provided them with little or no value.[199]

Concurrently with these developments, Julia Angwin revealed and reported on the numerous ways companies track and mine information from consumers through her *What They Know* series. Beginning in 2010, Angwin's work analyzed "what the rise of ubiquitous surveillance means for consumers and society."[200] Some of her first pieces focused on how invisible trackers embedded in websites surveilled users,[201] how companies used detailed information collected by cookies to decide which product they should advertise to a user,[202] and the advent of fingerprinting tracking

---

[193] *Id*.
[194] *Id*.
[195] Kathryn Zickuhr & Aaron Smith, *28% of American Adults Use Mobile and Social Location-Based Services*, PEW RESEARCH CTR. (Sept. 6, 2011), http://www.pewinternet.org/2011/09/06/28-of-american-adults-use-mobile-and-social-location-based-services/.
[196] Kathryn Zickuhr, *Location-Based Services*, PEW RESEARCH CTR. (Sept. 12, 2013), http://www.pewinternet.org/2013/09/12/location-based-services/.
[197] Susannah Fox & Lee Rainie, *The Web at 25 in the U.S.*, PEW RESEARCH CTR. (Feb. 27, 2014), http://www.pewinternet.org/2014/02/27/the-web-at-25-in-the-u-s/.
[198] *Annual State of the Net Survey*, CONSUMER REPORTS (Feb. 14, 2014), on file with author; *see* Jeff Fox, *85% of Online Consumers Oppose Internet Ad Tracking, Consumer Reports Finds*, CONSUMER REPORTS (May 27, 2014), https://www.consumerreports.org/cro/news/2014/05/most-consumers-oppose-internet-ad-tracking/index.htm.
[199] *Id*.
[200] *What They Know* Series, JULIA ANGWIN, http://juliaangwin.com/the-what-they-know-series/ (last visited Aug. 30, 2019).
[201] Julia Angwin & Tom McGinty, *Sites Feed Personal Details to New Tracking Industry*, WALL ST. J. (July 30, 2010), https://www.wsj.com/articles/SB10001424052748703977004575393173432219064.
[202] Emily Steel & Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, WALL ST. J. (Aug. 4, 2010), https://www.wsj.com/articles/SB10001424052748703294904575385532109190198.

methods.[203]The reporting in this series "shocked" the "technology elite, many of whom hadn't realized how sophisticated the tracking industry had become."[204] The series also "unveiled a massive surveillance industry using sophisticated tool to secretly monitor users' behavior – and to use that information to make important decisions about people's lives."[205]Julia Angwin's work sparked a number of changes at the federal level, with the Obama administration reversing the government's hands-off approach to privacy online and calling for a privacy bill or rights and the FTC backing off from their support for self-regulatory measures and calling for a Do Not Track tool on internet browsers.[206] The articles on online tracking also inspired some self-regulatory adjustments by companies.[207]

B. Snowden Disclosures and Legislative Activity Contribute to Growing Concern about Privacy

Following the Snowden disclosures in the summer of 2013, however, the public became much more worried about another privacy threat: their own government. In November of that year, the Pew Research Center reported that: individuals had less faith in the security of their messages;[208] most of those surveyed said that they were "aware of government efforts to monitor communications" and agreed that Americans should be concerned about the government's monitoring of phone calls and internet communications; and the vast majority (91 percent) agreed that consumers had lost control over how personal information is collected and used by companies.[209] Furthermore, in the commercial context, consumers were "are skeptical about some of the benefits of personal data sharing, but were willing to make tradeoffs in certain circumstances when their sharing of information provided access to free services."[210] In addition, this survey found

---

[203] Julia Angwin & Jennifer Valentino-DeVries, *Race is on to 'Fingerprint' Phones, PCs*, WALL ST. J. (Nov. 30, 2010, 12:01 AM), https://www.wsj.com/articles/SB10001424052748704679204575646704100959546.

[204] *What They Know: The Business of Tracking You on the Internet*, WALL ST. J. (July 21, 2010), http://www.cs.cornell.edu/~shmat/courses/cs5436/whattheyknow.pdf.

[205] *Id*.

[206] *Id*.

[207] "Companies also began changing their privacy practices in response to the Journal's reporting. Facebook banned the data collection company RapLeaf Inc. from its website after the Journal revealed that RapLeaf was taking user information and transmitting it to tracking companies. After the Journal's article, Nielsen said it would no longer create fake usernames and passwords to log into private message boards to scrape data.
In December, Microsoft Corp. reversed its decision to remove privacy tools from its Web browser. It will add a powerful privacy feature similar to the one it dropped from an earlier version back into Internet Explorer 9 when it launches in 2011. Mozilla Corp. soon followed by announcing it would add a do-not-track tool to the Firefox Web browser. And Google said it would improve an anti-tracking tool it offered." *Id*.

[208] "81% feel "not very" or "not at all secure" using social media sites when they want to share private information with another trusted person or organization. 68% feel insecure using chat or instant messages to share private information. 58% feel insecure sending private info via text messages. 57% feel insecure sending private information via email. 46% feel "not very" or "not at all secure" calling on their cell phone when they want to share private information. 31% feel "not very" or "not at all secure" using a landline phone when they want to share private information." Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

[209] *Id*.

[210] *Id*.

that consumers wanted to do more to protect their privacy, but face barriers: "Just 24% of adults "agree" or "strongly agree" with the statement: "It is easy for me to be anonymous when I am online.""[211] Correspondingly, fewer than half (44 percent) of those surveyed in another report from the Pew Research Center were "aware that when a company posts a privacy statement, it does not necessarily mean that they are actually keeping the information they collect on users confidential."[212] Although we had snapshots of what the public understood in 2003 and 2005 though Joseph Turow's studies,[213] this nationwide survey demonstrates that consumers still lacked a full understanding of what a privacy policy signals to a user and what terms are contained therein.

In 2015, while the growth of the most dominant social media platform, Facebook, had slowed,[214] consumers began to turn to different social media companies, like Instagram, LinkedIn, and Pinterest.[215] More than half of all online adults (52 percent) were using two or more social media sites, which was a "significant increase" from the 42 percent of internet users in 2013 who reported using more than one platform.[216] Additionally, a Consumer Reports survey found that 29 percent of respondents were told or discovered that their personal information was compromised in the past year.[217] Half of those affected by a data breach reported that they "do not change their online behavior at all as a result of the breach" and 15 percent or fewer of impacted individuals responded to news of a breach by reducing their use of the internet for sending personal information, stopping to enter information on websites, or altering their behavior in another way.[218] Meanwhile, some consumers were using their phones to make their lives easier by depositing checks, making purchases at retail stores, or using phones as a ticket for public transportation.[219]

However, the effects of the Snowden revelations of 2013 continued to permeate society: 34 percent of those individuals who were aware of the government surveillance programs (30 percent of all adults) reported taking at least one step to shield or hide their information from the government.[220] Such steps included changing their privacy settings on social media, using social media less often, avoiding certain apps, uninstalling certain apps, and speaking more in person in order to avoid

---

[211] *Id*.
[212] Aaron Smith, *What Internet Users Know about Technology and the Web*, PEW RESEARCH CTR. (Nov. 25, 2014), http://www.pewinternet.org/2014/11/25/web-iq/.
[213] In both years, the majority of respondents (57 percent in 2003 (*The System is Broken*, *supra* note 63); 59 percent in 2005 (*Open to Exploitation*, *supra* note 97) agreed that the following statement is true: "When a web site has a privacy policy, I know that the site will not share my information with other websites or companies."
[214] "While Facebook remains the most popular social media site, its overall growth has slowed and other sites continue to see increases in usership" Maeve Duggan et al., *Social Media Update 2014*, PEW RESEARCH CTR. (Jan. 9, 2015), http://www.pewinternet.org/2015/01/09/social-media-update-2014/.
[215] *Id*.
[216] *Id*.
[217] *State of the Net*, CONSUMER REPORTS NAT'L RESEARCH CTR. (Feb. 23, 2015), on file with author.
[218] *Id*.
[219] *Id*.
[220] Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RESEARCH CTR. (Mar. 16, 2015), http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/.

online communications.[221] Overall, 25 percent of those who were aware of the surveillance programs (22 percent of all adults) said they had changed their usage patterns on various technological platforms either "a great deal" or "somewhat" in response to the Snowden revelations.[222]

Despite the growing desire to have control over their personal information (93 percent of adults said in 2015 that being in control of who can get information about them is important[223]), consumers still faced barriers in achieving these privacy protections. According to the Pew Research Center, "[o]ne potential reason some have not changed their behaviors is that 54% believe it would be "somewhat" or "very" difficult to find tools and strategies that would help them be more private online and in using their cell phones."[224] Even with this challenge, the Snowden disclosures of 2013 had an impact on consumers and their concerns about their privacy. In addition, the revelations disclosed in Julia Angwin's What They Know series showed consumers that companies were also invading their privacy and inspired a swell of "public concern" that drove the federal government, and the FTC to call for stronger online privacy protections. [225] Another Pew Research Center report from later in 2015 found that 90 percent of all adults thought that controlling what information is collected about them is important and 88 percent said it is important not to be watched or listened to without their permission.[226] This study also provided evidence that consumers' trust eroded in the ability of organizations to protect their private information: only six percent of adults were very confident that government agencies can keep their records private and secure.[227] Furthermore, the survey also found that the majority (59 percent) of adults cleared their cookies or browser history and 57 percent of adults refused to provide information about them that was not relevant to a transaction.[228] Around this time, over a third of smartphone users reported using messaging apps like WhatsApp, iMessage, or Kik and 17 percent used apps that automatically delete messages, like Wickr and Snapchat.[229]

This trend was even more pronounced in the younger generations, as about half (49 percent) of all "smartphone owners age 18 to 29 use messaging apps, while 41% use apps that automatically delete sent messages."[230] The adoption of messaging apps grew concurrently with smartphone

---

[221] *Id*.
[222] *Id*.
[223] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RESEARCH CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ [hereinafter *Americans' Attitudes*].
[224] Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RESEARCH CTR. (Mar. 16, 2015), http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/.
[225] *What They Know*, *supra* note 200.
[226] *Americans' Attitudes*, *supra* note 223.
[227] *Id*.
[228] *Id*.
[229] Maeve Duggan, *Mobile Messaging and Social Media 2015*, PEW RESEARCH CTR. (Aug. 19, 2015), http://www.pewinternet.org/2015/08/19/mobile-messaging-and-social-media-2015/.
[230] *Id*.

adoption, with 68 percent of adults reporting owning a smartphone in 2015.[231] By contrast, in 2011 only 35 percent of adults had a smartphone.[232] Consumers also started to adopt tablets during this time period with 45 percent of adults reporting they owned one.[233] This growth in connected device ownership was accompanied by a growth in technology and privacy literacy, with 60 percent of people reporting that they had chosen not to install an app once they learned how much personal information was required to use it and 43 percent reporting that they have uninstalled apps that asked for too much information.[234] In total, 90 percent of app downloaders stated that the way their personal information will be used by an app is "very" or "somewhat" important to them when they decide whether to download it.[235]

A Consumer Reports survey from 2015 found that 42 percent of shoppers who shopped online in the past 12 months say they are "equally concerned about identity theft or privacy issues" when shopping at a physical store and online.[236] Social media use continued to grow, with 65 percent of adults using these platforms—a seven percent increase from when this issue was first tracked in 2005.[237]

Responding to consumer concerns, the US Congress introduced a flurry of privacy-protective measures: Senators John McCain and John Kerry introduced their Commercial Privacy Bill of Rights;[238] Representative Bobby Rush introduced The Data Accountability and Trust Act;[239] Representative Bill Boucher introduced his Best Practices Act.[240] In addition, President Barack Obama introduced his Consumer Privacy Bill of Rights framework.[241] This was perhaps one of the most active periods for privacy legislation at the federal level until 2017-19.

---

[231] Monica Anderson, *Technology Device Ownership: 2015*, PEW RESEARCH CTR. (Oct. 29, 2015), http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/.
[232] *Id*.
[233] *Id*.
[234] Michelle Atkinson, *Apps Permissions in the Google Play Store*, PEW RESEARCH CTR. (Nov. 10, 2015), http://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store/.
[235] *Id*.
[236] *Online vs. Walk-in Retailer Shopping Behavior Study*, CONSUMER REPORTS NAT'L RESEARCH CTR. (Oct. 1, 2015), on file with author.
[237] Andrew Perrin, *Social Media Usage: 2005-2015*, PEW RESEARCH CTR. (Oct. 8, 2015), http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/.
[238] *Kerry, McCain Circulate "Commercial Privacy Bill of Rights,"* INSIDE PRIVACY (Mar. 25, 2011), https://www.insideprivacy.com/united-states/kerry-mccain-circulate-commercial-privacy-bill-of-rights/.
[239] David Fagan, *Rep. Rush Reintroduces Data Breach Legislation*, INSIDE PRIVACY (May 9, 2011), https://www.insideprivacy.com/data-security/rep-rush-reintroduces-data-breach-legislation/.
[240] *Summarizing the Boucher Privacy Bill*, ARENT FOX LLP (Oct. 29, 2010), https://www.lexology.com/library/detail.aspx?g=5a9eaa35-d288-40ad-8ede-aadcac23ea15.
[241] Mickey Meece, *President Obama's Consumer Privacy Bill of Rights*, FORBES (Feb. 23, 2012, 5:08 PM), https://www.forbes.com/sites/mickeymeece/2012/02/23/president-obamas-consumer-privacy-bill-of-rights/#72ef6688789b.

C. Concerned Users Period

During this period, consumers became more aware of tracking technologies due to investigative reporting, the Snowden revelations, and federal engagement on the issue. Although consumers remained relatively unaware of how tracking occurs, they developed more defensive tactics. Concerns over access and collection of personal information hits an all-time high,[242] which helped push lawmakers to introduce legislation aimed at alleviating these concerns. Although consumers did not get the protections they wanted, they did begin to reevaluate their relationship with technology companies and the internet with a critical eye.

VI. Critical Users, 2016-2019

In this final period, which encompasses the present day, consumers have become more skeptical of the technologies they once embraced. This wariness stems from repeated reports of data breaches, privacy overreaches, and grand scale manipulation of consumers. Importantly, the Cambridge-Analytica scandal is also revealed during this period, pushing the growing tech-lash into center stage as Congress, the media, and the public ponder their relationships with technology companies. While consumers are more aware than ever that they are tracked, they also lack sufficient tools to take control of such data collection. In addition, without an easy way of understanding how tracking translates into targeted advertisements, consumers are driven to wonder whether or not their phone is listening to them. This tech-lash also features decreased use of the still-dominant social media platform, Facebook. Although consumer understanding of tracking continues to lag, consumer support for laws that stem rampant data collection is high.

A. Consumer Awareness of Tracking Leads to Distrust

In 2016, Consumer Reports completed one of its first surveys on tracking technologies, finding that more than half of adults have experienced some common forms of digital tracking and profiling in the past three years. Approximately half of all Americans have experienced common forms of digital tracking: 53 percent of adults were served with an ad for remedies after searching for an illness online; 53 percent reported that a website demanded their email address before they could read an article; and 49 percent reported that an app had asked for access to their phone's location data.[243] More than half of adults found these common forms of tracking to be intrusive or very intrusive, regardless of whether the individual had personal experience with these them.[244]

In particular, our survey found that three out of five Americans find it very intrusive when: a website demands their email address before they can read an article (58%); a game app wants access to their phone's GPS data (56%); and their photos are easily be tagged or grouped in a

[242] *Americans' Attitudes*, *supra* note 223.
[243] Privacy *Survey Research Report*, CONSUMER REPORTS NAT'L RESEARCH CTR. (Aug. 23, 2016), on file with author.
[244] "For each common form of digital tracking and profiling, at least one-third of adult Americans (ranging from 33% to 58%) find it very intrusive, and nearly a quarter (ranging from 23% to 36%) finds it somewhat intrusive, regardless of whether they have experienced it in the past three years or not." *Id.*

friend's profile on social media through facial recognition without their approval (55%).[245] In addition, 73 percent of Americans felt that it would be very intrusive if a firm collected their browsing and shopping history and sold it to advertisers.[246] Consumers said they found targeted ads in the form of friends' "likes" less intrusive than other practices we asked about.[247] Our survey found that consumers reported using a variety of privacy-protective tactics: 86 percent set a secure password on their home WiFi network; 75 percent required a password or another verification method to unlock their smartphone; and 62 percent reported using two-factor authentication on personal accounts.[248] Less commonly-endorsed privacy-protective methods included backing up their computer regularly (45%); regularly using a virtual private network (VPN) to get on public WiFi (38%); and covering a laptop camera when it is not in use (28%).[249]

2016 also continued the trend of social media dominance, with 79 percent of all online Americans (and 68 percent of all US adults) using Facebook.[250] Aside from Facebook, other social media platforms were also widely used, with 28 percent of all US adults using Instagram, 26 percent using Pinterest, 25 percent using LinkedIn, and 21 percent using Twitter.[251] Adoption of messaging apps that automatically delete sent messages increased, with 24 percent using apps like Snapchat or Wickr—a 7-point increase from 2015.[252] Similar to 2015, this trend was more pronounced among younger adults, 56 percent of whom used auto-delete apps in 2016.[253] The same year, Americans started to use anonymous chat apps, with five percent of all adults reporting that they have used apps like YikYak or Whisper.[254]

In 2017, a Pew Research Center poll found that the majority of Americans (64 percent) have been affected by a major data breach and many lacked faith in key institutions, especially the federal government and social media sites, to protect their personal information.[255] Accordingly, about half of the population (46 percent) said they feel like their personal information is less secure than it was five years ago.[256] A Consumer Reports survey supported these findings, reporting that 66 percent of Americans do not trust the government to protect consumers' interests and that many Americans (65 percent) are either slightly or not at all confident that their personal data is private

---

[245] *Id*.
[246] *Id*.
[247] Roughly 30% of Facebook users find it not at all intrusive when their friends' "likes" show up as ads in their news feed, and only a third of users (33%, the lowest rate on our list) find the practice very intrusive. *Id*.
[248] *Id*.
[249] *Id*.
[250] Shannon Greenwood et al., *Social Media Update 2016*, PEW RESEARCH CTR. (Nov. 11, 2016), http://www.pewinternet.org/2016/11/11/social-media-update-2016/.
[251] *Id*.
[252] *Id*.
[253] *Id*.
[254] *Id*.
[255] Aaron Smith, *Americans and Cybersecurity,* PEW RESEARCH CTR. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.
[256] *Id*.

and not distributed without their knowledge.[257]

As with previous years, the growth of tech adoption outpaced consumers' understanding of and ability to identify common cybersecurity threats and tracking methods. With regard to cybersecurity, 54 percent of internet users were able to identify examples of phishing attacks and 48 percent could define the term "ransomware." 46 percent knew that all email is not encrypted by default, and 45 percent knew that all WiFi traffic is not encrypted by default.[258] With regard to tracking technologies, 52 percent knew that turning off the GPS function on a phone does not prevent all tracking of that device and 39 percent of internet users were aware that ISPs are able to see the sites their customers visit even when the "private browsing" mode is turned on.[259]

In April 2017, repealed the Federal Communications Commission's broadband privacy rules. Following this reversal, a Consumer Reports survey found that 92 percent of Americans felt that ISPs should be required to get their permission before selling or sharing their data with other companies.[260] The same proportion of Americans, 92 percent, said that internet companies and websites should be required to provide them with a complete list of data that they have collected about them and almost two-thirds (65%) of consumers either strongly (47 percent) or somewhat (18 percent) oppose dynamic pricing—the practice of automatically adjusting prices for individuals based on their behavior.[261] Between February and May 2017, consumers became less confident that their personal data is private and not distributed without their knowledge.[262] Another Consumer Reports survey in May 2017 found that 60 percent of Americans thought ISPs should not be allowed to sell or share their data and 80 percent of Americans thought that internet companies ought to get their permission to share their data.[263] A third 2017 Consumer Reports survey found that 66 percent of Americans have a social media account.[264] Of those that have an account, 33 percent are highly concerned about how the social media site uses the data they collect about them and 53 percent have changed their behavior on social media platforms due to privacy concerns.[265] Additionally, 41 percent of social media users have deactivated or deleted an account due to concerns such as social media taking too much or their time or worries over their privacy.[266]

Most consumers (88 percent) also want online companies to get their permission before selling or

---

[257] *Consumer Voices Survey I*, CONSUMER REPORTS NAT'L RESEARCH CTR. (Feb. 16, 2017), on file with author.
[258] Aaron Smith, *What the Public Knows About Cybersecurity*, PEW RESEARCH CTR. (Mar. 22, 2017), http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/.
[259] Aaron Smith, *What the Public Knows About Cybersecurity*, PEW RESEARCH CTR. (Mar. 22, 2017), http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/.
[260] *Consumer Voices II Survey*, CONSUMER REPORTS NAT'L RESEARCH CTR. (May 11, 2017), on file with author.
[261] *Id*.
[262] The February *Consumer Voices Survey* found that 65 percent of the population were not confident that their personal information is private, compared to 70 percent in the May Survey. *Id*.
[263] *Privacy/Net Neutrality Survey*, CONSUMER REPORTS NAT'L RESEARCH CTR. (May 15, 2017), on file with author.
[264] *Consumer Voices III Survey*, CONSUMER REPORTS NAT'L RESEARCH CTR. (Dec. 2017), on file with author.
[265] *Id*.
[266] *Id*.

sharing their personal information.[267] This attitude carries over to products that are not traditionally connected to the internet, such as cars: 82 percent say automakers should be required to get their permission before collecting data on their driving behavior and 55 percent think that automakers should get their permission before sharing information about customer driving behavior with other companies.[268]

In September 2017, the credit reporting agency Equifax announced a historic data breach[269] that was revealed to have affected at least 148 million[270] Americans. This breach, which affected half of all US adults, disclosed the names, Social Security numbers, birth dates, addresses, credit card numbers, and other personally identifiable information about individuals.[271] This data breach revealed to many individuals that while they lack a relationship with credit reporting agencies, these companies still collect a lot of information about them, and sometimes this data is not properly secured.[272] This breach, which revealed how little control consumers have over data collected about them, resulted in some nationwide changes: (1) in March 2018, Alabama and South Dakota passed data breach notification laws, the last two states to do so;[273] (2) other states like Arizona, Colorado, and Oregon amended to provide more timely notice for consumers and expand the definition of personal information;[274] and (3) in May 2018, Congress passed a law making credit freezes free.[275] In order to help consumers recover, the Federal Trade Commission reached a settlement with Equifax that included a requirement for the company to pay at least $575 million (but possibly up to $700 million), a portion of which would be given directly to individuals.[276]

In 2018, Facebook and YouTube were the dominant social media platforms, but the portion of US

---

[267] *Id*.
[268] *Id*.
[269] Kaya Yurieff, *Equifax Data Breach: What You Need to Know*, CNN (Sept. 10, 2017, 1:11 PM), https://money.cnn.com/2017/09/08/technology/equifax-hack-qa/index.html.
[270] *Equifax Data Breach Affected 2.4 Million More Consumers*, CONSUMER REPORTS (Mar. 1, 2018), https://www.consumerreports.org/credit-bureaus/equifax-data-breach-was-bigger-than-previously-reported/.
[271] Kaya Yurieff, *supra* note 269.
[272] Cybele Weisser, *Equifax Data Breach Puts Spotlight on How Credit Agencies Work*, CONSUMER REPORTS (Oct. 3, 2017), https://www.consumerreports.org/credit-bureaus/equifax-data-breach-puts-spotlight-on-how-credit-agencies-work/.
[273] Adam Janofsky, *One Year After Equifax Breach: Criminal Charges, New State Laws and Lost Chances*, WALL ST. J. (Sept. 7, 2018, 11:34 AM), https://www.wsj.com/articles/one-year-after-equifax-breach-criminal-charges-new-state-laws-and-lost-chances-1536334479; *see*, Heather Morton, *Consumer Report Security Freeze State Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (June 26, 2018), http://www.ncsl.org/research/financial-services-and-commerce/consumer-report-security-freeze-state-statutes.aspx; and *2016 Security Breach Legislation*, NAT'L CONFERENCE OF STATE LEGISLATURES (Nov. 29, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/2016-security-breach-legislation.aspx.
[274] Janofsky, *supra* note 273; *Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Aug. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx#2.
[275] Octavio Blanco, *Good News for Consumers: Free Credit Freezes*, CONSUMER REPORTS (May 24, 2018), https://www.consumerreports.org/credit-protection-monitoring/credit-freezes-are-now-free/.
[276] Alfred Ng & Sean Keane, *Equifax to Pay at least $575 Million as Part of FTC Settlement*, CNet (July 22, 2019, 11:44 AM), https://www.cnet.com/news/equifax-to-pay-at-least-575m-as-part-of-ftc-settlement/.

adults who used Instagram, Snapchat, and Twitter continued to grow.[277] However, a larger number of Americans were beginning to question the effect the internet has had on the world, with a declining number of adults believing that the internet has been good for society.[278] And although the majority of adults reported using social media (73 percent of adults report using YouTube and 69 percent use Facebook[279]), about half of Facebook users did not understand how Facebook News Feed are ordered.[280] This fact stands in stark contrast to the reality that the News Feed was (and still is) one of the primary points of interaction for Facebook users. Similar to online tracking, the method of ordering News Feed items is proprietary and therefore obscured from the user.

B. Missteps by Technology Companies Sparks Backlash and a Negative Opinion of the Internet

On March 17, 2018, the New York Times reported the sharing arrangement between Facebook and a voter-profiling firm, Cambridge Analytica, which enabled the firm to harvest private information from Facebook profiles of more than 50 million users without their permission.[281] This data sharing arrangement "allowed [Cambridge Analytica] to exploit the private social media activity of a huge swath of the American electorate, developing techniques that underpinned its work on President's Trump campaign in 2016."[282]

During this time period, consumers started to reevaluate their use of Facebook, with 54 percent of users reporting that they have made changes to their privacy preferences, 42 percent reporting that they have taken breaks from the platform for several weeks or longer, and a quarter reporting that they deleted the Facebook app from their mobile devices.[283] Overall, 74 percent of users had taken at least one of these three actions.[284]

---

[277] Aaron Smith & Monica Anderson, *Social Media Use in 2018*, PEW RESEARCH CTR. (Mar. 1, 2018), http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/.

[278] "A sizable majority of online adults (70%) continue to believe the internet has been a good thing for society. Yet the share of online adults saying this has declined by a modest but still significant 6 percentage points since early 2014, when the Center first asked the question. This is balanced by a corresponding increase (from 8% to 14%) in the share of online adults who say the internet's societal impact is a mix of good and bad. Meanwhile, the share saying the internet has been a mostly bad thing for society is largely unchanged over that time: 15% said this in 2014, and 14% say so today." *Id*.

[279] Andrew Perrin & Monica Anderson, *Share of U.S. Adults Using Social Media, including Facebook, is Mostly Unchanged Since 2018*, PEW RESEARCH CTR. (Apr. 10, 2019), https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/.

[280] Aaron Smith, *Many Facebook Users Don't Understand How the Site's News Feed Works*, PEW RESEARCH CTR. (Sept. 5, 2018), https://www.pewresearch.org/fact-tank/2018/09/05/many-facebook-users-dont-understand-how-the-sites-news-feed-works/.

[281] Matthew Rosenberg, Nicolas Confessore, & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html?module=inline.

[282] *Id*.

[283] Andrew Perrin, *Americans are Changing Their Relationship with Facebook*, PEW RESEARCH CTR. (Sept. 5, 2018), http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/.

[284] *Id*.

Unfortunately, 2018 held another privacy breach. In November 2018 Marriott announced that the company exposed the data of 383 million guests,[285] including credit card information, passport numbers, email addresses, phone numbers, dates of birth, and addresses. [286] Although it is still unclear what legal implications this breach will have for the company, the breach and the subsequent blowback have yet to affect Marriott's business.[287]

By 2019, 81 percent of Americans reported going online on a daily basis, while 28 percent reported being online almost constantly.[288] The users that were online the most reported connecting through mobile devices such as a smartphone or a tablet.[289]

In 2019, the use of smart speakers assisted by digital voice assistants is on the rise, with approximately 21 percent of the adult population reporting that they own a smart speaker.[290] However, many have trouble trusting these products, with 58 percent of owners worrying that hackers could use the speaker to access their home or personal information, 49 percent worrying about the government using their speaker to spy on them, and 51 percent worrying that a smart speaker is always listening.[291] These concerns are also reflected by non-owners in similar proportions: 63 percent worry about hackers, 55 percent are concerned about speakers always listening, and 40 percent fear that the government could listen in.[292] Despite their privacy and security concerns, 69 percent of smart speaker owners report that they interact with their speaker daily.[293] Finally, only eight percent of adults are "very confident they know what data are being collected when they use connected devices," while only 25 percent are somewhat confident and 58 percent are not confident at all.[294]

---

[285] Chris Isidore, *Marriott Hasn't Paid the Price for its Massive Data Breach*, CNN (May 10, 2019, 8:05 AM), https://www.cnn.com/2019/05/10/business/marriott-hack-cost/index.html.

[286] Nicole Perlroth, Amie Tsang, & Adam Satariano, *Marriott Hacking Exposes Data of Up to 500 Million Guests*, N.Y. TIMES (Nov. 30, 2018), https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html.

[287] "Marriott's massive data hack was certainly bad news for its reputation, as well as its customers. But it barely made a dent in its bottom line. Marriott's giant hack has cost it $72 million so far, with $44 million of those costs coming in the first quarter, the company disclosed Friday. But it has collected $71 million in insurance reimbursements for the incident. $46 million of those payments came in the first quarter, meaning that it ended up with a slight gain in its first quarter financial results, after a slightly larger loss at the end of last year." Chris Isidore, *Marriott Hasn't Paid the Price for its Massive Data Breach*, CNN (May 10, 2019, 8:05 AM), https://www.cnn.com/2019/05/10/business/marriott-hack-cost/index.html.

[288] Andrew Perrin & Madhu Kumar, *About Three-in-Ten U.S. Adults Say They Are 'Almost Constantly' Online*, PEW RESEARCH CTR. (July 25, 2019), https://www.pewresearch.org/fact-tank/2019/07/25/americans-going-online-almost-constantly/.

[289] *Id.*

[290] Chris Eggertsen, *Smart Speaker Ownership Continues to Rise Among Americas, Even as Privacy Concerns Grow*, BILLBOARD (June 26, 2019), https://www.billboard.com/articles/business/8517828/smart-speaker-ownership-study-rising-privacy-concerns-npr-edison.

[291] *Id.*

[292] *Id.*

[293] *Id.*

[294] Darrell M. West, *Brookings Survey Finds Three-Quarters of Online Users Rarely Read Business Terms of Service*, BROOKINGS (May 21, 2019), https://www.brookings.edu/blog/techtank/2019/05/21/brookings-survey-finds-three-quarters-of-online-users-rarely-read-business-terms-of-service/.

Although 2018 featured many news stories highlighting the ill effects of social media sites, the number of US adults on social media remained unchanged from 2018 to 2019.[295] YouTube (73 percent of adults are users) and Facebook (69 percent) remained the most popular sites, followed by Instagram (37 percent), Pinterest (28 percent) and LinkedIn (27 percent).[296] The adoption of these social media sites has plateaued, since 2016. Only Instagram's share rose during these three years,[297] and daily use of Facebook, Instagram, and Snapchat stayed relatively constant, despite many high-profile controversies over the past year—particularly those involving Facebook and their subsidiary Instagram.[298] It appears that these controversies failed to make consumers fully aware of Facebook's inference-based audience system, since 74 percent of users reported that they were not aware of the ad preferences section on the site that informs users how the company classifies them.[299] Additionally, 51 percent were not comfortable with Facebook compiling this information.[300]

Considering the frequency that people use these platforms, it is noteworthy that consumers are not making use of the Social Login systems that companies like Facebook and Google offer. According to a Consumer Reports' survey in June of 2019, about half of Americans that have accounts with Facebook or Google say that, if given the option, they never use Social Login supported by Facebook (51 percent) or Google (49 percent) to sign into other accounts.[301]

Over the past four years, consumers' negative opinions about technology companies have nearly doubled. Though the majority of adults in 2015 (71 percent) thought that tech companies have a positive effect on the way things are going in the US, this rate dropped to 50 percent by 2019.[302]

While the internet has almost always been modeled on notice and consent—the practice of notifying users of the terms of use in a particular situation and then asking for their consent through an action such as clicking "I Agree"—findings from a 2019 Brookings survey suggest that this system is suboptimal: 32 percent of US adults never read the privacy or terms of use policies before consenting.[303] In this same survey, 80 percent of adults stated that online privacy is important and

---

[295] Andrew Perrin & Monica Anderson, *Share of U.S. Adults Using Social Media, including Facebook, is Mostly Unchanged Since 2018*, PEW RESEARCH CTR. (Apr. 10, 2019), https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/.
[296] *Id.*
[297] *Id.*
[298] *Id.*
[299] Paul Hitlin & Lee Rainie, *Facebook Algorithms and Personal Data*, PEW RESEARCH CTR. (Jan. 16, 2019), https://www.pewinternet.org/2019/01/16/facebook-algorithms-and-personal-data/.
[300] *Id.*
[301] *Data Privacy Survey*, CONSUMER REPORTS (June 4, 2019), on file with author.
[302] Carroll Doherty & Jocelyn Kiley, *Americans Have Become Much Less Positive About Tech Companies' Impact on the U.S.*, PEW RESEARCH CTR. (July 29, 2019), https://www.pewresearch.org/fact-tank/2019/07/29/americans-have-become-much-less-positive-about-tech-companies-impact-on-the-u-s/.
[303] Darrell M. West, *supra* note 294.

73 percent thought that companies should not be allowed to sell consumer data to firms that are not bound by the privacy rules of the original company.[304]

A survey from Consumer Reports in June 2019 found that 43 percent of Americans with smartphones believe that their phone is recording what they say even when they do not ask it to, while nearly half believe it does not.[305] The survey also demonstrated that consumers worry about sharing location data. Over half of Americans who own smartphones (54 percent) said they allow apps to track their location only when it is necessary for the functioning of the app, and more than a quarter (28 percent) said they do not allow any apps to track them via this feature.[306]

C. Survey of Current Consumer Attitudes

In 2019, Consumer Reports conducted another survey on the public's perspectives on privacy, technology, and tracking. This survey found that many Americans (61%) want to be asked for permission before mobile apps are allowed to collect personal data when you aren't using the app, such as location, contacts, and other apps you use. And, individuals on average think sharing their personal information is more risky than beneficial, but it varies based on the type of data. The survey showed that the most commonly used privacy practices are: using a strong password on a home WiFi network (74 percent report doing this), not using apps that collect too much information (71 percent), and requiring a password or other method to unlock their smartphone (69 percent).[307] Several important privacy practices were used less frequently, such as a password manager (36 percent report doing this) and a virtual private network (VPN) (34 percent report doing this).[308] The majority of consumers (67 percent) said they think that mobile apps should be able to collect information about them when they are not using the app; but, of those who think apps should be able to do so, 90 percent think that the app should get the consumer's permission first.[309]

The results on a per-product basis reveal a deeper sophistication of risk evaluation: at least 60 percent of consumers felt that the risks of sharing their email addresses, access to their camera and photos, or location data outweigh the benefits.[310] On the other hand, more believe the benefits of sharing Smart TV watch history outweigh the risks (41%) than those who think risks outweigh benefits (27%). However, the people who take the most care in protecting their privacy online—though methods such as using strong passwords for their WiFi networks, setting up permissions on their smartphone apps, and even less common activities such as using a VPN or the "incognito" mode on their browser—are not necessarily those who think the risks outweigh the benefits when

[304] *Id*.
[305] *Data Privacy Survey*, CONSUMER REPORTS (June 4, 2019), on file with author.
[306] *Id*.
[307] *Privacy--Sloan Grant Survey: a 2019 Nationally Representative Phone Survey*, CONSUMER REPORTS (July 29, 2019), on file with author.
[308] *Id*.
[309] *Id*.
[310] *Id*.

sharing information online.[311] This perhaps is due to a misplaced feeling that their preventative actions help mitigate their vulnerability to these risks.

The survey also demonstrated that younger Americans and those who use smartphones do a lot to protect their privacy online. For example, those aged 18 to 34 do an average of 5.8 of the protective actions we asked about compared to 4.3 by those aged 55 and up. They have come to rely on technology in their daily lives, and are comfortable (or complacent) with the risks. They are even in favor of apps collecting their personal information (72% of those aged 18 to 34 say mobile apps should be allowed to collect this data when you aren't using the app), but most want the apps to ask permission first.[312] These types of users want to be in control of their online presence so they can take advantage of the benefits to be gained.[313] It remains to be determined whether this stance is due to a truly more nuanced grasp of technology, or an unsophisticated and inexperienced view of the dynamics of the technology and advertising industries.

On the other hand, some individuals do very little to protect their privacy online. The survey implied that these people are more likely to want formal regulation of mobile app data collection. For instance, many of these respondents (47%) think mobile apps should not be allowed to collect personal information when you are not using the app, compared to those who use more methods to protect their privacy who think it should not be allowed (29%).[314]

D. Critical Users Period

Consumer angst and anger about their lack of control over their privacy and digital security peak during this period. Individuals know more about how pervasive tracking is, even if they are unable to effectively stop or control such surveillance. Although Congress responds to historic data breaches by providing free credit freezes for all, most of the public's concerns about privacy and their digital security remain unresolved. In response, individuals increasingly turn to third-party services like ad blockers to partially protect their privacy.

VI. Conclusion

In the current environment, users are more aware of the existence of tracking than they are aware of how this tracking is done. People have few tools to control tracking online and relatively similar rights online as they had in the late 1990s. Unfortunately, consumers have believed for decades that they have more rights and protection online than they actually have. This lack of awareness has led to frustrating and confusing outcomes. For instance, a survey in 2018 found that a quarter of Americans use the "Do Not Track" (DNT) setting to "protect their privacy" despite the fact it

[311] *Id.*
[312] *Id.*
[313] *Id.*
[314] *Id.*

is widely ignored,[315] and considered defunct by many of its key supporters (Apple removed the feature from Safari citing the possibility of DNT being used for fingerprinting).[316]

Many of the techniques recommended to users to protect their privacy by consumer education organizations like Consumer Reports have remained the same since the late 90s and early aughts: giving false information, change your default settings, block third party cookies, and clear cookies often. Though the community has added tools like VPNs to this list, the cognitive load and degree of effort for consumers to protect their privacy continues to increase. Even the tools and techniques recommended will fail to protect consumer privacy entirely.

Over time, there has been greater awareness of tracking as a result of consumers' increased experience on the web, personal experiences with corporate tracking and tailored ads, news moments like Cambridge Analytica, and consumer education efforts. Yet, awareness that you are being tracked has not on its own translated into better consumer control over their data. In the current environment, consumers know they are being tracked, but they are largely unaware of how this tracking is done, unable to control such data collection, and may even be resigned or complacent to it.

In 2019, there remains a significant gap between consumer understanding of tracking technology and their means to control it. Yet the capabilities of technology and advertising companies to Track consumers and create detailed pictures of their behavior is still accelerating.

For the majority of the web's existence, the onus to protect and secure private data has largely fallen directly on the consumer, whose data is being collected and used to undermine their autonomy by predicting their behavior, providing them with biased service and pricing, and exploiting their trust to achieve political gains. It is useful to study what consumers know and understand about tracking and tracking technology to reflect on how rampant data collection has led to the current system. However, the initial findings of this research show that awareness of tracking and the techniques by which one is tracked do not on their own empower consumers to better control their data.

---

[315] Philippe Le Hegaret (@plehegar), GITHUB (Jan. 18, 2019), https://github.com/w3c/dnt/commit/5d85d6c3d116b5eb29fddc69352a77d87dfd2310.

[316] *Safari 12.1 Release Notes*, APPLE, https://developer.apple.com/documentation/safari_release_notes/safari_12_1_release_notes (last visited Aug. 26, 2018).