LIBERTY UNIVERSITY

Liberty University Law Review

Volume 18
Issue 3 *Spring 2024*

Article 5

April 2024

# To Track or Not to Track: The Privacy Dilemma and the Veil of Consumer Choice

Amber L. Solberg
*Liberty University*

AMBER L. SOLBERG

# To Track or Not to Track: The Privacy Dilemma and the Veil of Consumer Choice

**ABSTRACT**

Technology has contributed to rapid yet fundamental changes in the way society functions—but the information revolution is just getting started. Ubiquitous, distributed, and interconnected computational power and massive data storage, coupled with human ingenuity and entrepreneurship, have led to profound impacts on society, changing the way we live, work, and interact with each other. However, these rapid advances have given rise to new legal challenges and upended the balance between the interests of corporations and consumers regarding privacy, ownership of personal data, and fundamental concepts of intellectual property. As multi-billion-dollar corporations thrive by monetizing personal data, existing legal frameworks struggle to address privacy violations in this evolving landscape. This Comment sheds light on contemporary data privacy challenges by juxtaposing how the law has previously developed in response to new technology with the current gaps in federal legislation and argues that outdated statutes offer no recourse for contemporary Internet privacy violations that were not anticipated. This Comment underscores the growing public interest in robust privacy protection, evidenced by the emergence of voluntary market-level regulations. Despite making progress, these market-level solutions fall short for the reasons explored in this Comment, leaving consumer privacy vulnerable without a clear avenue for protection or legal redress.

To address this problem, this Comment advocates for the implementation of a private right of action to effectuate meaningful accountability against data abusers and reshape the data privacy landscape. Specifically, this Comment aims to resolve the "privacy dilemma" by leveraging a common

law privacy tort and proposes a framework that centers on consumer consent with context-relevant factors to analyze. Specifically, it argues for the expansion of intrusion upon seclusion in Internet privacy disputes with the goal of establishing clear boundaries for the tort's scope and application to cases where corporations have exceeded or improperly obtained user consent. Courts should adopt this proposed framework to address the modern Internet privacy concerns in light of advancing technology. Without clearly delineated responsibilities and liabilities that consider the context and scope of user consent, corporations will continue to weaponize user consent and sidestep privacy-by-design defaults.

## AUTHOR

*Business Manager*, LIBERTY UNIVERSITY LAW REVIEW, Volume 18. J.D. Candidate, Liberty University School of Law (2024); A.L.M. in Extension Studies, Concentration: Data Science, Harvard University (2021); J.M. American Legal Studies, Liberty University (2020); B.S. Financial Mathematics and Statistics, University of California, Santa Barbara (2018).

The Author accumulated a diverse educational background including advanced mathematics, statistics, and data science prior to beginning her journey into law. As she studied the current and future impacts of data science and artificial intelligence, the Author became intrigued first with the societal implications of these technological advances, and then the associated legal and legislative dimensions. The Author would like to thank her parents for always encouraging her to pursue her passions and for always being a source of wisdom as she navigates through this crazy thing called life. The Author would also like to thank Professor Lucas for some of the insights that have led to the development of this Comment.

COMMENT

# TO TRACK OR NOT TO TRACK: THE PRIVACY DILEMMA AND THE VEIL OF CONSUMER CHOICE

*Amber L. Solberg*[†]

*"Nothing vast enters the life of mortals without a curse."*

- Sophocles[1]

ABSTRACT

*Technology has contributed to rapid yet fundamental changes in the way society functions—but the information revolution is just getting started. Ubiquitous, distributed, and interconnected computational power and massive data storage, coupled with human ingenuity and entrepreneurship, have led to profound impacts on society, changing the way we live, work, and interact with each other. However, these rapid advances have given rise to new legal challenges and upended the balance between the interests of corporations and consumers regarding privacy, ownership of personal data, and fundamental concepts of intellectual property. As multi-billion-dollar corporations thrive by monetizing personal data, existing legal frameworks struggle to address privacy violations in this evolving landscape. This Comment sheds light on contemporary data privacy challenges by juxtaposing how the law has*

---

[†] *Business Manager*, LIBERTY UNIVERSITY LAW REVIEW, Volume 18. J.D. Candidate, Liberty University School of Law (2024); A.L.M. in Extension Studies, Concentration: Data Science, Harvard University (2021); J.M. American Legal Studies, Liberty University (2020); B.S. Financial Mathematics and Statistics, University of California, Santa Barbara (2018).

The Author accumulated a diverse educational background including advanced mathematics, statistics, and data science prior to beginning her journey into law. As she studied the current and future impacts of data science and artificial intelligence, the Author became intrigued first with the societal implications of these technological advances, and then the associated legal and legislative dimensions. The Author would like to thank her parents for always encouraging her to pursue her passions and for always being a source of wisdom as she navigates through this crazy thing called life. The Author would also like to thank Professor Lucas for some of the insights that have led to the development of this Comment.

[1] *See, e.g.*, THE SOCIAL DILEMMA (Netflix 2020).

*previously developed in response to new technology with the current gaps in federal legislation and argues that outdated statutes offer no recourse for contemporary Internet privacy violations that were not anticipated. This Comment underscores the growing public interest in robust privacy protection, evidenced by the emergence of voluntary market-level regulations. Despite making progress, these market-level solutions fall short for the reasons explored in this Comment, leaving consumer privacy vulnerable without a clear avenue for protection or legal redress.*

*To address this problem, this Comment advocates for the implementation of a private right of action to effectuate meaningful accountability against data abusers and reshape the data privacy landscape. Specifically, this Comment aims to resolve the "privacy dilemma" by leveraging a common law privacy tort and proposes a framework that centers on consumer consent with context-relevant factors to analyze. Specifically, it argues for the expansion of intrusion upon seclusion in Internet privacy disputes with the goal of establishing clear boundaries for the tort's scope and application to cases where corporations have exceeded or improperly obtained user consent. Courts should adopt this proposed framework to address the modern Internet privacy concerns in light of advancing technology. Without clearly delineated responsibilities and liabilities that consider the context and scope of user consent, corporations will continue to weaponize user consent and sidestep privacy-by-design defaults.*

CONTENT

## I. INTRODUCTION

Privacy is consistently viewed as a fundamental human right[2] and has been regarded as vital to sustaining individual freedoms and upholding social systems.[3] It has been defined as "the right to be left alone,"[4] the state of "control,"[5] and a person's right to control "when, how, and to what extent information about them is communicated with others."[6] Despite this definition, the "overall understanding of what is private" and what constitutes an invasion of privacy has evolved over time.[7] Privacy invasions are no longer predominantly discrete or isolated incidents.[8] Encroachments are increasingly concealed, undetected, and continuous.[9] The right to privacy is "[n]o longer delineated by tangible physical barriers," but rather privacy includes one's "information, thoughts, and movements."[10] By virtue of the expansion of the Internet and new technologies for gathering information,

---

[2] While not explicitly guaranteeing the right to privacy, the Supreme Court has found that the U.S. Constitution does provide for a right to privacy in its First, Third, Fourth, and Fifth Amendments. *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (arguing that a right to privacy can be inferred legitimately from the language of at least four amendments) ("[S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy." (citation omitted) (citing Poe v. Ullman, 367 U.S. 497, 516–22 (1961) (Douglas, J., dissenting))); *see also* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958) (identifying the freedom to associate as a peripheral First Amendment right, thereby protecting privacy in one's associations); U.S. CONST. amend. III (proscribing the quartering soldiers "in any house" in time of peace without the consent of the owner); Boyd v. United States, 116 U.S. 616, 630 (1886) (interpreting the Fourth and Fifth Amendments to offer protection against all government invasions "of the sanctity of a man's home and the privacies of life").

[3] Debbie V.S. Kasper, *Privacy as a Social Good*, 28 SOC. THOUGHT & RSCH. 165, 167–68 (2007).

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

[5] Irwin Altman, *Privacy: A Conceptual Analysis*, 8 ENV'T & BEHAV. 7, 13–14 (1976).

[6] Jennifer Jiyoung Suh & Miriam J. Metzger, *Privacy Beyond the Individual Level*, *in* MODERN SOCIO-TECHNICAL PERSPECTIVES ON PRIVACY 91, 91 (Knijnenburg et al. eds., 2022).

[7] Kasper, *supra* note 3, at 170.

[8] *Id.*

[9] *Id.*

[10] *Id.*

the societal and individual need for privacy has been frustrated by the competing market for personal data.[11] Although the loss of information privacy is hard to quantify, the sentiment is tangible, and efforts to rectify information privacy intrusions on a mass scale face an uphill battle. Technological advancements in data gathering, mining, and manipulation have outpaced current legal frameworks. To understand how this has happened, one must first trace back to the root of the problem—the invention of the Internet.

The Internet began as an arcane tool for collaboration among scientists aiming to openly share information.[12] Nonetheless, it proved useful for many other purposes because it connected people and information world-wide. Technology companies arose to capitalize on this massively connected market, ushering in a digital economy of unprecedented reach and scope. In the early high-growth days of the Internet, technology startups focused on reaching as many users as possible—capturing users was considered far more important than short-term revenue considerations.[13] The titans of the digital economy came into existence by creating essentially free products used by very large numbers of people.[14] To deliver real-world financial returns on these massive technology investments, these "Big Tech"[15] giants turned to a

---

[11] Jathan Sadowski, *When Data is Capital: Datafication, Accumulation, and Extraction*, 6 BIG DATA & SOC'Y 1, 1 (2019) ("The collection and circulation of data is now a central element of increasingly more sectors of contemporary capitalism.").

[12] *The Birth of the Web*, CERN, https://home.cern/science/computing/birth-web (last visited Oct. 15, 2022).

[13] *See generally* Chris Alcantara et al., *How Big Tech Got So Big: Hundreds of Acquisitions*, WASH. POST (Apr. 21, 2021), https://www.washingtonpost.com/technology/interactive/2021/amazon-apple-facebook-google-acquisitions/ ("[Google's] products, most of which are free, are used by billions of people worldwide. . . . [User] growth is what Facebook has thrived on, and it hasn't been stingy about paying to buy new platforms that could pose a competitive threat in the future.").

[14] *See generally id.* ("In its first decade, Google used search to build a powerful advertising business that generated billions of dollars in revenue . . . . Facebook makes money through advertisements and has used its profits to spread its tendrils across the ad ecosystem.").

[15] "Big Tech" is ordinarily defined as the US-based, multinational corporations Apple, Amazon, Microsoft, Google, and Facebook/Meta. Kean Birch & Kelly Bronson, *Big Tech*, 31 SCI. AS CULTURE 1, 1 (2022). For the purposes of this Comment, the term "Big Tech" will refer to this same group of corporations.

tried-and-true monetization strategy: advertising.[16] The unique nature of this digital connectivity gave companies new tools that did not exist in prior forms of media: the ability to track engagement at a fine-grained level and correlate this engagement with a digitally-captured profile of our interests and activities.[17] This tracking began within individual sites, with first-party tracking. However, in a never-ending effort to increase the commercial value of users' information, companies devised ways to track users across the Internet with third-party tracking.[18]

In 2022, global Internet advertising revenue was $484 billion in U.S. dollars and is projected to increase to $663 billion by 2027.[19] Unfortunately, this windfall in Big Tech profits came at a cost to society—a mass-scale infringement on users' privacy. Despite originating from consumers' private behavior, user data was historically considered "company property and a proprietary secret."[20] For many years this enabled Big Tech to build a "digital curtain" around the data economy and "obscure the industry's practices from lawmakers and the public."[21] This curtain has since been lifted, as recent high-profile breaches (e.g., Equifax)[22] and scandals (e.g., Facebook and Cambridge Analytica)[23] have repeatedly cast the data economy in a negative

---

[16] *See* discussion *infra* Section II.B.

[17] *See* discussion *infra* Section II.B.

[18] *See* discussion *infra* Section II.B.

[19] Statistica Research Department, *Global Internet Advertising Revenue 2018–2027*, STATISTICA (Sept. 27, 2023), https://www.statista.com/statistics/237800/global-internet-advertising-revenue/.

[20] Hossein Rahnama & Alex Pentland, *The New Rules of Data Privacy*, HARV. BUS. REV. (Feb. 25, 2022), https://hbr.org/2022/02/the-new-rules-of-data-privacy.

[21] *Id.* (internal quotation marks omitted).

[22] Gregory S. Gaglione Jr., *The Equifax Data Breach: An Opportunity to Improve Consumer Protection and Cybersecurity Efforts in America*, 67 BUFF. L. REV. 1133, 1160 (2019) ("On September 7, 2017, Equifax announced that criminal hackers attacked and infiltrated its servers. This data breach affected approximately 143 million U.S. consumers, which accounts for nearly 44% of the U.S. population.").

[23] Alexis Ward, *The Oldest Trick in the Facebook: Would the General Data Protection Regulation Have Stopped the Cambridge Analytica Scandal?*, 25 TRINITY C.L. REV. 221, 221 (2022) ("[Whistleblower] Christopher Wylie revealed that Cambridge Analytica had accessed millions of users' Facebook data for hyper-targeted messaging aimed at garnering votes for Republican political clients.").

light, raising public awareness about the risks associated with insufficient information privacy standards.[24]

This systemic state of compromised privacy—referred to in this Comment as "the privacy dilemma"—forced society to search for solutions, and the convergence of consumer, foreign government, and market forces has played a role in giving users more control over their personal data.[25] The broader implication of these developments is a "notable incongruence between public preferences and current US data protection laws."[26] This incongruence is perpetuated by insufficient avenues of consumer redress. In an attempt to strengthen privacy protections and establish meaningful accountability for major offenders, this Comment provides a stepping stone toward consumer redress and will examine the possibility of a private right of action for consumers for Internet privacy disputes.

Part II of this Comment explores the demise of information privacy via the transition from the 1990s World Wide Web and analyzes legislative and judicial responses to similar privacy challenges triggered by early twentieth-century technologies. Part III examines the pitfalls of common statutory claims utilized by class action plaintiffs in Internet privacy disputes and the limitations of market-self regulation as a privacy solution. Part IV argues that the privacy dilemma has created circumstances that justify reexamining the scope of a common law private right of action and considers a new framework for recognizing intrusion upon seclusion in Internet privacy disputes. Part V concludes this Comment.

## II. BACKGROUND

### *A. Anonymous by Design: Foundations of Internet Privacy*

Anonymity played an important role in the political and social construction of the United States prior to and during its inception.[27] The

---

[24] Cason Schmit et al., *US Privacy Laws Go Against Public Preferences and Impede Public Health and Research: Survey Study*, 23 J. MED. INTERNET RSCH. 1 (2021).

[25] Rahnama & Pentland, *supra* note 20.

[26] Schmit et al., *supra* note 24.

[27] *See* Jennifer B. Wieland, Note, *Death of Publius: Toward a World Without Anonymous Speech*, 17 J.L. & POL. 589, 591–92 (2001) ("[T]he early political climate of the United States

United States Supreme Court recognized the fundamental importance of anonymous communication as a cornerstone of free speech: "Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society."[28] Inspired by the Founding Fathers,[29] the original architects of the Internet believed anonymous communication was the key to creating a public domain for free speech.[30] In light of this, the Internet was designed to enable the dissemination and free flow of information, with its foundations grounded in anonymity.[31]

In 1968, J.C.R. Licklider, a director at the United States Department of Defense Advanced Research Projects Agency (ARPA), believed society was on the cusp of a computing revolution and envisioned a new technology that would dramatically alter the way humans interacted with the world.[32] In a

---

was replete with anonymous writings. During pre-Revolution political debates, essays and pamphlets published under pseudonyms influenced public opinion. . . . [T]he *Federalist Papers* . . . were initially published as letters to the editor under the joint pseudonym 'Publius.'").

[28] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) (citation omitted) (citing J. Mill, ON LIBERTY AND CONSIDERATIONS ON REPRESENTATIVE GOVERNMENT 1, 3–4 (R. McCallum ed. 1947)).

[29] *See id.* at 360 (Thomas, J., concurring) ("There is little doubt that the Framers engaged in anonymous political writing.").

[30] *See Digital Future of the United States: Part I—The Future of the World Wide Web: Hearing Before the Subcomm. on Telecomms. and the Internet of the H. Comm. on the Energy & Com.*, 110th Cong. (2007) (statement of Sir Timothy Berners-Lee, Mass. Inst. of Tech.)(expressing to the Committee that the Web was envisaged as an extension of democratic traditions); *see also* Tim Berners-Lee, *A Magna Carta for the Web*, TED (Mar. 2014), https://www.ted.com/talks/tim_berners_lee_a_magna_carta_for_the_web (proposing a bill of rights for the Web that would include protection for privacy, free speech, and anonymity) ("What sort of web do you want? . . . I want a web which has got, for example, . . . a really good basis for democracy.").

[31] *See* James A. Hendler, *The Future of the Web*, *in* THE INTERNET AND PHILOSOPHY OF SCIENCE 71, 78 (1st ed. 2022) (identifying openness, free exchange of information, and ability to scale as key design features of Berners-Lee's invention); *see also infra* text accompanying notes 24–33.

[32] Russell Brandom, *We Have Abandoned Every Principle of the Free and Open Internet*, THE VERGE (Dec. 19, 2017, 9:37 AM), https://www.theverge.com/2017/12/19/16792306/fcc-net-neutrality-open-internet-history-free-speech-anonymity.

landmark paper titled "The Computer as a Communication Device," Licklider described "a radically new organization of hardware and software, designed to support many more simultaneous users than the current systems, and to offer them . . . the fast, smooth interaction required for truly effective man-computer partnership."[33] Licklider was the first to conceptualize networked computers capable of sharing data across a distance.[34] Specifically, Licklider envisioned a patchwork of decentralized (i.e., anonymous by design) networks whose openness would serve as a forum for the free exchange of ideas.[35] Licklider's vision catalyzed the rapid evolution of technological advancements that were necessary to bring it to life.[36] Most notably, in 1989, Tim Berners-Lee invented the World Wide Web ("Web") in response to a demand for a universal automated information-sharing platform between scientists in research institutions around the world.[37] Since its inception, the Web has evolved into a "powerful, ubiquitous tool because it was built on egalitarian principles."[38] According to Berners-Lee, information networks and the free flow of information "stand at the core of our economies, our democracies, and our cultural and personal lives."[39]

In its infancy, Internet engagement was inherently anonymous.[40] True anonymity represents "a state implying the absence of personally identifying

---

[33] J.C.R. Licklider & Robert W. Taylor, *The Computer as a Communications Device*, SCI. & TECH. (1968), *reprinted in* IN MEMORIAM: J.C.R. LICKLIDER 1915–1990 21, 31 (Digit. Equip. Corp. 1990) (1968).

[34] Verblio, *Who is the Father of the Internet?*, WOZ U (June 23, 2020), https://woz-u.com/blog/who-is-the-father-of-internet/.

[35] Brandom, *supra* note 32.

[36] Verblio, *supra* note 34.

[37] *The birth of the Web*, CERN, https://home.cern/science/computing/birth-web (last visited Oct. 15, 2022).

[38] Tim Berners-Lee, *Long Live the Web: A Call for Continued Open Standards and Neutrality*, SCI. AM. (December 1, 2010), https://www.scientificamerican.com/article/long-live-the-web/.

[39] *Digital Future of the United States: Part I*, *supra* note 30.

[40] *See* Christian Keil, *The Origin Story of Web 1.0 and 2.0*, MEDIUM (Nov. 28, 2021), https://medium.com/pronouncedkyle/the-origin-story-of-web-1-0-and-2-0-d97f40b6f2a5 (referring to anonymity as one of the most powerful features of Web 1.0) ("There is no way to be truly anonymous in the real world. On the web, however, 'lurking' is simple and even those

qualities."[41] As a means for obtaining anonymity, users can employ pseudonyms, a tool used "to facilitate nonidentifiable content."[42] The use of pseudonyms in lieu of real-life personas ("pseudo-identities") was pervasive in the 1990s state of the Internet,[43] also known as Web 1.0.[44] To the average user, the Web was a formidable and strange place.[45] Although surfing the Web provided revolutionary ease of access to information, there was a common understanding among early users that safe Internet exploration necessitated pseudo-identities since it was impossible to know exactly who was on the other side of the screen.[46] Like nearly everything on the Internet, pseudo-identity culture fostered an anonymous Internet community that served positive, egalitarian purposes but also inadvertently protected illegal undertakings on the dark web.[47]

---

who participate on sites are only identifiable by a 'username' that needn't bear any relation to one's true self."); *see also* Peter Steiner, *"On the Internet, Nobody Knows You're a Dog"* (illustration), *in* NEW YORKER, July 5, 1993, at 61.

[41] Bernie Hogan, *Pseudonyms and the Rise of the Real-Name Web*, *in* A COMPANION TO NEW MEDIA DYNAMICS 290, 293 (John Hartley, Jean Burgess & Axel Bruns eds., 2013) (emphasis omitted).

[42] *Id.*

[43] *See id.* at 293–94, 298.

[44] Ku. Chhaya A. Khanzode & Dr. Ravindra D. Sarode, *Evolution of the World Wide Web: From Web 1.0 To 6.0*, 6 INT'L J. DIG. LIBR. SERVS. 1, 2 (2016) ("Web 1.0 was first implementation of the web and lasted from 1989 to 2005.").

[45] Hogan, *supra* note 41, at 298.

[46] *Id.*

[47] The web is comprised of three layers, known as the surface web, deep web, and dark web. *The Dark Web: An Overview*, CONG. RSCH. SERV. 1, 1 (2022), https://crsreports.congress.gov/product/pdf/IF/IF12172. The surface web is the familiar interface for regular users, comprised of content that has been indexed and is accessible through search engines. *Id.* The deep web describes the segment of content that is not indexed, and is therefore not accessible through traditional search engines. *Id.* The deep web is comprised of content from private intranets (internal networks of corporations and government agencies) and commercial databases (Westlaw/Lexis) that often require authentication and permission to access. *Id.* The dark web is the segment of the deep web where content is intentionally hidden and generally inaccessible without special software. *Id.* The dark web can be reached through "decentralized, anonymized nodes on various networks including Tor (short for The Onion Router) or I2P (Invisible Internet Project)." *Id.*

Because of its dual utility, anonymity on the Internet can be thought of as a double-edged sword. Anonymity and freedom of information promote the ideas repeatedly reflected by Berners-Lee—anonymous communication promotes free speech, makes political dissension safer in oppressive regimes, advances democracy, and facilitates desired practices such as whistleblowing.[48] The primary danger associated with anonymity, on the other hand, is lack of accountability.[49] This danger can manifest in various forms, including anonymous activities such as cybersmearing,[50] trolling,[51] doxing,[52] and cybercrime.[53]

Technology-driven solutions to make the Internet safer exist, and next-generation technology solutions such as Web3, a new iteration of the Internet based on blockchain technologies, are being contemplated.[54] Despite these developments, the loss of anonymity and the proliferation of tracking technologies have opened the door to a wide variety of new unresolved problems, while leaving the preexisting pitfalls of anonymous communication largely intact.[55] The bad actors who want to stay anonymous

---

[48] Craig R. Scott, *Benefits and Drawbacks of Anonymous Online Communication: Legal Challenges and Communicative Recommendations*, 41 FREE SPEECH Y.B. 127, 131–32 (2004).

[49] *Id.* at 130.

[50] Cybersmearing is a form of online defamation where the identity of the defendant is unknown. *See, e.g.*, Joshua R. Furman, *Cybersmear or Cyber-SLAPP: Analyzing Defamation Suits Against Online John Does as Strategic Lawsuits Against Public Participation*, 25 SEATTLE U. L. REV. 213, 214 (2001).

[51] The Merriam-Webster dictionary defines trolling as "to antagonize (others) online by deliberately posting inflammatory, irrelevant, or offensive comments or other disruptive content." *Troll*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/troll (last visited Jan. 18, 2024).

[52] Doxing involves taking a person's personal information and disseminating it as widely as possible as a form of online harassment. *See, e.g.*, Eric Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing*, 21 GLOB. COMM'N ON INTERNET GOVERNANCE 1, 3 n.7 (2015).

[53] Scott, *supra* note 48, at 130–31.

[54] *See* discussion *infra* Section III.B.2.

[55] *See, e.g.*, Sarah Oates, *The Easy Weaponization of Social Media: Why Profit has Trumped Security for U.S. Companies*, 1 DIGIT. WAR 117, 117 (2020) (arguing that the myriad of problems wrought by social media including misinformation, deepfakes, and trolling, are not unfortunate side effects of a democratizing technology, but rather the design of social

remain able to do so,[56] while the innocent user now creates a digital footprint that is used to sell personally identifiable information; nurture addiction to maximize profit; and manipulate people's views, emotions, and behavior.[57] Thus, the issue can be stated as a modern twist on a famous quote by Benjamin Franklin: if you trade privacy for security, you lose both.[58]

### *B. The Technological Unraveling of Privacy: Tracking Across the Internet and the Data Monopoly*

As times changed, it became clear that the qualities that made the early version of the Web simplified, sparse, and unfamiliar were bound to be replaced.[59] The current version of the Web, also known as Web 2.0, is now densely connected, detailed, and intertwined into virtually every aspect of people's daily lives.[60] By default, present-day engagement on the Internet is anything but anonymous. This can be attributed to two primary developments. First, Big Tech unraveled Internet anonymity through the use of tracking technology and the collection and monetization of personally identifiable information.[61] Second, the use of pseudo-identities fell out of

---

media fosters information warfare) ("The problem with trying to 'balance' both the benefits of social media such as its challenge to censorship and ability to aggregate social movements against destructive elements such as disinformation and the loss of privacy suggests we can somehow offset one side against the other.").

[56] Jardine, *supra* note 52, at 1 ("Illegal markets, trolls and online child abuse rings proliferate due to the technology of Tor and other similar systems.").

[57] *See, e.g.*, THE SOCIAL DILEMMA (Netflix 2020).

[58] Benjamin Franklin is often quoted to have said: "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." *Ben Franklin's Famous 'Liberty, Safety' Quote Lost its Context in 21st Century*, NPR (Mar. 2, 2015, 4:15 PM), https://www.npr.org/2015/03/02/390245038/ben-franklins-famous-liberty-safety-quote-lost-its-context-in-21st-century. Although there is a debate about the interpretation and application of this quote in the context of new technology amid concerns of government surveillance, Franklin's words are often applied to these issues. *Id.*

[59] Hogan, *supra* note 41, at 299.

[60] *Id.*

[61] Asunción Esteve, *The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA*, 7 INT'L DATA PRIV. L. 36, 36–37 (2017).

favor due to the rise of social media.[62] Accordingly, the "real-name web" has emerged,[63] eradicating the control users once had over their privacy through self-secured anonymity.[64]

Following the expansion of the Web, Big Tech emerged, along with new business models based on acquiring users' personal information and monetizing that data.[65] All too soon the idealistic promise of the free flow of information and anonymity envisioned by Berners-Lee was "steamrolled by businesses doing what businesses do best: generat[ing] returns for [their] shareholders and putting [consumer] privacy second."[66] As it turns out, luring a critical mass of users proved to be the most important prerequisite to the success of present-day data monopolies.[67] Big Tech is present-day proof that collecting and analyzing information about a user's interests and activities is extremely useful for micro-targeted advertising, and it is

---

[62] The rise in Internet tracking was accompanied by the gradual decline in online pseudo-identities in favor of real-name user profiles. The growth of social networking sites can be attributed to this phenomenon because the utility of these applications could only be derived if users used their real names. *See generally* Hogan, *supra* note 41, at 290–307. If one created a fake profile, they would be hindered from the main benefit of using a social network site—transcending real-life connections into the online sphere. For example, Facebook requires people to use their real identities on their social network because Zuckerberg believes people behave differently when they cannot hide behind online pseudoidentities. Zuckerberg is famously quoted to have said "[h]aving two identities for yourself is an example of a lack of integrity." Miguel Helft, *Facebook, Foe of Anonymity, Is Forced to Explain a Secret*, N.Y. TIMES (May 13, 2011), https://www.nytimes.com/2011/05/14/technology/14facebook.html.

[63] The mass success of social media companies reinforced the newfound sense of comfort in having an online presence attached to users' real identities, and as a result, the real-name web was born. *See generally* Hogan, *supra* note 41.

[64] The choice to remain anonymous or not has been described as an "interest in . . . self-determination that is central to an interest in privacy." Hogan, *supra* note 41, at 302. Some commentators have likened the harm of deanonymization to the loss of the ability to be anonymous—the dilemma choice between being deanonymized and self-censorship. *See, e.g.*, Björn Lundgren, *Beyond the Concept of Anonymity: What is Really at Stake?*, *in* BIG DATA AND DEMOCRACY 201, 213 (Kevin Macnish & Jai Galliott eds., 2020).

[65] Esteve, *supra* note 61, at 36.

[66] Tom Chavez et al., *Toward Data Dignity: How We Lost Our Privacy to Big Tech*, FORTUNE (Jan. 28, 2022, 5:30 AM), https://fortune.com/2022/01/28/big-tech-data-privacy-ethicaltech/.

[67] *Id.*

unsurprising that the economic value of these companies is largely based on the monetization of user data.[68] This monetization of user data may be understood from the familiar phrase: "You are the product,"[69] which represents the idea that if a product is free for users, then the company makes money by allowing advertisers to reach its users.[70]

With the end goal of selling its viewership, Big Tech would employ new tracking technologies in order to maximize the value of otherwise disconnected information.[71] Thus, a new digital breadcrumb was born: the cookie.[72] First-party cookies are based on the idea that each website visitor stands in a "first-party, or direct, relationship with that site's owner."[73] This relationship is advertised as allowing Internet providers to cater to each visitor's individual needs.[74] Third-party cookies are those created by a different business than the website domain owner.[75] Although third-party cookies have proven beneficial for extensive personalization and utility across the Internet, they have also facilitated mass-scale tracking of user activity online.[76] Cookies were not created for the purpose of tracking, however: "Most information collected using cookies is anonymous because

---

[68] Esteve, *supra* note 61, at 36.

[69] The earliest mention of this quote can be traced back to a 1973 broadcast titled "Television Delivers People." *See You're Not the Customer; You're the Product*, QUOTE INVESTIGATOR (July 16, 2017), https://quoteinvestigator.com/2017/07/16/product/. The short film consists of white messages displayed against a blue backdrop, slowly scrolled upward to a soundtrack. *See* KunstSpektrum, *Richard Serra "Television Delivers People" (1973)*, YOUTUBE (Feb. 2, 2011), https://www.youtube.com/watch?v=LvZYwaQlJsg. The pertinent messages displayed state: "It is the consumer who is consumed" and "[y]ou are the product." *Id.*

[70] *See generally* John Lanchester, *You Are the Product*, 39 LONDON REV. BOOKS 1 (2017) (explaining how Facebook exemplifies the idea that in this internet-age "if the product is free, you are the product").

[71] *Id.* at 3.

[72] Rico Bornschein et al., *The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices*, 39 J. PUB. POL'Y & MKTG. 135, 135 (2020) ("Online retailers, publishers, and ad networks have long had unrestrained power over consumers' private information through one key technology: cookies.").

[73] Chavez et al., *supra* note 66.

[74] *Id.*

[75] *Id.*

[76] *Id.*

the user's computer does not convey any personally identifiable information about the user to the third party in the process."[77] It is only once a user submits personal information to a website that the third party can "begin to create a personally identifiable profile of the user."[78] The amount of information that can be gathered from a single third-party cookie is substantial, representing "approximately 300 pages of single[-]spaced information about the user."[79] Once the value of this information was realized, cookies became susceptible to abuse. Consequently, Big Tech "used cookies to seize control over the data economy and maintained market power" ever since—at the expense of user privacy.[80]

### *C. The Development of Privacy Law in Response to New Technology*

#### 1. Common Law Origins of the Right to Privacy and the Invasion of Privacy Torts

Mark Twain once said that "[h]istory doesn't repeat itself, but it often rhymes."[81] Throughout the nineteenth and twentieth centuries, new technology was frequently accompanied by an erosion of privacy. In 1890, Harvard law students Samuel Warren and Louis Brandeis authored *The Right to Privacy*, a seminal article that advocated for a distinct right to privacy for the first time.[82] The article was influenced by the vast expansion of the newspaper and the proliferation of "yellow journalism," under which companies profited off of "sensationalistic topics such as scandals and gossip about people's lives."[83] Warren and Brandeis were concerned that the sensationalistic press coupled with the invention of the hand-held camera

---

[77] Mathew C. Keck, *Cookies, the Constitution, and the Common Law: A Framework for the Right of Privacy on the Internet*, 13 ALB. L.J. SCI. & TECH. 83, 90 (2002).

[78] *Id.*

[79] *Id.*

[80] Chavez et al., *supra* note 66.

[81] Brian Adams, *History Doesn't Repeat, But It Often Rhymes*, HUFFINGTON POST (Jan. 18, 2017, 6:47 PM), https://www.huffpost.com/entry/history-doesnt-repeat-but-it-often-rhymes_b_61087610e4b0999d2084fb15.

[82] DANIEL J. SOLOVE, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY 1–1, 1–10 (Christopher Wolf ed., 2006).

[83] *Id.* at 1–10, 1–11.

would lead to a "dangerous mix" where unsolicited photographs could subsequently be exploited for the media.[84] These unprecedented intrusions would require a remedy—one that Warren and Brandeis recognized existing common law did not afford.[85] Defamation law was limited to protecting false, as opposed to private, information.[86] Contract law could only control privacy to the extent it was defined as part of a contractual relationship between two parties and, therefore, could not protect against third-party intrusions.[87] Property law was similarly inadequate: "[W]here the value of the production is found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all, it is difficult to regard the right as one of property."[88]

Warren and Brandeis instead argued for an expansion of the common law to meet the new demands of society. They recognized that "[t]he common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[89] These rights, the authors argued, were derived from "the more general right of the individual to be let alone."[90] From this, Warren and Brandeis proposed "[a]n action of tort for damages in all cases"[91] and opined that "[i]f the invasion of privacy constitutes a legal [injury], the elements for demanding redress exist, since already the value of mental suffering, caused by an act wrongful in itself, is recognized as a basis for compensation."[92] Although "[t]he article had little immediate effect upon the law[,]"[93] courts eventually began to recognize a right to privacy, and the common law tort for invasion of privacy was born.[94]

---

84 *Id.* at 1–11.

85 *Id.*

86 *Id.*

87 *Id.*

88 Warren & Brandeis, *supra* note 4, at 200.

89 *Id.* at 198.

90 *Id.* at 205.

91 *Id.* at 219.

92 *Id.* at 213.

93 William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 384 (1960).

94 *Id.* at 386.

In 1960, Warren and Brandeis's privacy tort was reevaluated by the distinguished tort scholar William Prosser, who surveyed over three hundred privacy cases that had arisen since *The Right to Privacy*'s publication.[95] From the cases, Prosser deduced four distinct torts: (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) publicity placing a person in false light, and (4) appropriation of name or likeness.[96] This delineation proved to be highly influential. The categories were formally adopted into the Restatement (Second) of Torts[97] and today the vast majority of states recognize these torts either by statute or common law.[98]

### 2. The Evolution of Wiretapping Statutes and the "Reasonable Expectation of Privacy" Test

The influence of the common law right to privacy on both legislative efforts and judicial interpretation is exemplified in Fourth Amendment jurisprudence and the development of the "reasonable expectation of privacy" test, which uncoincidentally borrowed its critical element from one of the four original privacy torts—intrusion upon seclusion.[99] As such, wiretap case law and subsequent statutes are prime examples of how one area of privacy law evolved in response to emerging technologies, including the various legislative and judicial approaches employed to mitigate these challenges.

Wiretapping first became an issue of public concern when new methods of intercepting communications were developed shortly after the telephone was patented in 1881.[100] As the public grew aware of "[t]he ease of wiretapping and the value of the information that could be learned," state legislatures moved swiftly to condemn the conduct, and by 1927 wiretapping

---

95 *Id.* at 388–89.

96 *Id.* at 389.

97 *See* RESTATEMENT (SECOND) OF TORTS §§ 652B–E (AM. LAW INST. 1965).

98 *See id.* § 652A cmt. a (AM. LAW INST. 1965) ("[T]he existence of a right of privacy is now recognized in the great majority of the American jurisdictions that have considered the question.").

99 *See* discussion *infra* Section IV.

100 PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 111 (1995).

was a crime in more than twenty-five states.[101] Despite this, federal and state law enforcement agencies regularly utilized wiretapping in criminal investigations.[102] Paradoxically, illegally obtained wiretap evidence was admissible in court notwithstanding the state law prohibitions against wiretapping.[103] The constitutionality of this practice was tested in *Olmstead v. United States*.[104] The Court upheld a conviction predicated on illegal wiretap evidence collected by federal agents, ruling that the wiretapping did not violate the Fourth or Fifth Amendments because there was no physical trespass and hence no "search" was involved, and there was no "seizure" of tangible property.[105] In his oft-quoted dissent, Justice Brandeis argued that the Fourth Amendment protected individual privacy and warned against "[t]he progress of science in furnishing the Government with means of espionage."[106] The *Olmstead* decision in effect added illegal wiretapping to the arsenal of the common law of evidence—a result that sparked wide criticism from the dissenting Justices,[107] the public, and the media.[108] Once the constitutional argument was foreclosed, the opposition "moved the policy debate to the executive and Congress."[109] The efforts were not in vain.

---

101 *Id.*

102 *Id.*

103 *Id.* ("Although wiretapping was prohibited under Washington state law, Washington did not deny the admissibility of illegally obtained evidence.").

104 *See generally* Olmstead v. United States, 277 U.S. 438 (1928) (holding that wiretapping that is unaccompanied by a physical intrusion into a constitutionally protected area is not a search under the Fourth Amendment).

105 *Id.* at 464–65.

106 *Id.* at 474 (Brandeis, J., dissenting).

107 *Id.* at 470 (Holmes, J., dissenting) ("If the existing code does not permit district attorneys to have a hand in such dirty business it does not permit the judge to allow such iniquities to succeed.").

108 REGAN, *supra* note 100, at 112 ("Public and press reaction to the *Olmstead* decision was largely critical. The *New York Times*, for example, editorialized that 'Prohibition, having bred crimes innumerable, has succeeded in making Government the instigator, abettor and accomplice of crime. It has now made universal snooping possible.'" (quoting Editorial, *Government Lawbreaking*, N.Y. TIMES, June 6, 1928, at 24)).

109 *Id.*

Six years after *Olmstead*, Congress enacted section 605 of the Federal Communications Act of 1934.[110]

The wiretap debates illustrated an important principle: the outer boundaries of the constitutional right to privacy hinge on the ever-changing societal perception of what should remain private.[111] From the judiciary's recognition of this maxim emerged a new approach to determining the Fourth Amendment's applicability—the reasonable expectation of privacy test.[112] A skeletal application of the test was used to overturn *Olmstead* in *Katz v. United States* and asks (1) whether a person exhibits an "actual (subjective) expectation of privacy" and whether (2) "the expectation [is] one that society is prepared to recognize as 'reasonable.'"[113] In adopting this new framework, the Court rejected a strict application of *Olmstead*'s physical trespass requirement and instead stated that the absence of trespass was not determinative.[114] This sudden shift in perspective could be explained by the recent publication of the Restatement (Second) of Torts in 1965, a mere two years before *Katz* was decided.[115] Based on this suspicious timing, it is conceivable that the "reasonable expectation of privacy" language of *Katz* was borrowed from Prosser's enumerated common law privacy torts. Similarly, the Court's deviation from the trespass doctrine may have subconsciously heeded the calls of Warren and Brandeis for courts to recognize a right to privacy that could not otherwise be secured through property law.[116] These common law underpinnings demonstrate that the judiciary, at a minimum, searches for inspiration from the common law to better meet the demands of

---

[110] The Communications Act of 1934, Pub. L. No. 73-416, § 605, 48 Stat. 1103 (codified at 47 U.S.C. § 605 (1982)).

[111] *See generally* Kasper, *supra* note 3, at 170 (explaining the social implications of changes in privacy).

[112] REGAN, *supra* note 100, at 122.

[113] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[114] *Id.* at 353 (majority opinion) ("[T]he reach of [the Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.").

[115] *See id.* (decided in 1967); John W. Wade, *Second Restatement of Torts Completed*, 65 AM. BAR. ASS'N. J. 366, 366 (1979) (noting that the first two volumes of the Second Restatement of Torts came out in 1965).

[116] Warren & Brandeis, *supra* note 4, at 200.

changing times, particularly in cases where technology appears to have outpaced the previous tests observed.

After *Katz*, Congress promptly enacted a comprehensive statute to address the wiretapping concerns, expanding its statutory protections to state officials as well as private parties and removing the issue from the courts—at least temporarily.[117] The harmony was short-lived, as the introduction of new technology has continuously revived the privacy issues presented in *Katz,* and the Court has had numerous opportunities to enrich Fourth Amendment case law since the turn of the Century.[118] The continued expansion of the reasonable expectation of privacy test has solidified the common law's influence on Fourth Amendment jurisprudence and may serve as a model for privacy infringements in other contexts. From this it is clear that the spirit of Warren and Brandeis' seminal article ought to be maintained—the common law is suitable to adapt to changing views and perspectives in the absence of conflicting laws or regulations.[119] As one commentator has stated: "Given the background provided by the traditional common law invasion of privacy torts, the creation of a new tort or the extension of an existing tort is not beyond the role of the judiciary or the legislature."[120]

---

[117] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 34 U.S.C. § 10101).

[118] *See, e.g.*, Riley v. California, 573 U.S. 373, 401–02 (2014) (quoting Kentucky v. King, 563 U.S. 452, 460 (2011)) (searching a cell phone seized incident to arrest without first obtaining a warrant to search violates the Fourth Amendment absent exigent circumstances); United States v. Jones, 565 U.S. 400, 404 (2012) (installing a GPS device on a target's vehicle and using the device to monitor the vehicle's movements without a warrant violates the Fourth Amendment); Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (denying Fourth Amendment protection to pen registers).

[119] *See generally* Warren & Brandeis, *supra* note 4 (arguing for an expansion of the common law to meet the demands of society); *see also* Keck, *supra* note 77, at 107 (recognizing the role of the judiciary in the expansion of the common law and the creation of the traditional privacy torts).

[120] Keck, *supra* note 77, at 107.

### 3. Federal Privacy Law as a Balancing of Interests and the Rise of Government Surveillance

Following the era of wiretap debates, the invention of the computer and the Internet vastly changed the type and quantity of information that could be gathered and the means by which interested parties could gather it. Privacy once again became an increasing public concern.[121] In response to these concerns, the 1980s and 1990s marked a progressive era for federal privacy statutory protection.[122] The most influential of these laws were the Electronic Communications Privacy Act of 1986, the Electronic Freedom of Information Act Amendments of 1996, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[123] The Electronic Communications Privacy Act of 1986 was the expansion of the previous wiretap statute and restricts the interception of new forms of transmitted communication with a particular focus on computers.[124] This Act, more commonly known as the "Wiretap Act," continues to serve as a basis for modern Internet privacy disputes, despite the fact that the language was drafted to fit the privacy issues presented by technology in the 1980s.[125] The Electronic Freedom of Information Act Amendments of 1996 and its predecessors[126] were born in response to a public desire for government transparency, and the laws have been described as "benchmark[s] of

---

[121] Solove, *supra* note 82, at 1–24.

[122] *See id.* at 1–33 to 1–39.

[123] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. § 2510); Electronic Freedom of Information Act Amendments of 1996, Pub. L. No. 104-231, 110 Stat. 3048 (codified as amended at 5 U.S.C. § 552); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended at 42 U.S.C. § 1320d-6).

[124] Electronic Communications Privacy Act of 1986.

[125] *See* discussion *infra* Section III.A.1.

[126] The original Freedom of Information Act was passed in 1966, and was amended twice: once in 1986 and 1996. *See generally* Freedom of Information Act of 1966, Pub. L. No. 89-487, 80 Stat. 250 (codified as amended at 5 U.S.C. § 552); Freedom of Information Reform Act of 1986, Pub. L. No. 99-570, 100 Stat. 3207; Electronic Freedom of Information Act Amendments of 1996.

democratic development."[127] The amendments embodied in the 1996 Act reflect the desire to match previous protections offered by earlier versions of the same statute by including language that better fits the demands of new technology.[128] HIPAA was the first federal statute to directly address medical information privacy[129] and strictly regulates the use and disclosure of sensitive health information by "covered entities."[130] HIPAA's privacy directive was one of the first aimed at balancing the privacy interests of the individual with the competing interests of an entire industry.[131]

These major milestones in privacy law temporarily led to a delicate equilibrium in the interests of four parties to any given form of information: the individual, the government, the relevant industry, and the public. In particular, these legislative efforts were directed at protecting the individual's privacy interests by regulating the actions of the more powerful parties. This trend did not last long—following the September 11 terrorist attacks, individual privacy interests yielded to the government's high national security interest in surveillance.[132] In light of this, the early 2000s witnessed a rollout of various directives, including the enlargement of foreign intelligence gathering methods;[133] the creation of the Department of

---

[127] OPEN SOC'Y JUST. INITIATIVE, TRANSPARENCY AND SILENCE: A SURVEY OF ACCESS TO INFORMATION LAWS AND PRACTICES IN FOURTEEN COUNTRIES 21 (2006).

[128] The amendments require administrative agencies to include electronic documents within the scope of Freedom of Information Act (FOIA) requests, respond to FOIA requests electronically, and create electronic agency reading rooms in order for the public to access to commonly requested agency documents. *See generally* Electronic Freedom of Information Act Amendments of 1996.

[129] Solove, *supra* note 82, at 1–37.

[130] *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/phlp/publications/topic/hipaa.html (last visited Jan. 16, 2024); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended at 42 U.S.C. § 1320d-6).

[131] *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, *supra* note 130.

[132] Solove, *supra* note 82, at 1–41.

[133] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

Homeland Security;[134] the facilitation of greater information sharing between federal agencies;[135] and the imposition of new federal standards on state driver's licenses.[136] The shift in focus was not inconsequential—it was during this time that new technologies for data aggregation exploded, and the modern view of data science as an independent discipline was realized for the first time.[137] The security risks associated with the collection and storage of sensitive personal information came to light when several data brokers announced major data breaches in 2005.[138] This renewed public attention to the growing problem of identity theft in the digital age prompted state legislators to enact various forms of data breach notification laws.[139] Despite legislative attempts, however, no federal data breach laws were passed.[140] As such, the development of information privacy law in the United States has largely been left to the states.[141]

---

[134] The Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (codified at 6 U.S.C. § 101).

[135] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458 § 1016, 118 Stat. 3638.

[136] Real ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 302 (codified at 49 U.S.C § 30301).

[137] William S. Cleveland is often attributed to coining the term "data science" in a 2001 paper, by advocating for a new field premised on the expansion of statistics into technical areas. *See* William S. Cleveland, *Data Science: An Action Plan for Expanding the Technical Areas of the Field of Statistics*, 69 INT'L STAT. REV. 21 (2001). In 2003, Columbia University launched *The Journal of Data Science*—the first academic journal to use the term in its title. Gil Press, *A Very Short History of Data Science*, FORBES (May 28, 2013, 9:09 AM), https://www.forbes.com/sites/gilpress/2013/05/28/a-very-short-history-of-data-science/. Since then, "data science" has become a buzzword, and nearly every business wants to employ a data scientist—a position hailed by Harvard Business Review in 2012 as "the sexiest job of the 21st century." Thomas H. Davenport & DJ Patil, *Data Scientist: The Sexiest Job of the 21st Century*, HARV. BUS. REV. (Oct. 2012), https://hbr.org/2012/10/data-scientist-the-sexiest-job-of-the-21st-century.

[138] Solove, *supra* note 82, at 1–45.

[139] *Id.* at 1–46.

[140] *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 917 (2009) ("Congress remains unable to agree on a data breach notification bill—a perfect illustration, as noted earlier, of the slow trajectory of federal privacy legislation.").

[141] *See* Keck, *supra* note 77, at 91 ("[T]here have been many hearings in Congress and over 400 bills mentioning privacy have been proposed. In the state legislatures, the number of

## III. THE PRIVACY DILEMMA

The evolution of common law invasion of privacy torts, wiretap cases, and subsequent statutes illustrate a recurring theme in the development of privacy law: the difficulty in balancing the interest of one party in obtaining private information with the other party's interest in keeping such information private.[142] Justice Alito's concurrence in *United States v. Jones* testifies to the limited ability of courts to gatekeep these issues: "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[143] However, as seen in *Olmstead* and *Katz*, lobbying for progressive interests takes time, and subsequent Fourth Amendment jurisprudence demonstrates that once legislation is passed, new technology can quickly render statutes archaic.[144] This pattern was especially prevalent in wiretapping laws because "advances in communication technologies both precipitate advances in interception technologies and create gaps in existing laws."[145] In the Internet privacy context, the situation is more grim, because "personal information in the private sector is often unaccompanied by the presence of basic legal protections. Yet, private enterprises now control more powerful resources of information technology than ever before."[146] The result is a conundrum—those lobbying for increased privacy rights must wait on the sidelines for the democratic process to hopefully pan out in their favor. Meanwhile, injured

---

privacy-related bills that have been introduced is quadruple that."); *see also* Schwartz, *supra* note 140, at 916 ("[T]he states in the United States have been especially important laboratories for innovations in information privacy law. As noted, the state tradition begins with the recognition of privacy torts throughout the twentieth century.").

142 *See generally* Solove, *supra* note 82 (exploring how the law has emerged and evolved in response to new technologies that have increased the collection, dissemination, and use of personal information).

143 United States v. Jones, 565 U.S. 400, 418, 429 (2012) (Alito, J., concurring).

144 *See, e.g.*, *id.* at 427–28 (first citing 18 U.S.C. §§ 2510–22 (2006 & Supp. IV); and then citing Olmstead v. United States, 277 U.S. 438, 465–66 (1928)).

145 REGAN, *supra* note 100, at 137.

146 Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1633–34 (1999).

plaintiffs are forced to rely on outdated statutes in hopes that modern interpretations will provide relief. When these options fail, market self-regulation through opt-in tracking becomes the sole remedy by which consumers can control third-party access to their personal data. These two alternatives—failed legislation and failed market self-regulation—will be explored in this Part, highlighting why Big Tech has virtually no accountability for privacy violations against its users.

### *A. Legislation Falls Short on Remedies for New-Era Internet Privacy Violations*

Informational asymmetry between Internet users and Big Tech has resulted in lawsuits predicated on Internet tracking violations. In *In re Google*, Google exploited loopholes in competing browser cookie blocker software, allowing them to place third-party cookies on browsers that had activated blockers, despite public assurances that the browsers were designed to prevent just that.[147] Similarly, in *In re Nickelodeon Consumer Privacy Litigation*, Viacom made explicit public assurances that they would not collect any personal information about children who browse their websites and then proceeded to engage in deceitful conduct by furnishing Google with the opportunity to place third-party cookies on the children's computers and track their Internet activity.[148] In *Davis v. Facebook*, Facebook knowingly exceeded user consent agreements by tracking users' online activity after they had logged out of the application.[149] These cases are tied together by a common theme: Big Tech's willingness to engage in deceitful behavior and ability to find and exploit a backdoor to ad revenue at the expense of user privacy.

Plaintiffs in these disputes had difficulties coming up with a strong theory of liability that could appropriately fit their respective injuries into a viable claim, and only recently has there been a shift towards granting plaintiffs with

---

147 *In re* Google Inc., 806 F.3d 125, 132 (3d Cir. 2015).

148 *In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 267 (3d Cir. 2016).

149 Davis v. Facebook, Inc., 956 F.3d 589, 596 (9th Cir. 2020).

an Internet tracking-related privacy injury standing to sue at all.[150] Nonetheless, the most common causes of action for these disputes have all failed for one reason or another—primarily because the federal statutes at issue predate the Internet boom and, as a result, were not intended to be utilized for Internet privacy violations.

1. Wiretap Act[151]

The interception and disclosure of wire, oral, or electronic communications is regulated by 18 U.S.C. § 2510 et seq (Wiretap Act).[152] "A plaintiff pleads a prima facie case under the Act by showing that the defendant '(1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device.'"[153] Congress has created an exemption to criminal and civil liability for a private party

> where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.[154]

In the context of Internet tracking, courts struggle to apply the Wiretap Act because it is unclear whether defendants are a "party" to the electronic

---

[150] *See In re* Facebook Internet Tracking Litig., 140 F. Supp. 3d 922, 932 (N.D. Cal. 2015) (no Article III standing); *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 988 F. Supp. 2d 434, 442 (D. Del. 2013) (no Article III standing). *But see In re* Facebook Internet Tracking Litig., 263 F. Supp. 3d 836 (N.D. Cal. 2017) (Article III standing in second amended complaint); *In re Google*, 806 F.3d at 135 (Article III standing).

[151] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. § 2510). Although formally titled the Electronic Communications Privacy Act of 1986, the Act is widely known as the "Wiretap" Act and is referred to as such in the cases mentioned in this Comment.

[152] 18 U.S.C. §§ 2510–23.

[153] *In re Google*, 806 F.3d at 135 (quoting in *In re* Pharmatrak, Inc. Priv. Litig., 329 F.3d 9, 18 (1st Cir. 2003)).

[154] 18 U.S.C. § 2511(2)(d).

communications they acquired and tracked via third-party cookies.[155] There is a prevalent circuit split on the issue, with the Ninth Circuit holding that defendants that gather data via third-party cookies are not parties to the transaction,[156] and the Third Circuit holding that they are.[157] Because this determination can be fatal to a plaintiff's claim, the lack of uniformity on this issue exemplifies why applying the Wiretap Act to Internet privacy cases is problematic. The disparity in the Act's interpretation further highlights the fact that, ultimately, the Act is "ill-suited to address modern forms of communication" because it "was written prior to the advent of the Internet and the World Wide Web."[158]

2. Stored Communications Act[159]

Enacted in 1986, the Stored Communications Act (SCA) was "born from congressional recognition that neither existing federal statutes nor the Fourth Amendment protected against potential intrusions on individual privacy arising from illicit access to 'stored communications in remote computing operations and large data banks that stored e-mails.'"[160] Importantly, the SCA protects electronic communications from unauthorized access by third-parties.[161] To state a claim under the SCA, a plaintiff must show that the defendant "(1) intentionally accesse[d] without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed[ed] an authorization to access that facility; and thereby obtain[ed], alter[ed], or prevent[ed] authorized access to a wire or electronic communication while it is in electronic storage in such system."[162]

---

155 *See In re Google*, 806 F.3d at 140.

156 Davis v. Facebook, Inc., 956 F.3d 589, 608 (9th Cir. 2020).

157 *In re Google*, 806 F.3d at 145.

158 United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003) (quoting Konop v. Hawaiian Airlines, 302 F.3d 868, 874 (9th Cir. 2002)); *see also* Blumofe v. Pharmatrak, Inc. (*In re Pharmatrak, Inc. Priv. Litig.*), 329 F.3d 9, 21 (1st Cir. 2003) (expressing the same concern).

159 Stored Communications Act, Pub. L. No. 99-508, 100 Stat. 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701–13).

160 *In re Google*, 806 F.3d at 145 (quoting Garcia v. City of Laredo, 702 F.3d 788, 791 (5th Cir. 2012)).

161 *See* 18 U.S.C. § 2701.

162 *Id.* § 2701(a).

The illicit access that is alleged in Internet tracking disputes is the defendants' access to the plaintiffs' personal web browsers.[163] In this context, standing to sue under the SCA turns on whether an individual's personal computing device is a "'facility through which an electronic communications service is provided.'"[164] Courts considering the issue have accepted that the SCA's "enactment was driven by a congressional desire to protect third-party entities that stored information on behalf of users,"[165] and thereby only "covers access to electronic information stored in *third party* computers."[166] Consequently, personal computing devices are not protected "facilities" under the statute.[167] This illustrates why attempting to squeeze a modern claim into an antiquated statute can be tenuous—claims could be easily limited to those that fall within the statute's original purpose, which likely did not anticipate the plaintiff's particular injury.

3. Computer Fraud and Abuse Act[168]

The Computer Fraud and Abuse Act (CFAA) was enacted in 1986 and is codified at 18 U.S.C. § 1030.[169] The CFAA creates a private right of action for persons "who suffer[] damage or loss" because a third party "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[170] For Internet privacy violations, the viability of a plaintiff's claim rests on whether impermissibly received, personally identifiable information meets the statutory requirement of "damage" or "loss."[171] Under the CFAA, "the term

---

163 *In re Google*, 806 F.3d at 146; *see also In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 277 (3d Cir. 2016).

164 *In re Google*, 806 F.3d at 146 (quoting *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 988 F. Supp. 2d 434, 446 (D. Del. 2013).

165 Davis v. Facebook, Inc., 956 F.3d 589, 609 (9th Cir. 2020).

166 Graf v. Zynga Game Network, Inc., 750 F.3d 1098, 1104 (9th Cir. 2014) (emphasis added).

167 *In re Google*, 806 F.3d at 148.

168 Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030).

169 *See* 18 U.S.C. § 1030.

170 *Id.* § 1030(a)(2)(C), (g).

171 *In re Google*, 806 F.3d at 148; *see* 18 U.S.C. § 1030.

'damage' means any impairment to the integrity or availability of data, a program, a system, or information."[172] Meanwhile, "the term 'loss' means any reasonable cost to any victim, including the cost of . . . restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[173] In recognizing that there is indeed a market for the plaintiffs' personal data, courts nonetheless held that the plaintiffs did not suffer any "damage" or "loss" as contemplated by the CFAA because they "allege[d] no facts suggesting that they ever participated or intended to participate in the market."[174] If the plaintiffs did not intend to monetize their personal information, then the defendants' actions did not prevent the plaintiffs from "capturing the full value of their [I]nternet usage information for themselves."[175] This holding provides another example of courts' general reluctance to broaden the interpretation of statutory language to accommodate unanticipated factual circumstances.

### *B. The Pitfalls of Market-Level Solutions*

#### 1. A Market Standard: Nudging Via Opt-In Tracking

For all of the reasons listed above, it is evident that current federal legislation fails to effectively protect a user's privacy on the Internet. Many argue that federal legislation is not the proper defense in the first place, lobbying instead for a hands-off market approach.[176] Those who subscribe to this view will cite a general "freedom of contract" as the ultimate protector of these rights.[177] But Internet privacy, unfortunately, is one area of life and law

---

[172] 18 U.S.C. § 1030(e)(8).

[173] *Id.* § 1030(e)(11).

[174] *In re Google*, 806 F.3d at 149; *see also In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 278 (3d Cir. 2016) (citing *In re Google*, 806 F.3d at 149).

[175] *In re Google*, 806 F.3d at 149.

[176] Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *in* U.S. DEP'T OF COM., PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE 3, 9–11 (1997) (making a case for market self-regulation).

[177] *Id.* at 5. ("Under the contractual approach, the primary goal is to understand what well-informed parties would agree to, if there were no costly hurdles to their reaching an agreement. A pure market model will fail to the extent that it protects privacy less well than these parties

that is not sufficiently protected by Adam Smith's free market.[178] To show why this is the case, the concept of the "default nudge" merits introduction. "'Nudging' involves structuring the choices that people make in order to lead them towards particular outcomes."[179] Nudging is a "default-based tool" where the default setting is the outcome desired by the provider of the service, and users must "opt-out" to deviate from the pre-selected path.[180] Because opt-out nudges rely on the "volitional limitations of individuals"[181] to depart from the default choice, studies show that the employment of opt-out nudges dramatically increases user participation rates compared to opt-in participation.[182]

In the context of Internet tracking, nudging is utilized as a tool to obtain user consent and facilitate a *quid pro quo* between users and Big Tech—"an imperfect barter transaction in which data [is] swapped for a product."[183] By implementing a no-tracking default, market self-regulation can theoretically be optimized if users are empowered to opt-in to tracking, thereby playing an active role in providing consent to the *quid pro quo*.[184] This approach has been coined "privacy self-management" because it "provid[es users] with a set of rights to enable them to make decisions about how to manage their

---

would have agreed to, if they were fully informed and had some equality of bargaining power.").

178 *Id.*

179 Robert Baldwin, *From Regulation to Behaviour Change: Giving Nudge the Third Degree*, 77 MOD. L. REV. 831, 831 (2014).

180 Robert J. Landry III, *Credit Card Debt and Consumer Bankruptcy: Can We 'Nudge' Our Way Out?,* 27 AM. BANKR. INST. L. REV. 139, 146, 152 (2019).

181 *Id.* at 152.

182 *See* Shlomo Benartzi et al., *Should Governments Invest More in Nudging?,* 28 PSYCH. SCI. 1041, 1046 tbl.2. (2017) (collecting and summarizing studies of the "Relative Effectiveness of Interventions Targeting Retirement Savings").

183 Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1385 (2017).

184 The implementation of this nudge typically involves a pop-up consent banner that requires the user to either accept or reject cookies when entering a webpage or downloading an app. *See* Saniya Dhanjani, *Nudging Privacy: Design Interventions for 'Better' Privacy Decision-Making in Cookie Banners*, 17 ISCHANNEL 55, 55 (2022).

data."[185] These rights include "rights to notice, access, and consent regarding the collection, use, and disclosure of personal data" and aim to reorient the state of control so individuals can "weigh the costs and benefits of the collection, use, or disclosure of their information."[186] This interaction of the free market, default nudging, and freedom of contract has thus been recognized as a viable privacy solution, even inspiring policymakers in California, Europe, and the UK to adopt mandatory opt-in tracking as part of comprehensive privacy regulations—formally known as the California Consumer Privacy Act (CCPA),[187] General Data Protection Regulation (GDPR),[188] and ePrivacy Directives.[189] As a result, consent to data gathering through the form of opt-in tracking is now a market standard.[190]

While opt-in tracking is widespread and theoretically effective, there are two pitfalls. First, although legislation in Europe and California mandates the opt-in tracking model, implementation in the United States is largely voluntary because no state or federal law governs the substance of privacy policies.[191] As a result, Internet users in the United States often do not face "real" choices, because the options are often limited to either "pure withdrawal from specific services or the complete reliance on market

---

185 Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013).

186 *Id.*

187 CAL. CIV. CODE § 1798.100 (Deering 2023).

188 Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 [hereinafter GDPR].

189 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002 O.J. (L 201) 37, as amended by Directive 2006/24/EC [the Data Retention Directive], and Directive 2009/136/EC [hereinafter the Citizen's Rights Directive].

190 Dhanjani, *supra* note 184.

191 Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. ST. L. REV. 587, 597, 601–02 (2007) ("As applied to most commercial websites, the existing legislation requires that a privacy policy be posted, and that the entity abide by that policy, but does not regulate the substance of that policy. . . . State law too mandates online privacy policies without governing the substance of those policies.").

provided privacy protection."[192] The complete withdrawal from social networking sites can hardly be regarded as a neutral decision, despite being the reality of a user's denial of consent.[193] Second, even where opt-in tracking is implemented in the United States, "uninformed" consent functions to bar users from reasonable privacy protections.[194]

a. Informed vs. uninformed consent

In the online sphere, an individual's right to information privacy is supposedly implemented—but in actuality is thwarted—by the principle of informed consent.[195] The opt-in tracking nudge is commonly implemented through pop-up consent banners, and informed consent is obtained when a user selects *accept* or otherwise agrees to the terms displayed on the banner.[196] The idea that the choice to opt-in to tracking was "informed" is premised on the notion that privacy agreements provide notice to the consumer of their rights, that they are then free to disclaim.[197] This idealistic form of privacy self-management fails to consider the complexities that surround privacy decisions, as users "often face hurdles that limit individual decision-making," leading to "instances when privacy decision-making and behav[ior] do not align with privacy preference."[198] Within the context of consent banners, even minor user interface (UI) design decisions—such as the position of the notice, what is already highlighted when a user sees a notice, or the presence of pre-selected check boxes—all have significant impacts on how users interact with the cookie consent banners.[199] Further, studies have shown that the natural desire to resume browsing creates subconscious habitual behaviors, for instance, clicking interaction elements that "cause[] the notice

---

[192] Leyla Dogruel, *Privacy Nudges as Policy Interventions: Comparing US and German Media Users' Evaluation of Information Privacy Nudges*, 22 INFO., COMMC'N & SOC'Y 1080, 1082 (2019).

[193] *Id.*

[194] *See* discussion *infra* Section III.B.1.a.

[195] Dogruel, *supra* note 192, at 1082 (citing Solove, *supra* note 185).

[196] *Id.*; Dhanjani, *supra note* 184*, at 55.*

[197] *See* Dogruel, *supra* note 192, at 1082.

[198] Dhanjani, *supra* note 184, at 55–56.

[199] Christine Utz et al., *(Un)informed Consent: Studying GDPR Consent Notices in the Field*, ASS'N FOR COMPUTING MACH. 973, 985 (2019).

to go away instead of actively engaging with it."[200] Thus, in practice, the average consumer will agree to a provider's privacy policies without reading them.[201] These considerations help explain why users commonly opt-out of the no-tracking default, and why those opt-out decisions are, by and large, uninformed.[202]

The uninformed opt-out is a recognized phenomenon in many other contexts, and the issue typically arises when a regulatory default can easily be disclaimed by contract.[203] For example, "[e]very sales contract contains a default (implied) warranty, but they are massively disclaimed [by the] fine print."[204] As for information privacy, nearly every digital product is "subject to privacy rules that govern by default, but they are so often contracted around in the vendor's terms of service."[205] These examples illustrate why a consumer's freedom to contract away their rights works against any market default designed to protect those rights—the service provider ultimately controls the terms of service. This is particularly true in commercial contexts dominated by take-it-or-leave-it contractual exchanges, where the consumer has no real choice other than to accept the terms or be denied service.[206] In

---

[200] *Id.* at 974.

[201] *See generally* Nili Steinfeld, *"I Agree to the Terms and Conditions": (How) do Users Read Privacy Policies Online? An Eye-tracking Experiment*, 55 COMPUTS. HUM. BEHAV. 992 (2016) (noting that eye tracking methodology reveals that users often skip reading privacy policies, despite the widespread use of such policies in regulating the use of personal data collected by online service providers).

[202] *See, e.g.*, Swire, *supra* note 176, at 6 ("Not only are there imperfections in the ability of consumers to learn about and monitor a company's privacy policies. The problems are exacerbated by the costs of bargaining for the desired level of privacy. It is a daunting prospect for an individual consumer to imagine bargaining with a distant Internet marketing company or a huge telephone company about a desired privacy regime.").

[203] Oren Bar-Gill & Omri Ben-Shahar, *Rethinking* Nudge*: An Information-Costs Theory of Default Rules,* 88 U. CHI. L. REV. 531, 538 (2021).

[204] *Id.*

[205] *Id.*

[206] *See id.* at 574 ("[F]irms engineer mechanical costs to induce, rather than prevent, opt-out. These are situations in which consumers want to stick with the default, but firms make it artificially hard to do so. For example, consumers want to buy a standard product, but firms prompt them to select the (more profitable) premium version and nudge them to do so again

sum, Big Tech has a strong incentive to obtain user consent to tracking, and while opt-in tracking gives the illusion of a choice, many privacy agreements are offered on a take-it-or-leave-it basis, particularly those that include consent to tracking as part of a larger service agreement users must accept to register an account.[207]

b. Free market limitations

In order to understand the limitations of the free market for regulating privacy, it is important to first understand why any measure of privacy protection is voluntarily assumed by Big Tech in the first place. Data breaches, lawsuits, and scandals have given rise to a culture of consumer distrust and pitted Big Tech corporations against one another, clawing for the largest market share of users.[208] As a result, competition and the economic value of consumer goodwill have been the driving forces behind recent market-level growth in consumer privacy protection. However, there are demonstrable limitations, as the altruistic appearance of privacy measures have always been tainted by ulterior economic motives.

For example, in 2021, Apple updated its operating system to iOS 14.5, which introduced two significant privacy modifications: the implementation of App Tracking Transparency (ATT), a mandatory opt-in tracking system to be applied uniformly across all mobile applications; and "Privacy Nutrition Labels," a disclosure mandate for the type of data each app processes.[209] Switching to ATT yielded dramatic results. Once users were faced with a "simple, comprehensible choice" to opt-in to tracking and selling of their personal information, "only 15% of responding consumers in the

---

and again."); *see also* Sam Schechner, *Agree to Facebook's Terms or Don't Use It*, WALL ST. J. (May 11, 2018 5:31 AM), https://www.wsj.com/articles/stage-is-set-for-battle-over-data-privacy-in-europe-1526031104.

[207] Cadie Thompson, *What You Really Sign Up for when You Use Social Media*, CNBC (May 27, 2015, 12:18 PM), https://www.cnbc.com/2015/05/20/what-you-really-sign-up-for-when-you-use-social-media.html.

[208] Rahnama & Pentland, *supra* note 20 ("People are starting to vote with their thumbs: in the core North American market, both Facebook and Twitter are facing declines in their daily active users.").

[209] Konrad Kollnig et al., *Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels*, FACCT 2022 ACM CONF. 508, 508 (2022).

United States [granted] consent."[210] The implementation of ATT devastated the advertising industry's previously unrestrained trend of exponential growth: Meta announced an estimated loss of $10 billion in ad revenue following the iOS update.[211] Consequently, by implementing privacy directives aimed at transparency and consumer control, Apple was able to gain a competitive market advantage over its ad-dependent Big Tech counterparts.

Following in the wake of Apple's success, several Big Tech corporations vowed to phase out third-party cookies from their browsers and platforms.[212] Of course, there is a catch: the first-party ad businesses remain unaffected due to favorable terms in user privacy agreements.[213] As a result, the decision to phase out third-party tracking is unlikely to be philanthropic—first-party ad campaigns have proven to outperform third-party counterparts by large margins,[214] and the Big Tech members that are more dependent on ad revenue likely want to exploit those gains for themselves.[215] Thus, while the race to regain consumer confidence via opt-in privacy measures illustrates the "United States consumers' [indisputable] interest in protecting privacy," the limitations of these same market-level approaches illustrate the "palpable

---

[210] Chris Jones, *The iOS 14.5 Update: A Game Changer in Federal Privacy Law*, 28 RICH. J.L. & TECH. 254, 255 (2021).

[211] Daniel Newman, *Apple, Meta And The $10 Billion Impact of Privacy Changes*, FORBES (Feb. 10, 2022, 7:40 PM), https://www.forbes.com/sites/danielnewman/2022/02/10/apple-meta-and-the-ten-billion-dollar-impact-of-privacy-changes/?sh=475b089472ae.

[212] Google recently joined Apple and Mozilla (the makers of Safari and Firefox) in preventing third-party targeted digital advertising after a recent announcement that it would block third-party cookies on Chrome. *See* Damien Geradin & Dimitrios Katsifis, *Taking a Dive into Google's Chrome Cookie Ban*, Paper No. DP2020-042, TILBURG U. 1 (2020).

[213] *See id.* at 10.

[214] *See* Adform, *PwC Study Shows Marketers Can Achieve Value Today With First-Party IDs*, ADWEEK (June 22, 2022), https://www.adweek.com/adweek-wire/pwc-study-shows-marketers-can-achieve-value-today-with-first-party-ids/.

[215] *See* Yakira Young, *Ad Tech is Full of Surprises: Big Tech Wins First-Party Data Party; Utah Hops on Privacy Law Train; AI Ad Spend Rises*, ADMONSTERS (Apr. 19, 2022), https://www.admonsters.com/eletters/ad-tech-is-full-of-surprises/ ("Apple and Google's latest privacy crusades are less about consumer privacy, and likely more about simply growing their ad businesses.").

need for federal privacy regulation," or at the very least, an avenue for consumer redress.[216]

2. The Movement Towards Decentralized Internet: Web3

The free market has devised one more method of ameliorating Big Tech's data smorgasbord, and the proposed solution involves injecting new technology into the backbone of the Internet. Tech startups and investors aspire to "devolve [Big Tech's] control evenly across the entire [I]nternet, representing the transition to Web3."[217] Drawing inspiration from Berners-Lee's version of the Web in the 1990s (Web 1.0), the goal of Web3 is to create a new Web experience based on decentralized data ownership.[218] Because Big Tech relies on the current Web 2.0's centralized data interface, Web3 could potentially turn the industry on its head by displacing data ownership back into the hands of Internet users.[219] However, this solution too has limitations—the technologies and protocols that would underlie the interface still need to be developed.[220] Currently, Web3 is no more than an "emerging concept."[221] Despite this, the concept has proved to be feasible enough to garner Web3 startups over $7.1 billion in investments in 2022 alone.[222] The

---

[216] Jones, *supra* note 210, at 329.

[217] Gaurish Korpal & Drew Scott, *Decentralization and Web3 Technologies*, TECHRXIV 1, 1 (2022).

[218] Alex Pentland, *Building a New Economy: Data, AI, and Web3*, 65 COMMC'NS ACM 27, 29 (2022), https://dl.acm.org/doi/pdf/10.1145/3547659 ("When Web 1.0 and Web 2.0 were first developed, they were touted as decentralized systems that would empower marginalized communities. Unfortunately, these hopes faded as big commercial players developed platforms and interfaces that centralized data and AI. It is promising that the decentralization of data ownership and distributed AI provides ways to ensure decentralization of Web3, something that was not possible when Web 1.0 and 2.0 were deployed.").

[219] *Id.*

[220] Korpal & Scott, *supra* note 217. ("In order for [Web3] to be successful, technologies and protocols must be developed to enable web users to use the web securely without trusting any other user. That is, today's web is structured so that users must trust these companies, so trustless alternatives haven't already been developed.").

[221] Qin Wang et al., *Exploring Web3 from the View of Blockchain*, CORNELL U. 1, 24 (Jun. 17, 2022), https://arxiv.org/pdf/2206.08821.pdf.

[222] Valeria Goncharenko, *Metaverse Fundraising Report for 2022: Trends in NFT, Gaming, Infrastructure, AI*, METAVERSE POST (Jan. 01, 2023, 10:41 AM), https://mpost.io/metaverse-fundraising-report-for-2022-trends-in-nft-gaming-infrastructure-ai/.

sheer volume of investment and research and development (R&D) on Web3 as a technology solution that is capable of disrupting Big Tech's abuse of data privacy buttresses the public interest in stronger privacy protections, albeit through unconventional methods. But a technology solution, by itself, is also inadequate. Web3 is not a silver bullet that will eliminate privacy concerns. It is very uncertain whether Web3 is viable technically or that users will embrace the new technology and change their consumption habits.

## IV. THE PRAGMATIC SOLUTION—NUDGING TOWARDS PRIVACY VIA PRIVATE RIGHT OF ACTION

It is abundantly clear that the American public wants to be able to use the Internet and online services without being tracked and exploited by corporations that aren't looking out for consumers' privacy interests. The solutions discussed above have been implemented with only minor incremental improvements, and, although progress has been made, it is evident that these solutions do not fully address the problem. The missing key element is a uniform and reliable avenue for consumer redress. While sweeping privacy legislation such as the European Union's General Data Protection Regulation (GDPR) provides consumers with a direct claim under the statute,[223] such a comprehensive legislative framework is unlikely to be enacted in the United States. However, legislation is not necessary if an existing common law tort can be utilized to encompass these contemporary privacy claims.[224] Indeed, "[t]he common law is not static, but is a dynamic and growing thing and its rules arise from the application of reason to the

---

[223] In 2014, the EU passed the European General Data Protection Regulation (GDPR)—a sweeping privacy directive with the strongest pro-consumer format to date. *See* Jones, *supra* note 210, at 295. The GDPR's unprecedented strength in protecting privacy is derived from its unique mandatory opt-in tracking model and establishment of a private right of action. *See id.* The GDPR defines the type of tracking and information sharing that triggers the mandatory opt-in consent provision as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." *See* GDPR, *supra* note 188, art. 4(11) (defining consent). Importantly, "[s]ilence, pre-ticked boxes or inactivity" do not constitute consent, and concealing a consent clause in a lengthy privacy agreement is prohibited." *See id.* at 6 (enumerating a non-exhaustive list of practices that do not constitute consent).

[224] *See* discussion *infra* Section IV.A.

changing conditions of society."[225] The United States Supreme Court noted in *Hurtado v. California* that "[t]his flexibility and capacity for growth and adaptation is the peculiar boast and excellence of the common law,"[226] and this reasoning has been followed by a number of courts in recognizing a common law right to privacy tort.[227] Because the right to privacy suffers from a rapidly changing technology landscape, the right is well-suited to adapt through the common law. Further, a viable common law private right of action would add teeth to existing protections and eliminate plaintiffs' dependence on other unreliable modes of redress while legislatures shuffle their feet.

The proposed solution rests on the recognition of a pre-existing common law tort and its uniform application in the new context of Internet tracking disputes is derived from two fundamental assertions. The first assertion is that the judicial system currently does not have an adequate private right of action that effectuates the public policy of increased Internet privacy protection.[228] This assertion was established above in Part III.[229] The second assertion is that a private right of action has the outcome of effectuating public policy that would otherwise require a default regulatory scheme.[230] Both the default opt-in nudge and a private right of action have the effect of establishing a preference for certain rights that shifts the burden onto the more informed party to protect those rights.[231] However, while the uninformed opt-out phenomenon risks frustrating the purpose of the default

---

225 McCormack v. Okla. Publ'g Co., 613 P.2d 737, 740 (Okl. 1980).

226 Hurtado v. California, 110 U.S. 516, 530 (1884).

227 *See, e.g.*, Birnbaum v. United States, 436 F. Supp. 967, 978 (E.D.N.Y. 1977), *aff'd in part*, *rev'd in part*, 588 F.2d 319, 325 (2d Cir. 1978).

228 *See* discussion *supra* Section III.A.

229 *See* discussion *supra* Section III.A.

230 *See generally* ANTONIOS KARAMPATZOS, PRIVATE LAW, NUDGING AND BEHAVIOURAL ECONOMIC ANALYSIS: THE MANDATED-CHOICE MODEL 120–31 (2020) (arguing that a strict liability regime offers more products liability protection to consumers than market self-regulation involving a default choice scheme). "Even if there is no negligence [ . . . ] public policy demands that responsibility be fixed *wherever it will most effectively reduce the hazards* to life and health inherent in defective products that reach the market." *Id.* at 120 (alteration in original).

231 *See generally id.* at 123 ("The imposition of mandatory law protects the party suffering from such an information deficit: namely, the consumer.").

opt-in nudge, enforcing a private right of action does not share this pitfall.[232] In essence, a private right of action fills the void where regulatory nudging proves insufficient even though both have the same objective—protecting certain rights by default. Below, the second assertion will be illustrated by a historical analysis on the development of strict products liability, followed by the proposal for the expansion of common law intrusion upon seclusion that synthesizes consent factors from recent case law.

### *A. A Case Study on Strict Liability: Common Law Origins, Informational Asymmetry, and Strong Public Policy Converge to Create Redress for Consumers*

As discussed in Section III.B.1, uninformed consent is the primary problem associated with opt-in tracking.[233] This type of informational asymmetry has been the driving force behind the imposition of mandatory judicial-created law in other spheres of commerce—most notably, strict product liability.[234] Strict liability arose as a means of protecting a consumer from the informational superiority of manufacturers, which are in the best position to minimize the risk of harm to the public, even where there has been no negligence by the manufacturer.[235] As an alternative to mandatory law, scholars have instead suggested a market solution that involved nudging through the implementation of a "mandated-choice model."[236] This scheme would allow consumers to be presented with two choices: a product with liability assumption on the part of the manufacturer, or a cheaper product

---

[232] *See also id.* at 128 ("A fundamental pre-condition for such market self-regulation to take place is consumers' access to sufficient information . . . . if there is inadequate information or no information at all, the danger of a 'market for lemons' becomes imminent. And under a regime without mandatory product liability, more and more manufacturers will take advantage of consumers' information deficit and disseminate lower-quality, possibly unsafe, products at the same price, thus increasing their profit margin." (emphasis omitted)). *See generally id.* at 26 ("[W]hen an individual is not aware—or cannot be easily informed—of the default rule, that individual *does not make a decision* to delegate the decision-making authority to someone else or to accept a pre-determined default option.").

[233] *See* discussion *supra* Section III.B.1.a.

[234] KARAMPATZOS, *supra* note 230, at 120.

[235] *Id.*

[236] *Id.*

without liability assumption.[237] In the hypothetical transaction, the risk-preferring consumer would purchase the cheaper product, while the risk-averse consumer would self-insure by purchasing the slightly more expensive product that comes with added protection.[238] The problem with this type of market self-regulation rests on the idea that consumers would make uninformed choices, and, more often than not, blindly purchase the less safe product.[239] Manufacturers, exploiting their "informational superiority in conjunction with the absence of a liability rule, would have a strong incentive to not do all they could to make products safe in order to increase their profits; thus they would fuel the flow of defective (or less safe) products into the market."[240] Consequently, the ineffectiveness of market self-regulation combined with the public policy in favor of consumer protection gave birth to the judicial enforcement of strict liability on manufacturers.[241] In effect, a strict liability tort superseded the free choice market and works to protect consumers from making uninformed choices about product safety. This bolsters the idea that a private right of action is more effective than voluntary market regulation, particularly in areas where there are both informational asymmetry between the consumer and product provider and strong public policy to offer protection.[242]

It is important to note that strict liability had strong common law roots prior to its application to defective products. Historically, no showing of negligence by owners was necessary for a private right of action to arise in cases of damage caused by trespassing or dangerous animals.[243] Similarly, many early decisions recognized that sellers could be strictly liable to immediate purchasers, a limiting concept called "privity and fault" that

---

237 *Id.* at 121.

238 *Id.*

239 *See id.* at 122–23.

240 KARAMPATZOS, *supra* note 230, at 123.

241 *Id.* at 120–24.

242 *See generally id.*

243 *See* McPherson v. James, 69 Ill. App. 337, 339–40 (Ill. App. Ct. 1896) (holding owner of trespassing barnyard animals strictly liable for damages caused by the animals); *see also* Graham v. Payne, 24 N.E. 216, 217 (Ind. 1890) (stating that vicious animals with known dangerous propensities will impose strict liability on their owners).

remained intact until the twentieth Century.[244] Once the Industrial Revolution spawned a profusion of new ways to be careless, manufacturers were able to escape liability for a long time because they lacked "privity" with the downstream purchaser.[245] Strict liability was not immediately recognized as a solution because the liability imposed is that of an insurer, and the free market did not demand manufacturers to be insurers of their products.[246] However, once it became clear that the free market would be unable to reliably regulate products, the consuming public's interest in product safety justified a reexamination of the scope of the common law tort.[247] The judiciary's choice to extend strict liability to manufacturers was a turning point in the development of product liability law—one that "reflect[ed] the courts' recognition of the consequences which occur when the wheel turns from a basically rural culture to one that is machine-oriented."[248]

Similar circumstances are at play in the Internet privacy sphere. New technology ushered in cultural changes that led to new kinds of injuries; the free market is unable to regulate itself in a manner that provides consistent or reliable protection against these injuries; and settled law is unable to provide reliable recourse for injured plaintiffs. Applying the same rationale that led to strict product liability leads to the conclusion that the imposition of uniform law in the context of Internet privacy is appropriate given the informational asymmetry between Big Tech and its users[249] and given the public policy in favor of increased consumer privacy protections.

### *B. A Proposal to Expand Common Law Privacy Tort of Intrusion Upon Seclusion in the Context of Internet Privacy Protection*

Like strict liability, the common law privacy torts originated in a pre-Internet context and have lived within their respective limited confines for

---

[244] Edward C. German, *Products Liability—Strict Liability?*, 33 INS. COUNS. J. 259, 259 (1966).

[245] *See id.*

[246] *See* Francis J. O'Brien, *The History of Products Liability*, 62 TUL. L. REV. 313, 319 (1988).

[247] *See* Charles E. Cantu, *Distinguishing the Concept of Strict Liability in Tort from Strict Products Liability: Medusa Unveiled*, 33 U. MEM. L. REV. 823, 865–66 (2003).

[248] O'Brien, *supra* note 246, at 314.

[249] *See* discussion *supra* Section III.B.

over a century.[250] As discussed in Section II.C.1, the original four privacy torts (intrusion upon seclusion, public disclosure of private facts, false light, and misappropriation) were derived from Warren and Brandeis' general right to privacy, categorized by Prosser to suit different types of injuries.[251] Although the four torts share generalized "overlapping areas," the commonalities trace back to borrowed language from intrusion upon seclusion.[252] Juxtaposing intrusion upon seclusion with the other three torts reveals a tracing from generals to particulars: the other three torts were created to deal with special types of injuries, specifically those public or commercial in nature. Public disclosure of private facts focuses primarily on the "public disclosure" of information and provides a private right of action for persons whose private information is made public in a highly offensive manner.[253] Similarly, false light focuses on the publicity of false information.[254] Misappropriation focuses primarily on the "commercial nature" and abuse of information and provides redress for persons whose name and likeness are exploited for commercial gain without prior consent.[255] Because these three torts are carefully designed for specialized injuries, general privacy grievances, such as those that may be unanticipated, would not be suited to these common law actions.

Unique to intrusion upon seclusion is the fact that the tort is not concerned with "the manner in which the [private] information was disclosed, but the *manner in which the information was collected*."[256] This understanding comes within the purview of the Supreme Court's interpretation of the right to privacy as encompassing "the individual's control of information concerning his or her person."[257] This focus on the

---

250 *See* discussion *supra* Section II.C.1.

251 *See* discussion *supra* Section II.C.1.

252 Keck, *supra* note 77, at 107 (noting that public disclosure of private facts borrows elements from intrusion). "The overlapping areas of these three torts, then, involve the offensive nature of the intrusion or disclosure, whether there is a legitimate reason for the disclosure, and whether the information is of a private nature." *Id.*

253 *Id.* at 107.

254 RESTATEMENT (SECOND) OF TORTS § 652E (AM. LAW INST. 1965).

255 Keck, *supra* note 77, at 106.

256 *Id.* (emphasis added); *see also* Doe v. Mills, 536 N.W.2d 824, 832 (Mich. Ct. App. 1995).

257 U.S. Dep't of Just. v. Reps. Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

manner in which information was collected makes intrusion upon seclusion the ideal candidate for expansion into technology-precipitated privacy violations.

1. Common Law Intrusion Upon Seclusion

Generally, state legislatures and judiciaries adopt the common law to the extent it is not inconsistent with statutory law.[258] This practice is particularly relevant in the law of torts, which substantively remains a creature of state common law.[259] Given the widespread lack of statutory law regarding Internet privacy protections, intrusion upon seclusion is recognized as a common law tort in the vast majority of states, and courts typically defer to the Restatement (Second) approach when analyzing state law claims for intrusion.[260] Restatement (Second) of Torts § 652B, titled "Intrusion Upon Seclusion," states: "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[261] Thus, a claim for intrusion upon seclusion has two elements: (1) the defendant must "'intentionally intrude[] into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy[,]' and (2) the intrusion [must] 'occur[] in a manner highly offensive to a reasonable person.'"[262]

---

[258] Anita S. Krishnakumar, *The Common Law as Statutory Backdrop*, 136 HARV. L. REV. 608, 610 (2022) ("[T]he common law has played an underappreciated, often dispositive, gap-filling role in statutory interpretation for decades . . . .").

[259] Mark A. Geistfeld, *Hidden in Plain Sight: The Normative Source of Modern Tort Law*, 91 N.Y.U. L. REV. 1517, 1527 ("The modern tort system did not fully develop until the writ system was eliminated in the latter half of the nineteenth century . . . During this period, torts developed into one of the recognized substantive fields of the common law.").

[260] *See generally* Eli A. Meltz, Note, *No Harm, No Foul? "Attempted" Invasion of Privacy and the Tort of Intrusion Upon Seclusion*, 83 FORDHAM L. REV. 3431, 3440–43 (2015) (surveying the states that have adopted the Restatement's approach to this tort as well as those that have recognized this tort under common law).

[261] RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1965).

[262] *See, e.g.*, Davis v. Facebook, Inc., 956 F.3d 589, 601 (9th Cir. 2020) (second alteration in original) (listing these as the elements for common law intrusion upon seclusion under California law).

Central to a successful claim of intrusion upon seclusion is the existence of a plaintiff's reasonable expectation of privacy and acts consistent with his or her expectation of privacy.[263] Whether a plaintiff has a reasonable expectation of privacy is a difficult inquiry, because not only must the plaintiff prove the defendant "penetrated some zone of physical or sensory privacy surrounding, or obtained unwanted access to data about, the plaintiff," the plaintiff must further establish they possessed an "objectively reasonable expectation of seclusion or solitude in the place, conversation or data source."[264] Similar to the struggles faced by Fourth Amendment jurisprudence,[265] what constitutes a reasonable expectation of privacy under an intrusion claim is highly variable depending on the jurisdiction. Some courts mimic *Olmstead*'s trespass doctrine in the assessment of actionable intrusions and impose a physical intrusion requirement.[266] Conversely, other courts take a more flexible approach and recognize that intrusions can occur without a physical trespass.[267] One court reflected *Katz*'s emphasis on society at large in determining whether expectations are reasonable:

> [P]rivacy for purposes of the intrusion tort, is not a binary, all-or-nothing characteristic. There are degrees and nuances to societal recognition of our expectations of privacy: the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law.[268]

This framework for intrusion upon seclusion, however, is not unlimited. Clearly, society must tolerate some intrusions to remain a functioning society. The Restatement of Torts elaborates on this limiting principle in a comment: "[c]omplete privacy does not exist in this world except in a desert,

---

263 3 BUSINESS TORTS § 33.02 (Frances P. Hayes ed., 2022).

264 Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 490 (Cal. 1998).

265 *See* discussion *supra* Section II.C.2.

266 *See* Cmty. Health Network, Inc. v. McKenzie, 150 N.E.3d 1026, 1045 (Ind. Ct. App. 2020), *rev'd on other grounds*, Cmty. Health Network v. McKenzie, 185 N.E.3d 368 (Ind. 2022); Creel v. I.C.E. & Assocs., 771 N.E.2d 1276, 1280 (Ind. Ct. App. 2002).

267 *See* Jackman v. Cebrink-Swartz, 334 So. 3d 653, 657 (Fla. Dist. Ct. App. 2021); Anderson v. Mergenhagen, 642 S.E.2d 105, 110 (Ga. Ct. App. 2007).

268 Sanders v. Am. Broad. Cos., 978 P.2d 67, 72 (Cal. 1999).

and anyone who is not a hermit must expect and endure the ordinary incidents of the community life of which he is a part."[269] The requirement that an intrusion be highly offensive ameliorates the concern of tolerable intrusions becoming an actionable injury. To determine whether an intrusion is highly offensive, courts evaluate the following factors: "(1) the degree of intrusion; (2) the context, conduct and circumstances surrounding the intrusion; (3) the intruder's motives and objectives; (4) the setting into which the intrusion occurs; and (5) the expectations of those whose privacy is invaded."[270] These factors reinforce the idea that privacy is highly context-dependent, a recurring theme in privacy law.

As it stands, the varied interpretation of the first element—a plaintiff's reasonable expectation of privacy—would lead to inconsistent results for plaintiffs depending on the nature of the intrusion. For Internet privacy disputes, the potential for varied outcomes would render intrusion upon seclusion as equally problematic as the more commonly asserted Wiretap claims.[271] However, while the outdated federal statutes discussed in Section III.A are limited in scope, the evolution of Warren and Brandeis' right to privacy and strict liability law demonstrates the malleability of common law and its ability to adapt to new contexts. Thus, intrusion upon seclusion remains a viable contender for the particular injuries faced in Internet tracking disputes and leaves the door open for any future unforeseen Internet privacy violations. The effectiveness of intrusion upon seclusion for providing consumer redress, however, will hinge on the uniformity under which it can prospectively be applied. This creates a need for expanding intrusion upon seclusion—more specifically, for calculating uniform factors to aid in the reasonable expectation of privacy analysis. Accordingly, in proposing to expand intrusion upon seclusion to new contexts, it is necessary to engage in thoughtful analysis about society's fluctuating standards and leverage precedent to help redefine the outer limits of behavior that constitutes an invasion of privacy.

---

[269] RESTATEMENT (SECOND) OF TORTS § 652D cmt. c (AM. LAW INST. 1977).

[270] *See* Mezger v. Bick, 280 Cal. Rptr. 3d 720, 728 (Cal. Ct. App. 2021) (quoting Sanchez-Scott v. Alza Pharms., 103 Cal. Rptr. 2d 410, 419 (Cal. Ct. App. 2001)).

[271] *See* discussion *supra* Section III.A.1.

### 2. Application of Intrusion Upon Seclusion to the Internet: Outer Boundaries

The application of intrusion upon seclusion to new contexts has resulted in issues of first impression.[272] While it is evident that technology is a catalyst for privacy violations, at the center of actionable illicit access is a lack of consent. Consent banners and privacy agreements provide functional hurdles for the application of intrusion upon seclusion in Internet tracking disputes, because the general consensus is that the collection of cookies, without more, does not result in the commission of a privacy tort.[273] In order to overcome these hurdles, it is necessary to propose a shift away from the common law perspective of consent as outcome-determinative. Instead, courts should analyze consent in light of the social-normative construct under which information is shared.[274] Professor Nissenbaum coins this approach as "privacy as contextual integrity," and identifies several factors known to affect the contextual norms and flow of information: free choice, discretion, and confidentiality affect the nature by which information is shared.[275] Using Nissenbaum's multi-factor analysis as a starting point for intrusion claims, plaintiffs in tracking disputes could circumvent prior consent to tracking by establishing common exigent circumstances: no free choice (take-it-or-leave-it privacy agreements), the otherwise unavailability of discretion (misleading advertising or inducement to obtain consent), or confidentiality was breached (data breach). Several modern cases that have addressed intrusion upon seclusion in the Internet tracking context have developed rules establishing similar exigent circumstances, thereby allowing the plaintiff's claim for intrusion upon seclusion to proceed. From these

---

[272] *See* Howard v. Aspen Way Enters., 406 P.3d 1271 (Wyo. 2017) (application of intrusion upon seclusion to invasive computer software installed by lessor without lessee's consent); *see also* Ringelberg v. Vanguard Integrity Pros.-Nev., Inc., 2018 U.S. Dist. LEXIS 203835 (D. Nev. Dec. 3, 2018) (application of intrusion upon seclusion to unlawful surveillance via GPS monitoring).

[273] *See* Bose v. Interclick, Inc., 2011 U.S. Dist. LEXIS 93663, at *15 (S.D.N.Y. Aug. 17, 2011); LaCourt v. Specific Media, Inc., 2011 U.S. Dist. LEXIS 50543, at *12 (C.D. Cal. Apr. 28, 2011).

[274] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 119, 138 (2004).

[275] *Id.* at 142.

cases, this Comment will propose a synthesized multi-factor rule in Section IV.B.3.

a. *In re Google Inc.*[276]

In *In re Google*, the Third Circuit found that Google's backdoor around browsers with activated cookie-blockers "implicated a protected privacy interest."[277] The scope of the plaintiffs' reasonable expectation of privacy was determined by whether the alleged misconduct was "in violation of the law or [other] social norms."[278] Critically, the court found that "a user would also reasonably expect that her activated cookie blocker meant her URL queries would not be associated with each other due to cookies."[279] The court held that the activated cookie blocker equated to "an express, clearly communicated denial of consent," and as such, the installation of cookies violated the plaintiffs' reasonable expectation of privacy.[280] As to whether the intrusion was highly offensive, Google's public assurances that they did not circumvent cookie blockers proved to be fatal. In finding an egregious breach of social norms, the court stated: "[w]hether or not data-based targeting is the [I]nternet's pole star, users are entitled to deny consent, and they are entitled to rely on the public promises of the companies they deal with."[281] *In re Google* thus stands for the propositions that (1) an express denial of consent constitutes a violation of a person's reasonable expectation of privacy, (2) providing consent would likely be fatal to a plaintiff's intrusion claim, and (3) something more than a denial of consent is necessary for an intrusion to be highly offensive.

b. *In re Nickelodeon Consumer Privacy Litigation*[282]

In *In re Nickelodeon*, the court held that Viacom artificially created and then subsequently violated the children plaintiffs' reasonable expectation of

---

276 *In re* Google Inc., 806 F.3d 125 (3d Cir. 2015).

277 *Id.* at 151.

278 *Id.* (quoting Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1072 (Cal. 2009)).

279 *Id.*

280 *Id.*

281 *Id.*

282 *In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262 (3d Cir. 2016).

privacy by tracking the children's online activities after displaying a message on their website that read: "HEY GROWN-UPS: We don't collect ANY personal information about your kids."[283] Importantly, as opposed to *In re Google*, no showing of a denial of consent was necessary. The court stated "the wrong at the heart of the plaintiffs' intrusion claim is not that Viacom and Google *collected* children's personal information, or even that they *disclosed* it. Rather, it is that Viacom created an expectation of privacy on its websites and then obtained the plaintiffs' personal information under false pretenses."[284] *In re Nickelodeon* thus stands for the propositions that (1) claims made in targeted advertising claims designed to induce customers to provide their information can artificially create a plaintiff's reasonable expectation of privacy, and (2) behavior that goes directly against these claims is sufficient to violate a plaintiff's reasonable expectation of privacy in a manner that is highly offensive.

c. *In re Facebook Inc. Internet Tracking Litigation*[285]

In *In re Facebook*, the court held that Facebook's failure to acknowledge its tracking of logged-out users in privacy disclosures created an *implicit* expectation that logged-out users would not be tracked.[286] Facebook's Statement of Rights and Responsibilities read: "We designed our Privacy Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Privacy Policy, and to *use it to make informed decisions*."[287] Meanwhile, Facebook's relevant data use policy stated: "We receive data whenever you visit a game, application, or website that uses [Facebook's services]. This may include the date and time you visit the site; the web address, or URL, you're on . . . and, *if you are logged in to Facebook*, your user ID."[288] The court reasoned that Facebook's promise to "make important privacy disclosures" coupled with the type of disclosures

---

283 *Id.* at 291.

284 *Id.* at 292.

285 Davis v. Facebook, Inc., 956 F.3d 589 (9th Cir. 2020).

286 *Id.* at 602.

287 *Id.* (emphasis added).

288 *Id.* (first alteration in original).

that were made would have led a plaintiff to conclude that Facebook would not engage in tracking behaviors that were not enumerated.[289] Because the opinion was written in response to a Rule 12(b)(6) motion to dismiss, the court regarded the highly offensive element as "an issue that [could not] be resolved at the pleading stage," and did not address the merits.[290] The court did however state that "the highly offensive analysis focuses on the degree to which the intrusion is unacceptable as a matter of public policy."[291] *In re Facebook* thus stands for the propositions that (1) the common practice of maintaining privacy disclosures can implicitly create a reasonable expectation of disclosure and (2) acts inconsistent with disclosures may be a violation of a user's reasonable expectation of privacy.

3. A Synthesized Rule: Consent Factors

In light of these cases, it is evident that informed consent is at the center of a user's reasonable expectation of privacy. Moreover, it is clear that consent is not limited to the traditional market practice of accepting the terms of privacy agreements in exchange for service. The court in *In re Google* found that the installation of cookie blockers was an express denial of consent.[292] The court in *In re Nickelodeon* found misleading advertising practices prevented consumers from giving consent.[293] The court in *In re Facebook* was able to use the company's disclosure statements against them, suggesting that consent was only offered to the extent that it was informed, i.e. for the practices disclosed.[294] From these holdings, one can derive a sliding scale test for where and when consent may implicate a reasonable expectation of privacy. Accordingly, a proposed framework for determining whether a plaintiff had a reasonable expectation of privacy in cookies disputes involves the consideration of three factors: (1) whether the consent was improperly obtained, such as by misleading advertising or otherwise deceitful public

---

289 *Id.*

290 *Id.* at 606.

291 Davis v. Facebook, Inc., 956 F.3d 589, 606 (9th Cir. 2020) (citing Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1073 (Cal. 2009)).

292 *In re* Google Inc., 806 F.3d 125, 151 (3d Cir. 2015).

293 *In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 292 (3d Cir. 2016).

294 *Davis*, 956 F.3d at 602.

assurances; (2) whether the scope of consent was exceeded, either expressly or impliedly by conduct that falls outside of disclosure statements; and (3) whether consent was expressly denied, such as by any manifestation of the consumer that could reasonably be interpreted to be a denial of consent.

These factors can further illuminate whether a defendant's conduct is highly offensive. If consent is improperly obtained or expressly denied and circumvented, then such conduct can be characterized as a clear departure from accepted social norms and will therefore be highly offensive. For cases involving exceeded consent, the issue of whether a defendant has exceeded consent will result in a factual inquiry and must take into account "the degree to which the intrusion is unacceptable as a matter of public policy."[295] Thus, the proposed consent scale factors would allow courts to establish varied degrees of abuse of consent—the crux of a social norm violation that underpins the "highly offensive" analysis.[296]

Importantly, the proposed consent factors utilize a *presumption* of privacy, which can be voluntarily waived by providing consent. The factors capture the necessity for context-based consent analysis and broaden the protection afforded by opt-in consent practices by establishing exceptions to the general rule that consent is a *per se* bar to recovery. Under the proposed test, the act of granting consent does not automatically invalidate a plaintiff's reasonable expectation of privacy. The factors enumerate exigent circumstances under which consent can be voided due to misconduct by the defendant. This framework places an important check on data abusers, as user consent would no longer be a bright-line excuse for privacy violations. Consequently, the incorporation of the proposed consent factors would aid courts in evaluating intrusion upon seclusion claims in Internet privacy cases. These factors establish clear outer boundaries for the tort's scope, deter companies from employing deceptive practices, and promote extensive disclosure, enabling users to make informed decisions.

4. Applying the Consent Factors

The reasonable expectation of privacy element was fatal to the plaintiffs' claims for intrusion upon seclusion in *Busse v. Motorola, Inc.* and *Dwyer v.*

---

295 *Id.* at 606 (citing *Hernandez*, 211 P.3d at 1073).

296 *In re Google*, 806 F.3d at 151.

*American Express, Co.*[297] Due to this, the consent factors will be applied to the set of facts in both cases to demonstrate the proposed rule's functionality.

In *Busse*, cellphone service providers supplied customer data to a third-party research firm for use in a company-funded study investigating a potential link between wireless telephone use and mortality.[298] The data included the customers' "names, street addresses, . . . dates of birth, social security numbers, wireless phone numbers, account numbers, start-of-service dates[,] and the electronic serial numbers of the customers' phones."[299] The customers alleged intrusion upon seclusion, arguing that the service providers failed to provide notice or obtain consent for third-party use of their personal information.[300] The court held that no tortious intrusion occurred, i.e. the plaintiffs did not have a reasonable expectation of privacy in their information, because the information involved "[m]atters of public record" as opposed to "private facts."[301]

Applying the proposed consent factors to the facts of *Busse*, the plaintiffs' lack of consent or notice to third-party use could establish a reasonable expectation that their personal information would not be shared. This argument could take two forms. First, the plaintiffs could assert that they only provided personal information to effectuate their service contracts and that use of their information would be limited to matters ordinarily incidental to performing obligations under the service contract. Under the second consent factor—whether the scope of consent was exceeded—a court would likely determine that third-party use of the plaintiffs' information for a study entirely unrelated to the service contracts was a clear violation of the plaintiffs' consent and, therefore, an actionable intrusion. Alternatively, the plaintiffs could argue that the lack of notice of the third-party use amounted

---

297 *See generally* Busse v. Motorola, Inc., 813 N.E.2d 1013 (Ill. App. Ct. 2004) (holding that third-party disclosure of social security numbers, names, addresses, and the particulars of customers' cell phone use was not an invasion of privacy); Dwyer v. Am. Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995) (holding that there was no intrusion where credit card holders voluntarily provided financial information and where individualized financial information was not shared with third parties).

298 *Busse*, 813 N.E.2d at 1015.

299 *Id.*

300 *Id.* at 1016.

301 *Id.* at 1017–18.

to an express denial of consent as to that particular use. Under the third consent factor—whether consent was expressly denied—the actions by the defendant would similarly constitute an actionable intrusion. These outcomes illustrate an important shift from the *Busse* court's analysis—it matters not whether the information itself could be classified as private or public, but rather whether the plaintiffs *consented* to the dissemination of their information.

In *Dwyer*, plaintiffs asserted intrusion upon seclusion in a class action lawsuit against American Express based on the company's practice of renting information regarding cardholder spending habits.[302] American Express would "categorize and rank their cardholders into six tiers based on spending habits and then rent this information to participating merchants as part of a targeted joint-marketing and sales program."[303] The court held that the acts of compiling information voluntarily given and subsequently renting its compilation were not actionable intrusion.[304] While not explicitly stated, in finding no actionable intrusion, the court implied that because the plaintiffs voluntarily provided information as part of their service, the plaintiffs did not have a reasonable expectation of privacy in the information they voluntarily disclosed.[305]

Applying the proposed consent factors to the facts of *Dwyer* would reveal that the plaintiffs did have a reasonable expectation of privacy in the information disclosed to American Express, despite voluntarily providing it as a part of their service. The rationale is similar to the application of the rule to *Busse*—the scope of consent remains an important function of where privacy begins and ends. In both *Busse* and *Dwyer*, the plaintiffs provided

---

302 Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1352–53 (Ill. App. Ct. 1995).

303 *Id.* at 1353.

304 *Id.* at 1354.

305 This is implied because the court did not explicitly follow the Restatement approach for intrusion, so no reasonable expectation of privacy language was discussed. *See id.* at 1353. However, the elements are substantially similar, and the element that failed in this case was an "unauthorized intrusion or prying into the plaintiff's seclusion." *Id.* at 1354. This language functionally mimics the first common law element requiring an intentional intrusion into "a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy." *See, e.g.*, Davis v. Facebook, Inc., 956 F.3d 589, 601 (9th Cir. 2020).

information pursuant to their service agreements.[306] Compared to *Busse*, where the data was being repurposed for non-commercial use,[307] *Dwyer* presents an even more compelling case of intrusion because sensitive financial information was aggregated and *sold* to third parties for purposes outside the scope of the plaintiff's financial services.[308] Plaintiffs could once again assert that they had a reasonable expectation of privacy in their personal information as confined to its consented use. This would trigger an analysis using the second consent factor—whether the scope of consent was exceeded. A court would likely find that disclosure of the plaintiffs' information was limited to internal use relating to the operation of the plaintiffs' financial accounts. And to the extent that the companies repurposed the plaintiffs' information for uses beyond this scope, the companies violated the plaintiffs' reasonable expectation of privacy.

*Busse* and *Dwyer* reflect a common law adherence to the categorization of information as either "wholly private or wholly public."[309] This paradigm results in courts adopting a "binary view of privacy—some bit of information is either public or private."[310] This ideology is directly in contrast with the underlying purpose served by the common law right to privacy: providing recourse for unprecedented intrusions in an evolving society. By nature, the evolution of societal standards means the right to privacy is in flux—"in reality information is only rarely entirely public or private in the modern age; context matters."[311] Consequently, a strictly binary approach would unreasonably limit the scope of privacy intrusions. The proposed consent factors ameliorate this common law limitation by adding a context-based inquiry for consent analysis while still defining the outer boundaries of an actionable injury.

---

306 *See generally Busse*, 813 N.E.2d 1013; *Dwyer*, 652 N.E.2d 1351.

307 *Busse*, 813 N.E.2d at 1015.

308 *Dwyer*, 652 N.E.2d at 1353.

309 DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 143 (2004).

310 Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 330 (2013).

311 *Id.*

Finally, it is important to note that neither of the above examples involved the misappropriation of third-party cookies and that, instead, concerned first-party data the defendants collected and repurposed for personal or third-party use. This highlights the proposed consent factors' applicability to a wide range of contexts beyond merely third-party tracking disputes, an important flexibility given the fact that Big Tech has been slowly shifting away from third-party data in favor of first-party advertising methods (a concern expressed in Section III.B.2.b).

## VI. CONCLUSION

Just as the Industrial Age ultimately led to protections for consumers who were vulnerable to the excesses of industry, the new Digital Age must offer protections to society from predatory invasions of privacy. The time has come once again for the common law to grow and meet the demands of a new age. Courts should look to uniformly expand intrusion upon seclusion to encompass Internet privacy disputes. Ultimately, the framework proposed by this Comment emphasizes the importance of consent as the linchpin of privacy violations. As illustrated by the application of the proposed consent factors to fact patterns distinguishable from third-party cookies disputes, the shift in focus to a context inquiry surrounding consent as part of the reasonable expectation of privacy analysis works well in a variety of contexts that implicate information privacy. By broadening the scope of intrusion upon seclusion to encompass Internet privacy violations while preserving its applicability to established contexts, this approach seeks to reset the balance and ensure that user privacy remains a paramount concern in the digital age. In an era defined by the continuous evolution of technology, it is crucial to adapt and strengthen legal protections to safeguard individual privacy and uphold the principles upon which the Internet was originally conceived. This will not only provide privacy protections that are overwhelmingly demanded by a connected society but will create guardrails in the digital economy while still allowing innovation and commerce to flourish, serving both the interests of industry and the common good of society.