Northwestern Journal of Technology and Intellectual Property

Volume 21 | Issue 1 Article 1

11-2023

The Right to Data Privacy: Revisiting Warren & Brandeis

Anthony G. Volini

NORTHWESTERN
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

THE RIGHT TO DATA PRIVACY: REVISITING WARREN & BRANDEIS

Anthony G. Volini

November 2023 VOL. 21, NO. 1

Volume 21, Number 1 (2023)
Northwestern Journal of Technology and Intellectual Property

THE RIGHT TO DATA PRIVACY: REVISITING WARREN & BRANDEIS

Anthony G. Volini[*]

ABSTRACT—In their famous 1890 article *The Right to Privacy,*[1] Samuel Warren and Louis Brandeis found privacy as an implicit right within existing law. Regarded as perhaps the most influential legal essay of all time,[2] it offers concepts that ring as true today as they did in 1890. In defining privacy as an important legal principle implicit in the law, they focused on information privacy, such as public disclosure of personal information, rather than decisional privacy. Analyzing the 1890 article is an ideal starting point to assess the origins of privacy law and to understand privacy issues from a simpler time in terms of law and technology. Its concepts thus provide an easily understandable frame of reference before diving into more challenging modern issues and assessing a path forward.

Accordingly, this article compares each key principle from 1890 and explores privacy issues that remain similar versus privacy issues that seem new based on particular advances in technology. The key similarity between 1890 and today is that problems of information dissemination present similar issues, albeit on a larger scale. Some key differences between 1890 and today, however, are that computer technologies now allow for massive data collection, massive data retention and increasingly aggressive data analysis that can be used to abuse privacy even with ostensibly public data. Warren and Brandeis taught us that new technologies continually present new privacy issues; so as new technologies are evolving today, thought must still be given to how the law might flexibly adapt to new and unforeseen changes in tech. Their article

[*] Professor of Legal Practice at DePaul University College of Law, Registered Patent Attorney, M.S. Cybersecurity (Networking & Infrastructure Conc.), (Certified Information Privacy Professional/United States (CIPP/US), CIPP/Europe (CIPP/E), Cybersecurity Fundamentals Certificate (CSXF). With many thanks to Professor Charlotte Tschider, Colin Black, Esq., Brett Davinger, Esq. and Matthew Messina (3L) for helpful research and insights.

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

[2] Jeffrey Bellin, *Pure Privacy*, 116 NW. U. L. REV. 463, 469 (2021) (*citing* Harry Kalven Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROBS. 326, 327 (1966)).

exposed that various U.S. laws were insufficient in 1890 to broadly protect information privacy, causing Warren and Brandeis to imply a broad right.

Today, the same problem persists: laws within the U.S. are inadequate to address privacy harms caused by continually evolving technologies. The U.S. still has no broad express privacy law, and a path forward might contemplate making express what Warren and Brandeis had to imply in order to address new privacy harms. I propose two key ideas. First, the law needs to more clearly distinguish decisional privacy from information privacy. Decisional privacy is really not a privacy interest at all and is instead a personal liberty interest separate from information privacy. Second, when contemplating legal protection for information privacy, perhaps it's time to consider the arduous and improbable task of enacting a constitutional amendment guaranteeing broad and general protection against *information* privacy abuse from both government and private actors. While difficult to enact, a broad express federal right could provide significant advantages, such as (1) establish a baseline right from which states and Congress could add consistent legislation; (2) enable courts to restrict clear instances of privacy abuse without waiting for Congress to act, which seems especially helpful given the expected proliferation of artificial intelligence ("AI") and new and unforeseen privacy harms; (3) increase harmonization with the European Union ("E.U.") and potentially other jurisdictions; (4) and finally, avoid the problem of originalist or strict constructionist judges refusing to infer or imply a constitutional information privacy right in the wake of the Supreme Court's *Dobbs v. Jackson Women's Health Organization,* 597 U.S. __ (2022)*,* decision. Thus, a flexible and general broad right of federal protection from information privacy abuse might provide an optimal, flexible baseline for courts and regulators to quickly restrict new privacy abuses while allowing time for the states and Congress to enact further detailed legislation.

I. BACKGROUND.

An overarching similarity between 1890 and today is the struggles of the U.S. legal system to adapt to massive technological advances. This challenge is perhaps best expressed by the character Olaf in Disney's 2019 Frozen 2 movie in which he offers his theory about advancing technology as being both our savior and our doom.[3] Essentially, advances in technology can offer both tremendous benefits and harms to humankind. The advancement of information delivery technologies, much like the splitting of the atom, can be used for helpful or harmful purposes. So, the law must evolve to reasonably enable commerce and innovation, as well as reasonable criminal discovery, while mitigating privacy abuses.

A. Liberty & Privacy

Regarding modern privacy, it's important to distinguish decisional privacy from information privacy and to realize that decisional privacy is arguably a misnomer. Decisional privacy essentially involves private decision-making, such as choice of marital partner, choices concerning contraception/abortion,[4] etc. In contrast, information privacy typically concerns the abuse of personal information via surveillance, including online surveillance of location, messages, purchasing history, etc., which governments could then use to restrict personal liberties.

It's important to understand the relationship between decisional privacy and information privacy because a government can't restrict decisional privacy without some form of surveillance (i.e., discoverable evidence). For example, if an out-of-state abortion is illegal in a defendant's home state, the home state must first detect it with some form of surveillance like location tracking or accessing financial or medical records. The connection between decisional privacy and information privacy is perhaps partly responsible for blurring the lines between these

[3] For this and other noteworthy Olaf quotes *see* https://www.imdb.com/title/tt4520988/quotes/ [https://perma.cc/W6AD-NRYR].For a discussion of regulation of new technologies, including assessments of harms and benefits brought by new technologies, see Lydia Lichlyter, *Encryption, Guns, and Paper Shredders: Analogical Reasoning with Physically Dangerous Technologies*, 31 HARV. J.L. & TECH. 259, 263 ("For any dangerous technology, the reason not to simply ban it outright is that it has benefits of some kind, when used in non-harmful ways.").

[4] Granted, abortion and contraception decisions may be kept private, such as where a woman chooses not to publicize an early stage pregnancy.

two rights. But, as Professor Jeffrey Bellin notes, the blurring of the lines between these two rights has been significantly influenced by courts inappropriately characterizing decisional freedom as a privacy interest rather than a liberty interest, causing various personal liberties issues to be placed perhaps erroneously within a large umbrella called privacy law; as Professor Bellin astutely states, when "privacy means everything, it means nothing."[5] He asserts that decisional privacy might not be a privacy interest at all: instead, it is better described as a personal liberty interest.[6] I agree: decisional privacy seems like just another term for liberty. I thus argue that privacy rights should generally return to the information privacy focus described by Warren and Brandeis in 1890. I further encourage courts and legal scholars to acknowledge "liberty" as a genus term and various other rights as species of the broader liberty right. Accordingly, a right to privacy and rights to various personal decisions should be viewed as distinct components of liberty. A free society should therefore embrace both strong privacy rights and decisional rights in order to be characterized as free.

Professor Bellin explained that the Supreme Court avoided referring to private decisions as a liberty right because it wanted to avoid the unpopular reasoning in *Lochner v. New York*, 198 U.S. 45, 56 (1905), a case invalidating a state law that limited bakery employee hours because the law violated "the right of the individual to his personal liberty." He describes that subsequent cases referring to *privacy* rather than *liberty* were essentially an effort to "exorcize the ghost of Lochner."[7]

So why didn't the Justices use "personal liberty" to describe a right against unwarranted government interference in peoples' lives? Because an earlier set of Justices poisoned the phrase. As one critic writing in 1975 framed the problem: "Terrified by history to talk openly in terms of substantive liberty rights under the Fourteenth Amendment, the Justices talked instead in fragile and convoluted reasoning of privacy rights swirling around in ectoplasmic emanations."[8]

With this legal history of the term liberty in mind, perhaps it's time to consider the ghost of *Lochner* sufficiently exorcized and embrace the concept of liberty as encompassing both information privacy and personal decisional liberty. To understand liberty, one should recognize that an authoritarian regime typically has both excessive restrictions on personal

---

[5] *See* Bellin, *supra* note 2, at 471.

[6] *Id.*

[7] *See* Bellin, *supra* note 2, at 479 (describing how Justice Douglas coined the term "ghost of Lochner" in a 1958 opinion).

[8] *See id.* at 478 (*citing* Graham Hughes, *The Conscience of the Courts* 72 (1975)).

liberties as well as highly intrusive surveillance. In contrast, a free society might be perceived as one that has only minimal or reasonable restrictions on personal liberties and also does not overreach with respect to surveillance. Thus, courts are essentially tasked with an implicit but overarching question of what is appropriate for life in a free society with regard to privacy and surveillance rights as well as any other rights that might be at issue, such as the right to travel, right to free speech, right to assembly, etc. The concern, however, is that some judges may be less willing than Warren and Brandeis to imply information privacy rights, despite the apparent importance of information privacy in a free society.

B. The Continuing Need for a Broad Federal Privacy Law

In 1890, Warren and Brandeis observed that the law had no broad express right to privacy, so they implied the right. The same is generally true today; while various specific privacy statutes have emerged, there is still no express broadly defined right. As discussed in greater detail in Part III, there is a continuing need for a broad federal privacy law given concerns over AI and the recent *Dobbs* decision, evincing possible judicial reluctance to imply a broad information privacy right.

The Supreme Court refused to imply a right to abortion in *Dobbs* as an implied liberty right with respect to deprivation of liberty under the Fourteenth Amendment (as discussed in Part III). This individual liberty decision may have reasoning that bleeds over into the information privacy context. Thus, enacting an express information privacy right would reduce concern that courts might not imply such a right from the Constitution. An express information privacy right could effectively eliminate debate between originalists and strict constructionists that privacy is not constitutionally defined versus others willing to imply an information privacy right from various other express constitutional guarantees.

Another concern is that the world is anticipating an explosion in AI technology and will face new and unknown privacy consequences. A federal law that broadly guarantees citizens freedom from information privacy abuse, both from government and commercial actors, would seem particularly preferable to waiting for Congress to craft a custom-tailored AI privacy law after society experiences a variety of negative privacy consequences. With a broad information privacy right, courts and regulators could decide what is an abuse, versus what is not, as technology and associated privacy harms evolve together.

As evidenced by the discussion below, I assert that neither governments nor private organizations can be trusted with personal data. Therefore, meaningful legislation is necessary for both consumer protection

and for providing a free society in the criminal context. In 2023, President Biden's State of the Union address specifically referenced the importance of privacy rights.[9] Perhaps it is now time to enact a broad federal privacy right, especially with concerns over AI rapidly expanding and changing our world in unforeseen ways. It would seem a fool's errand to create a detailed statute to address unknown new harms from AI or other advancing technology. Thus, a broad and flexible constitutional amendment seems preferable.

II. 1890 VS. TODAY

Interestingly, the 1890 article was written against a backdrop of yellow journalism (i.e., exaggerated or completely false news) fueled by the proliferation of photography and mass printing technology, which was a new mass media for information delivery. Today, the concerns are parallel, as mass information-sharing technology continues to proliferate. One key difference today is that the scale and speed of information dissemination is exponentially greater than it was in 1890 (evolving from newspapers and telegraphs to radio, then television and fax machines, to the internet and emails).

Today, the type of information media has changed from print to primarily electronic media. Historically, major news outlets dominated the landscape, but today there are more news sources, including social media which supports various influencers in the attention economy.[10] Another interesting historical parallel is that pre-Civil War, newspapers were often perceived as nothing more than appendices of political parties, and today, similar perceptions persist.[11] Beginning in the 1870s, however, with improvements in printing speeds and photography, newspapers started producing content that expanded beyond political propaganda and delved into the realm of public figure gossip. The problem of prying reporters invading the privacy of others arose.[12]

A second key difference today is the exponential increase in surveillance capability with respect to an individual's information (and the increasing ability for long-term storage of such information). This

[9] President Joseph Robinette Biden, Jr., State of the Union Address (Feb. 27, 2023), https://www.whitehouse.gov/state-of-the-union-2023/ [https://perma.cc/FSK5-CBT9].

[10] For a general discussion of social media influencers, *see* Monique Groen, *Swipe up to Subscribe: The Law and Social Media Influencers*, 21 TEX. REV. ENT. & SPORTS L. 113 (2020).

[11] Ken Gormley, One Hundred Years of Privacy, 1992 WIS. L. REV. 1335, 1350-51 (1992) (describing that "[p]rior to the Civil War, newspapers had been small and expensive, and largely served as appendages of local political parties" but describing yellow journalism expanding beyond politics in the 1870s).

[12] *Id.*

surveillance capability can be abused by both the government and private actors or government and private actors working together. Regarding information dissemination, the problems today are somewhat similar to 1890. But, surveillance capability is dramatically different from 1890, creating new benefits and abuses. To recap, I perceive two major changes: (1) a dramatically increased ability to disseminate information and (2) a dramatic increase in the ability to track and surveil individuals, whether by government or private actors. Both of these major changes will likely continue to advance.

Regarding surveillance capability of individuals, one of the greatest changes in privacy is that in 1890 (as discussed in section A.4 below) it was generally not possible to invade a person's private thoughts. Today, this is typically no longer true because an abundance of electronic data, such as browsing history, emails, social media usage, location history, text messages, and more, may reveal an individual's most sensitive information, including their private thoughts.[13] This leads to the question of whether surveillance capability should be reduced or not pursued further. The answer is likely no as the cat is essentially out of the bag, and stopping technology development seems contrary to human nature. Historically, antitechnologists have argued that humans are playing God with respect to certain new advances such as surgery, genetic engineering, or fertility/conception procedures.[14] That same futile argument could be applied to tech. Arguably, tech is the new God: it knows where you are, where you've been, if you're awake or asleep, where you might be going, your most intimate thoughts and desires, and perhaps even whether you might commit a crime. Stopping the expansion of these godlike powers is likely not practical, so establishing safeguards for when and how government or private actors can tap into this God power seems more practical than stopping technology.

---

[13] Brief of Laurent Sacharoff as AmicusAmicus Curiae Supporting Petition for Certiorari, Andrews v. New Jersey, 141 S. Ct. 2623 (2021) (No. 20-937). Smartphones function more like a part of our mind. Bryan H. Choi, *The Privilege Against Cell Phone Incrimination*, 97 TEX. L. REV. 73, 75 (2019). They have become an integral part of our memory, and we use them to accomplish numerous mental tasks. To the extent the Fifth Amendment protects a private mental sphere in connection with criminal investigations, at least, it should have a special application to these special devices. *Cf.* Riley v. California, 573 U.S. 373 (2014).

[14] For example, in vitro fertilization (IVF) was considered unnatural, immoral, and dangerous by religious leaders when the first IVF baby was born in 1978. Ariana Eunjung Cha, *How Religion is Coming to Terms with Modern Fertility Methods*, WASH. POST (Apr. 27, 2018), https://www.washingtonpost.com/graphics/2018/national/how-religion-is-coming-to-terms-with-modern-fertility-methods/ [https://perma.cc/B3ZP-S3ZZ]. However, today IVF and related technologies have helped to produce over 7 million babies and birthed a $17 billion industry. *Id.*

Privacy law is evolving alongside new technologies to disseminate and collect information (e.g., evolving from newspapers to door-to-door salesman to online tracking) and new methods of protecting information (e.g., evolving from locking papers in a safe to encrypting information on a third party cloud provider's platform). The 1970s saw the enactment in the U.S. of the Privacy Act of 1974[15] to protect government employee information, and the Fair Credit Reporting Act,[16] which was the most comprehensive privacy statute ever enacted at that time. The Fair Credit Reporting Act implicates many privacy principles relative to electronic records, such as a consumer's right to access and rectify financial information as well as to keep it from prying eyes. Around this time, the U.S. developed Fair Information Principles to guide new legislation. Simultaneously, Europe developed very similar OECD privacy principles. The U.S. and Europe have influenced, and continue to influence, each other regarding development of privacy.[17]

The U.S. should follow the E.U.'s lead and view information privacy as a fundamental human right necessary for a free society. Broad legal safeguards would then be critical to inhibit both private party and governmental infringements. Such privacy safeguards are critical given the reality that neither governments nor private organizations can be trusted with respect to personal data. However, enacting meaningful privacy safeguards is challenging given lobbying efforts by government agencies attempting to maximize investigatory power and tech platforms economically addicted to personal data.

A. New Technology Challenges: 1890 vs. Today

In their 1890 article, Warren & Brandeis were responding to new harms brought by new technologies, particularly instant photographs and mass printing, which facilitated privacy invasions. To combat these new harms, they discussed the birth of a new right: the right to be let alone, which they later express as supporting a right to privacy, in "recognition of man's spiritual nature, of his feelings and his intellect."[18] They referenced

[15] Privacy Act of 1974, as amended, 5 U.S.C. § 552a.

[16] Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x.

[17] As an example, the CCPA is regarded as a GDPR inspired law. *See* Navdeep K. Singh, *What You Need to Know about the CCPA and the European Union's GDPR*, AMERICAN BAR ASSOCIATION (Feb. 26, 2020), https://www.americanbar.org/groups/litigation/committees/minority-trial-lawyer/practice/2020/what-you-need-to-know-about-the-ccpa-and-the-european-unions-gdpr/ [https://perma.cc/UQX5-2GY6].

[18] Warren & Brandeis, *supra* note 1, at 193.

this right to be let alone as part of the right to liberty.[19] They emphasized the need for this right in reference to the evils of privacy invasions by newspapers especially in the face of this new technology of the day: instant photographs combined with mass printing capability.[20] They referenced the evil of the day as gossip columns procured by "intrusion upon the domestic circle," noting "even gossip apparently harmless, when widely and persistently circulated, is potent for evil."[21]

1. Feelings & Privacy Are Still Linked

Warren and Brandeis astutely recognized "feelings" as underlying a right to privacy. Arguably, freedom is a feeling (e.g., to what extent someone feels free or restricted), and privacy as a component of freedom is likewise a feeling. Certainly, individual needs for freedom can vary as some prefer to live in an unregulated rural area while others may feel sufficiently free living in a city high rise with a number of regulations (as these environments provide different levels of decisional freedom and freedom from surveillance). The concept of feeling discomfort with privacy invasion had been present in the law for many years prior to 1890. Perhaps one of the earliest legally significant embodiments of privacy occurred in around 1361, when the Justices of the Peace Act was promulgated against "peeping Toms" and eavesdroppers. In 1765, British Lord Camden protected the privacy of the home by striking down a baseless warrant-to-enter, thus reinforcing the basic notions of territorial privacy.[22] Soon after, the United States saw fit to embody a similar provision in its own Bill of Rights in the Fourth Amendment.

While various legal sources describe avoidance of legal damages for mere hurt feelings or discomfort,[23] it's interesting to observe case law shifting in recent years to allow standing to sue in data breach cases where there are no concrete economic damages alleged, but rather a mere fear of future identity theft.[24] This recent trend evokes a broader question of

[19] Warren and Brandeis credit Judge Cooley as securing an individual's "right to be let alone." Warren & Brandeis, *supra* note 1, at 195 (citing Thomas M. Cooley, *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract* 29 (2d ed. 1888).

[20] Warren & Brandeis, *supra* note 1, at 195.

[21] *Id.*

[22] Michael P. Couture, Constitutional Law—Administrative Inspections—Right to Refuse Inspector Admittance Without a Warrant, 17 BUFF. L. REV. 914, 915 (1968). Available at: https://digitalcommons.law.buffalo.edu/buffalolawreview/vol17/iss3/18.

[23] *See* Lujan v. Defs. of Wildlife, 504 U.S. 555 (1992) (holding hurt emotions not sufficient to establish actual or imminent injury for purposes of standing).

[24] Federal circuit courts are split on whether the risk of future harm stemming from a data breach satisfies the injury-in-fact requirement of Article III standing. Simone Cadoppi, *Injury-in-Fact: Solving the Federal Circuit Court Split Regarding Constitutional Standing in Data Theft Litigation*, 52 GOLDEN GATE U. L. REV. 163, 173 (2022). However, the Third, Sixth, Seventh, Ninth, and District of Columbia

whether and to what extent feelings are relevant to privacy and other legal claims.[25] A variety of non-legal scholarly sources discuss the role of feelings in human decision making,[26] so legal decisions on whether a plaintiff has been harmed could certainly have an emotional component. The general topic of the interrelationship between emotions and the law might merit further exploration in the legal context, particularly with regard to privacy.

Regarding psychological discomfort with privacy invasions, a Westlaw search of expert witness reports having the term "privacy" in proximity to "psychological distress"[27] reveals a number of psychology experts referencing psychological distress in connection with a party experiencing some form of privacy invasion.[28] Considering these reports along with the E.U. constitution (i.e., Charter of Fundamental Rights), which recognizes privacy as a fundamental human right,[29] it seems appropriate to argue that a human's right to privacy should be recognized as a fundamental human right in the United States too.[30] Further, perhaps Maslow could have included a need for privacy in his hierarchy of human

Circuits seem to take a plaintiff-friendly approach to the analysis. *Id.* at 177. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015); In re Zappos.com, Inc., 888 F.3d 1020, 1029-30 (9th Cir. 2018).

[25] Eric A. Posner, *Law and the Emotions*, 89 GEO. L.J. 1977 (2001).

[26] *See generally* Nasir Naqvi et al., *The Role of Emotion in Decision Making: A Cognitive Neuroscience Perspective*, 15 CURRENT DIRECTIONS IN PSYCH. SCI. 260 (2006); Jane So et al., *The Psychology of Appraisal: Specific Emotions and Decision-Making*, 25 J. CONSUMER PSYCH. 359 (2015).

[27] I searched Westlaw's Expert Reports and Affidavits database using the terms "privacy" and "psychological distress," which resulted in ninety-nine results. I perused only a few of the results which referenced privacy, noted below, which included some reference to privacy in connection to psychological distress.

[28] Vitoux Aff. at 1, *Hutchison v. Texas Cnty., Mo.*, No. 09-3018-CV-S-RED, 2010 WL 11509270 (W.D. Mo. Dec. 1, 2010) (referencing diagnosis of Posttraumatic Stress Disorder after search of home); Miller Aff. at 6, *Kilpatrick v. Skytel, Inc.*, No. 10CV00287, 2010 WL 8534272 (S.D. Miss. Dec. 14, 2010) (referencing psychological trauma after text messages leaked and published in newspaper); Vandenbelt Aff. at 3, *Quantz v. Edwards*, No. C04-5737RJB, 2005 WL 3500838 (W.D. Wash. Dec. 21, 2005), *aff'd in part, rev'd in part and remanded*, 264 F. App'x 625 (9th Cir. 2008) (discussing embarrassment associated with private matters); Rines Aff. at 2, *Tardiff v. Knox Cnty.*, 453 F. Supp. 2d 190 (D. Me. 2006) (discussing trauma as a result of invasion of privacy); Thrope Aff. at 3-4, *Hall v. Green Tree Servicing, LLC*, No. 1:10-CV-216-JAW, 2010 WL 8981687 (D. Me. Oct. 23, 2010) (referencing telephone harassment causing psychological distress).

[29] Art. 8 EU Charter of Fundamental Rights "Protection of Personal Data" ("Everyone has the right to the protection of personal data concerning him or her."), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT [https://perma.cc/F5DN-H4VB].

[30] AUSTRALIAN PRIVACY FOUNDATION, https://www.privacy.org.au/Resources/PLawsIntl.html [https://perma.cc/DSV8-N4GY] (last visited Mar. 6, 2023) (noting a number of legal sources supporting privacy as a fundamental human right).

needs,[31] given that some sources reference Maslow's hierarchy of needs when discussing privacy.[32] This article does not offer any deep analysis of psychology, but it seems plausible that a human need for privacy could be placed as somewhere in the middle of the hierarchy (e.g., somewhere above physiological and safety needs).

The right to be let alone captures a human's need for unobserved solitude both in 1890 and today.[33] In 1890, the abundance of prying reporters disrupted solitude among elites and others targeted by reporters. Later, as people moved from the cities to the suburbs in the 1940s and 50s, door-to-door solicitors were a key concern as many homeowners desired solitude from commercial, political, and religious solicitors. Today, advertisers serving these highly targeted online ads may be a new door-to-door salesman, one that is constantly watching and who regularly solicits.

2. Speed of Information Dissemination 1890 Versus Today

In many respects, information-sharing technology today is similar to 1890 but on a faster and larger scale. In 1890, the ability of the press to quickly churn out daily written newspaper content with photos was a substantial leap in information-sharing technology. This growth of printing technology was driven by a thirst for advertising dollars, just like the growth of electronic information technology in recent decades. Today, the scale of information sharing is much larger with instantaneous publication of written content, photos, and videos, and many of the problems in 1890 associated with false information or gossip content are similar today. The temptation to publish misleading or scandalous stories about individuals was a key privacy issue then, and still is today, given the same motivation to attract readers for generating advertising dollars. However, while faster information delivery today is one difference, perhaps the more significant difference is information collection.

---

[31] Maslow offered his hierarchy of human needs in 1943 with a general theory that needs lower in the hierarchy must be satisfied before individuals can attend to needs higher up. *See* Saul Mcleod, *Maslow's Hierarchy of Needs Theory*, SIMPLE PSYCHOLOGY (Mar. 6, 2023), https://simplypsychology.org/maslow.html [https://perma.cc/K3UM-RR7Y] (noting that a human must first meet lower level physiological (food and clothing) and safety needs before addressing love and belonging needs (friendship), esteem, and self-actualization needs).

[32] Roger Clarke, *What's 'Privacy'*, (Aug. 7, 2006), http://www.rogerclarke.com/DV/Privacy.html; Rick Falkvinge, *Understanding the Different Maslow Need Levels for Privacy*, PIABLOG (Feb. 15, 2017), https://www.privateinternetaccess.com/blog/understanding-the-different-maslow-need-levels-for-privacy/ [https://perma.cc/G57E-JW57].

[33] David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CAL. L. REV. 1069, 1121 (2014) ("In the coming era, when camera-bearing robots swarm the skies, we will all need . . . some zone of sanctuary we can feel unobserved. Some corner where our hearts can remain forever just our own.") (*citing* David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (1998)).

3. Information Collection Today Is Far More Extensive Than in 1890

In the 1940s and 1950s, door-to-door salesmen likely collected valuable information about households in terms of purchasing history and product preferences.[34] (Presumably, successful merchants in 1890 likewise collected customer information as an essential sales strategy.)

Today, technology's ability to quickly track consumer demographics and preferences is much greater than in the past. In 1890, a printed newspaper could not sense who was reading it and what their attributes are, but technology today can have a seemingly supernatural power of knowing who someone is, where they are, and potentially every intimate detail of their lives.[35] In 1890, a person's uncommunicated thoughts were likely considered undiscoverable, but today technological tools exist to develop sophisticated psychological profiles with the potential to effectively sway elections or sell tangible products with targeted propaganda.[36] For example, one source identifies a data broker, Acxiom, as collecting 1,500 data points about a person, going beyond mere demographic information and collecting a variety of behavioral information (such as political/philosophical views, family life, online purchase behavior, etc.).[37] Data collection can combine volunteered data, observed data, and inferred data to develop a detailed consumer profile.[38] A data broker may conduct web scraping (e.g., collecting public social media info) in combination with

---

[34] *See* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1377-80 (1992) (discussing door to door solicitation issues in case law in the context of religious or commercial solicitation).

[35] Consumer data falls under four basic categories: (1) personal data (e.g. location, gender, social security number), (2) engagement data (how consumers interact with a website), (3) behavioral data (e.g. purchase histories and product usage information), and (4) attitudinal data (satisfaction, purchase criteria). Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, BUSINESS NEWS DAILY (Nov. 21, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html [https://perma.cc/KU3Y-SLWT].

[36] "(A) person's patterns of behavior (such as their language patterns, number of friends, frequency of logins) can reveal certain demographic attributes or personality traits when analyzed by computer algorithms. The opportunity to study human behavior in this way has provoked much research seeking to predict how accurately personal information can be predicted from a person's digital footprints (e.g. Hinds and Joinson, 2018; Hinds & Joinson, 2019)." Joanne Hinds, Emma J. Williams & Adam N. JoinsonJoinson, *"It Wouldn't Happen to Me": Privacy Concerns and Perspectives Following the Cambridge Analytica Scandal,* 143 INT. J. HUM. COMPUT. STUD. 102498, at 2 (2020).

[37] Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES (June 16, 2012), https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html [https://perma.cc/M4BA-6WKY].

[38] *How Companies Profit and Use Your Personal Data*, CBS COMPLETE BACKGROUND SCREENING, https://cbscreening.co.uk/news/post/your-personal-data-and-how-companies-use-it/ [https://perma.cc/Q9VD-C8Z6] (last visited Mar. 6, 2023).

a search of public records to develop a consumer's profile,[39] and scraping tools won't hesitate to access data visible only to members, despite violating the site's terms of use.[40]

A famous example of surreptitious data collection was observed in the Cambridge Analytica Facebook scandal. Data scientists developed an app which offered users a series of questions in order to build psychological profiles of eighty-seven million users without their consent and then used this data for subsequent marketing purposes. The app harvested data not only from participating users but also from their connected friends. The psychological data was then used to influence the 2016 U.S. presidential election and also the U.K. Brexit referendum, resulting in a five-billion-dollar FTC fine against Facebook.[41]

Today, the massive collection of personal information, for advertising or other purposes, has exploded into new territory, effecting new potential abuses, such as some members of the public having an uncomfortable feeling of being constantly surveilled by both government and private actors.

4. Today, Private Thoughts are Far More Accessible Than in 1890

Due to the availability of massive amounts of personal data, personal data collection tools, and the use of statistics and psychological profiling, deciphering an individual's private thoughts is much easier than in 1890. The invasive power of technology in terms of providing massive amounts of personal information is certainly a concept recognized by courts as noted in *Riley v. California*, which was a case concerning warrantless seizures of smartphones.[42] Thus, the availability of so much information, and new

---

[39] Margaret Rouse, *Web Scraping,* TECHOPEDIA, https://www.techopedia.com/definition/5212/web-scraping [https://perma.cc/54EK-KMFK] (last visited Mar. 6, 2023).

[40] In HiQ Labs v. LinkedIn, 938 F.3d 985 (9th Cir. 2019), HiQ successfully fought against LinkedIn's cease-and-desist to prevent HiQ from copying data off of LinkedIn. This ruling, which affirmed that web scraping public data was not a violation of the Computer Fraud and Abuse Act, was upheld in April 2022. Zack Whittaker, *Web Scraping is Legal, US Appeals Court Reaffirms*, TECHCRUNCH (Apr. 18, 2022), https://techcrunch.com/2022/04/18/web-scraping-legal-court/ [https://perma.cc/E2PD-R2M4].

[41] Rob Davies & Dominic Rushe, *Facebook to Pay $5bn Fine as Regulator Settles Cambridge Analytica Complaint*, THE GUARDIAN (July 24, 2019), https://www.theguardian.com/technology/2019/jul/24/facebook-to-pay-5bn-fine-as-regulator-files-cambridge-analytica-complaint [https://perma.cc/2NX8-F7WG]; Patrick Day, *Cambridge Analytica and Voter Privacy*, 4 GEO. L. TECH. REV. 583, 585 (2020)(noting that Cambridge Analytica used what the firm called "psychological operations" or psyops to influence people not through persuasion but through information dominance, a set of techniques that includes rumor, disinformation, and fake news).

[42] Riley v. California, 573 U.S. 373 (2014).

usages thereof, will likely continue to provide both benefits and harms to society as technology continues to evolves.[43]

A good example of the potential God-like omniscience of technology can be seen in actor Jussie Smollett's prosecution in 2020.[44] There, an Illinois judge signed off on two separate search warrants ordering Google to turn over all files associated with Smollett's Gmail address, along with "any and all location data and information from the use of GoogleMapsTimeline."[45] The warrants also demanded all records and historical web history data associated with Smollett's email address, all geolocation and geotagging data, and any and all "private messages" – including sent email, drafts,[46] and deleted messages.[47] It's staggering to imagine how much private information could be revealed about a person by examining a year's worth of emails, text messages, and location data. Smollett's case highlights how large of a digital footprint nearly every person has with respect to virtually every aspect of his life (e.g., romantic and family relationships, medical issues, career, sexual or political interests, etc.). In some cases, browsing history could also be requested along with data from vehicles and other devices. While having the availability of so much evidence relative to a civil claim or criminal charge is useful for such purposes, the collection of so much data by one organization (in Smollett's case, Google), certainly evokes the need for suitable regulation to inhibit abuse. It also raises a related general question of whether a single entity should possess so many types of data about an individual.

Smollett's case essentially involved electronic surveillance of information held by a private entity. In 1968, Alan Westin advocated a balanced position regarding surveillance: "generally prohibiting surveillance but allowing limited use in cases of national security and major crimes."[48] Perhaps Smollett's offense constituted a major crime as it

---

[43] *See* Olaf quotes *supra* note 3.

[44] Smollett was charged in Cook County Illinois in 2019 with felony disorderly conduct for filing a false report after allegedly staging the attack against himself in Chicago.

[45] *Judge Signs Off On Search Warrants Demanding Jussie Smollett's Data From Google*, CBS CHICAGO (Jan. 8, 2020 10:31 PM), https://www.cbsnews.com/chicago/news/judge-signs-off-on-search-warrants-demanding-jussie-smolletts-data-from-google/ [https://perma.cc/89LR-YHZ8].

[46] As a side note, apparently the warrant shows awareness of an email trick commonly used by terrorists of using draft emails to share information as a way to avoid transmitting the message. *See* Nick Allen, *Petraeus And Lover Used An Email Trick Used By Terrorists To Keep Affair Secret*, INSIDER (Nov 13, 2012, 7:14 AM), https://www.businessinsider.com/petraeus-used-trick-to-hide-emails-2012-11 [https://perma.cc/F7KF-5WRA].

[47] *Judge Signs Off On Search Warrants Demanding Jussie Smollett's Data From Google*, *supra* note 45.

[48] Alan F. Westin, *Privacy and Freedom*, 25 WASH. & LEE L. REV. 166 (1968).

was a felony charge and involved use of considerable law enforcement resources to investigate his false claim. In any event, as surveillance capability continues to grow, Westin's concept should be kept in mind.[49]

5. Advertisements Are Far More Targeted Today Than in 1890

Data collection has allowed ads to become far more targeted than in 1890. At a high level, advertising motivation is a major cause of various privacy abuses and has evolved in phases. In 1890, newspaper ads likely had minimal targeting. For example, an ad for a common product might be placed next to a story of general interest, while an ad for cosmetics might be selectively placed near content that might appeal to a female audience. In contrast, today, tracking of browsing activity enables a social media platform to display highly targeted ads related to products a user was previously searching.

Regarding consumer surveillance, consumer opinions may vary about whether and to what extent they have privacy concerns. On one hand, if Amazon tracks a consumer's purchasing habits, and then suggests products she might actually want, this might be desirable to the consumer.[50] On the other hand, some consumers might be leery of excessive tracking if Amazon listens to conversations within a home, is aware of who is in the home at all times, shares ring camera footage with law enforcement without consent, etc.[51] Some authors have criticized targeted ads describing them as creepy; for example, if Google served up ads for hotel deals in Maryland based on a person's browsing history planning a trip there, this could be perceived as helpful or creepy.[52] In 2021, it was estimated that

[49] As well as my parallel theory applying Blackstone's ratio to privacy. *See* Anthony Volini, *A Deep Dive into Technical Encryption Concepts to Better Understand Cybersecurity & Data Privacy Legal & Policy Issues*, 28 J. INTELL. PROP. L. 291, 339-40 (2021) ("Just as the Blackstone ratio principle favors constitutional protections that allow ten guilty people to go free rather than allowing one innocent person suffer, individual privacy rights could arguably favor fairly unsurveillable encrypted communications at the risk of not detecting various criminal activity.").

[50] The popularity of targeted ads is itself difficult to determine. One July 2020 study conducted by Innovid showed that 43% of U.S. adults liked personalized digital ads, while a February 2021 YouGov study of French and German adults showed that 57% did not want to receive *any* targeted ads. *Compare* Neil Cummins, *Invasion of Privacy? What Consumers Think of Personalized Online Ads*, BUSINESS NEWS DAILY (Jul. 7, 2022), https://www.businessnewsdaily.com/4632-online-shoppers-personal-ads.html [https://perma.cc/X6TY-M2HZ], *with Do people really want personalized ads online?,* GLOBAL WITNESS (Apr. 15, 2021), https://www.globalwitness.org/en/blog/do-people-really-want-personalised-ads-online/ [https://perma.cc/5JTN-UR63].

[51] Katie Tarasov, *Amazon Dominates the $113 Billion Smart Home Market — Here's How It Uses the Data It Collects,* CNBC (Sep. 28, 2022), https://www.cnbc.com/2022/09/28/amazon-dominates-the-smart-home-now-privacy-groups-oppose-irobot-deal.html [https://perma.cc/89J6-SCPZ].

[52] Rebecca J. Rosen, *What Does It Really Matter If Companies Are Tracking Us Online?*, THE ATLANTIC (Aug. 16, 2013), https://www.theatlantic.com/technology/archive/2013/08/what-does-it-really-matter-if-companies-are-tracking-us-online/278692/ [https://perma.cc/MWX6-7WHL].

almost 259 million homes worldwide would qualify as a "smart home" with nearly a quarter of U.S. households possessing at least three smart house devices; a trend that is forecasted to continue growing.[53] Thus, the potential for abuse seems increasingly significant.

As advertisers become more sophisticated, their tactics could be perceived as abusive. For example, they may be able to exploit consumers at a time when they are most vulnerable to impulse purchasing decisions.[54] One author writes, "[t]here may be nothing particularly embarrassing or personal about my vulnerabilities as a consumer, but I do not especially want to share them with companies so that I can be manipulated for their financial gain."[55] As an example, suppose an advertiser engages in price discrimination and wants to upcharge a man "for flowers if a computer recognizes that he's looking for flowers the day *after* his anniversary."[56] As a further example, suppose I borrow a laptop from a family member and search for content on a particular type of product (e.g., a brand of guitar); thereafter, my family member begins receiving multiple emails from this guitar manufacturer. In a highly egregious example of privacy relative to targeted ads, one article describes a pregnant teenage girl receiving coupons for infant products, thereby informing her father that she was pregnant before she was ready to disclose her situation.[57]

To sum up targeted ads, some consumers may feel indifferent about them, while others wish to limit personal data collection. Individuals seem to vary in their level of privacy concern. The California Consumer Privacy Act ("CCPA") is one example of a recent state law that, like the E.U.'s General Data Privacy Regulation ("GDPR,") can have an impact on reducing unwanted targeted ads by fining organizations for collection without consent.[58] The CCPA and other emerging laws may curtail some practices by the data brokerage industry and will likely impact retailers like

---

[53] Jason Wise, *Smart Home Statistics 2022: How Many Smart Homes Are There?*, EARTHWEB (Oct. 24, 2022), https://earthweb.com/smart-home-statistics/ [https://perma.cc/25CS-G2K4] ("In 2021, there were 258.54 million smart homes across the world.")..").

[54] *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV 995, 999 (2014) (describing the means in which digital commerce influences consumers at a highly personal, individualized level, triggering irrationality or vulnerability in consumers, leading to harm).

[55] Rosen, *supra* note 52.

[56] *Id.*

[57] Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=8d1bcbb66686 [https://perma.cc/68ZR-3VQA].

[58] Patrick Coffee, *Brands Review Data Privacy Policies After $1.2 Million Sephora Settlement*, WALL STREET JOURNAL (Sep. 27, 2022), https://www.wsj.com/articles/brands-review-data-privacy-policies-after-1-2-million-sephora-settlement-11664272801 [https://perma.cc/FH9C-LDLD].

Amazon which collect personal information generally for internal use rather than transfers to third parties.[59] As discussed in various sections below, notice and consent statutes are likely not a privacy panacea.

6. In 1890, the Authors Imagined the Impact of Unknown New Technologies, Just Like We do Today

Warren and Brandeis seemed to imagine the possibility of future technologies posing similar dangers to those faced in 1890: the dangers of the "too enterprising press, the photographer, or the possessor of any other modern device for recording or producing scenes or sounds."[60] Modern technologies include ubiquitous video cameras in public or the ability to track a person's location in real time via cell phone information. Also included is the ability to track and record someone's browsing history, which may have some similarity to tracking via photos and videos which locations someone is visiting. Tracking browsing history is roughly analogous to tracking books one has checked out from a library, which was a topic of debate from a First Amendment standpoint both before and after enactment of the USA PATRIOT Act.[61] These modern technologies are essentially advances in the ability to observe and record a human's location and behavior. 1890 printing and photography technologies and their associated privacy harms seem simpler to understand than today's technologies. A key challenge today in assessing privacy often involves first understanding the relevant technology.

Evaluation of privacy risks of emerging technologies will continue to challenge lawyers and others as technology evolves. In my view, the most capable lawyers to engage in such analyses are those who have at least some basic understanding of information technology, particularly what's happening under the hood.[62] As an analogy, an attorney considering a products liability issue relative to an automotive technology would certainly benefit from knowing how to drive a car. However, having an understanding of how the car's components work and how they interact is likely far more helpful when assessing the relevant legal claims. After all,

---

[59] Brian Naylor, *Firms Are Buying, Sharing Your Online Info. What Can You Do About It?*, NPR: ALL TECH CONSIDERED (July 11, 2016), https://www.npr.org/sections/alltechconsidered/2016/07/11/485571291/firms-are-buying-sharing-your-online-info-what-can-you-do-about-it [https:/perma.cc/RSY2-ENAK].

[60] Warren & Brandeis, *supra* note 1, at 206.

[61] Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, beyond Chilling Speech*, 49 U. RICH. L. REV. 465 (2015).

[62] Anthony Volini, *A Perspective on Technology Education for Law Students*, 36 SANTA CLARA HIGH TECH. L. J. 165, 185 (2020) (noting that while "millennials have grown up with technology and are likely more adept than prior generations at its usage, this technology usage merely affords some awareness on the user side").

attorneys would likely struggle to apply the law effectively to facts they don't understand.

As an example, several years ago the tech community was assessing whether and to what extent DNS ("Domain Name Service") over HTTPS would further privacy interests (e.g., a technology that would make it somewhat difficult for an ISP to observe websites visited by consumers).[63] For an attorney to understand potential privacy shortcomings of this technology and then engage in helpful discussion on the topic, he would require some basic understanding of how both DNS and HTTPS work.[64] Such a basic understanding could be furthered by reviewing the sources cited on this topic to understand DNS is a key tool for computers to look up websites and how DNS queries can be encrypted from eavesdroppers via HTTPS.

In the mid–1990s, Judge Easterbrook referenced the "law of the horse" relative to cyber law, a theory that broad legal principles can accommodate any niche area without the need to create a new area of legal study.[65] Data privacy law does not appear to be the law of the horse as computer technologies have essentially presented new types of legal issues requiring enactment of new laws to address them. As Easterbrook noted, "[e]rror in legislation is common, and never more so than when the technology is galloping forward. Let us not struggle to match an imperfect legal system to an evolving world that we understand poorly."[66] This statement supports that law school training in technology and the laws pertaining thereto will continue to be a worthwhile goal from a legislative standpoint (and likely worthwhile for legal analysis in practice and other contexts).

Easterbrook's comment about technology always galloping forward is on point. For many decades, information technology has grown at an exponential rate, and this trend will likely continue, as witnessed through the evolution of AI. Perhaps one of the best indicators of this exponential growth is referenced in one of my prior works with regard to the world running out of IP addresses.[67] In the early 1980s, IPv4 (version 4) was developed to provide over four billion IP addresses to accommodate any

---

[63] Catalin Cimpanu, *DNS-over-HTTPS Causes More Problems Than It Solves Experts Say*, ZDNET (Oct. 6, 2019), https://www.zdnet.com/article/dns-over-https-causes-more-problems-than-it-solves-experts-say/ [https://perma.cc/C285-WGGF] (noting various criticisms of DoH in terms of privacy and security).

[64] Volini, *supra* note 49, at 339-40 (discussing mechanics of these protocols and potential privacy shortcomings).

[65] Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996).

[66] *Id.* at 215.

[67] *See* Volini, *supra* note 62, at 174-75.

computer to connect to the internet.[68] Since the early 1980s, humanity is running out of these IPv4 addresses as cars, smartphones, and other devices around the world are using up these addresses, which has necessitated the creation of IPv6,[69] which provides an exponentially larger number of IP addresses.[70] This need for IPv6 highlights the explosion of technology in the last few decades, and it seems plausible that exponential growth of tech will continue.

a. AI Proliferation Will Likely Present New Privacy Challenges

Today, AI technology is rapidly developing and will likely result in some abuses of privacy in new, presently unknown ways. Legal jurisdictions around the world are just beginning to address AI and privacy with proposed legislation.[71] AI proliferation is expected to rapidly produce new harms and benefits, and legal systems will likely fail at keeping up with regulating various unforeseen issues, particularly with a notice and consent approach to privacy, which seems wholly inapplicable to an AI tool gathering public data.[72] Individuals encounter notice and consent when presented with a barrage of notifications and banners linking to lengthy privacy policies, which very few people actually read.[73]

Privacy concerns with automation have been present since the 1960s as society imagined various profiling and decision-making activities performed by analysis of large data sets that were beginning to develop.[74] Thus, a review of helpful scholarship from the 1960s and 70s, from Westin and others, seems worthwhile to assess new AI issues (in addition to reviewing scholarship from this era regarding surveillance, as noted earlier).

---

[68] *Id.*

[69] IPv5 (version 5) never gained substantial traction. *See* Bradley Mitchell, *What Happened to IPv5?*, LIFEWIRE (Dec. 16, 2022), https://www.lifewire.com/what-happened-to-ipv5-3971327 [https://perma.cc/V5Y8-D2VP].

[70] *Id.*

[71] Daniel J. Felz et. al, *Privacy, Cyber & Data Strategy Advisory: AI Regulation in the U.S.: What's Coming, and What Companies Need to Do in 2023*, ALSTON & BIRD (Dec. 9, 2022), https://www.alston.com/en/insights/publications/2022/12/ai-regulation-in-the-us#:~:text=Several%20use%2Dcase%2Dspecific%20AI,and%20new%20NIST%20AI%20standards.&text=In%20the%20U.S.%2C%202022%20saw,on%20specific%20AI%2Duse%20cases [https://perma.cc/8F73-3PVM].

[72] Cameron F. Kerry, *Protecting Privacy in an AI-driven World*, BROOKINGS (Feb. 10, 2020), https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/ [https://perma.cc/UH3L-69B9].

[73] *Id.*

[74] Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's*, 66 COLUM. L. REV. 1003, 1010 (1966) ("Businessmen, government officials, behavioral scientists, and many others are now better able to make more fact-based, logical, and predictable decisions than they ever could before the age of electronic information storage and retrieval systems.").

At a high level, AI typically works by processing massive amounts of data, looking for patterns, and making suggestions to humans.[75] Data processed could be publicly available on the web or obtained from other parties. One type of privacy abuse might involve the AI platform obtaining consumer data from a third party where the consumers never consented to the collection. Another potential abuse might involve AI collecting deidentified data and then reidentifying individuals.[76] This would be one example of AI abuse involving harvesting publicly available data, published for one purpose, and then used by the AI platform for a different purpose that the data publishers never envisioned.[77] This category of potential abuse is described by Helen Nissbaum as "contextual integrity," which is violated when data is provided in one context and then is used in some other unexpected context.[78]

Such contextual integrity abuses would seem to arise when public data is combined from multiple sources and then used in a way to abuse individual privacy.[79] As a hypothetical, one could imagine a video camera mounted on a city building, facing a public sidewalk. The building owner might also have video cameras in the lobby and other publicly accessible common areas. The original intent of the cameras might be to have up to 48 hours of footage stored in the event of an accident or crime occurring on the premises. So far, this hypothetical doesn't seem violative of privacy, especially if the public is aware of these cameras. However, suppose a third party approaches the building owner, and other local building owners, offering to store the footage for free or at a low cost. Suppose further that the third party works with government agencies and or other private parties to apply facial recognition to all footage to enable tracking of individuals throughout the city for extended periods of time. Consider that AI is employed to look for patterns in the location data, offering suggestions on

---

[75] AWS Data Exchange, AMAZON, https://aws.amazon.com/data-exchange/?trk=59396dec-bd12-4138-addb-b1ff37b6bde8&sc_channel=ps&s_kwcid=AL!4422!3!645224671359!p!!g!!data%20sets&ef_id=CjwKCAiA3KefBhByEiwAi2LDHDA8zkgQdFlxQh4Keb0Bg0mcyn85ZSFhrz6GNdxBVU0YRS5woWzeDBoCCQ4QAvD_BwE:G:s&s_kwcid=AL!4422!3!645224671359!p!!g!!data%20sets [https://perma.cc/U3AR-3U36] (last visited, Mar. 6, 2023) (offering over a thousand free data sets for data pertaining to a variety of industries).

[76] W. Nicholson II Price, Problematic Interactions between AI and Health Privacy, UTAH L. REV. 925, 926 (2021) ("Artificial intelligence reduces the already-weak power of deidentification' to protect health privacy by making it easier to reidentify patients, either individually or at scale.").

[77] "As artificial intelligence evolves, it magnifies the ability to use personal information in ways that can intrude on privacy interests by raising analysis of personal information to new levels of power and speed." Kerry, *supra* note 72.

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

[79] See the discussion in Part III *infra* concerning ostensibly public license plate data creating privacy harm.

products the individuals might be inclined to purchase or if they are exhibiting indicators of potential criminal activity based on who they might be meeting. In this scenario, privacy is decreased as individuals will not feel much ability to walk the public streets anonymously. Traditional case law would not support an expectation of privacy in public areas. Also, consent to recording might be implied from the visible cameras in public places. The building owners might argue they did not need consent to share the footage because they were sharing public data. In the absence of a law restricting facial recognition, perhaps in some cities there might not be much of a legal barrier to this facial recognition activity. In such instances, a broad express federal privacy law would be useful should gaps in existing law not cover particular privacy abuses.[80] As Professor Solove observes, "[i]n the United States, the default rule in privacy is generally that if something is not prohibited, then it is permitted."[81]

AI could also be used to abuse privacy via online misinformation. For example, in theory a user could prompt an AI system to generate untrue defamatory content about an individual. The AI system might comply if it is designed to provide the user with answers he desires, and might cite various sources falsely alleging that those sources support the false content. One source predicts that by 2026, ninety percent of online information will be bot generated.[82] Thus, it's certainly a concern that misinformation generated by AI systems could be propagated on the internet by massive herds of bots to abuse privacy or cause other societal harms, such as securities manipulation.

As noted earlier, Warren and Brandeis seemed to imagine the possibility of new machines to record scenes or sounds. They likely did not imagine AI and its increasing ability to predict human behavior, potentially invading the human mind. In the 2002 film Minority Report, a specialized

---

[80] This hypothetical bears some similarity to an automated gathering of license plate information: Electronic Frontier Foundation (EFF) and the American Civil Liberties Union Foundation of Southern California (ACLU SoCal) reached an agreement with Los Angeles law enforcement agencies in 2019 to turn over license plate data they indiscriminately collected on millions of law-abiding drivers in Southern California. *Victory! EFF Wins Access to License Plate Reader Data to Study How Law Enforcement Uses the Privacy Invasive Technology*, ELEC. FRONTIER FOUND. (Oct. 3, 2019), https://www.eff.org/press/releases/victory-eff-wins-access-license-plate-reader-data-study-how-law-enforcement-uses [https://perma.cc/7456-FH2C].

[81] Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 BOSTON U. L. REV. (2023) (*citing* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 135 (2017) ("Unlike EU law, U.S. law starts with a principle of free information flow and permits the processing of any personal data unless a law limits this action.").

[82] Europol Publications Office of the European Union (2022), *Facing Reality? Law Enforcement and the Challenge of Deepfakes: An Observatory Report from the Europol Innovation Lab*, https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf [https://perma.cc/ZE2A-V49R].

"precrime" police force arrested criminals before they committed a crime, with the assistance of three psychics. While this summer blockbuster seems far-fetched, police departments around the country use surveillance and predictive policing tools every day.

A predictive policing practice was found unconstitutional by the German Constitutional Court, finding they violated a broad right to informational self-determination.[83] This German decision, relying apparently on a broad information privacy related right, raises the question of whether the U.S. legal system would benefit from a similar privacy-focused broad constitutional right in efficiently safeguarding harms from emerging AI privacy abuses

Imagine a future where humans are increasingly commoditized in terms of their purchasing preferences and interests and where even their future behavior is predicted. Imagine AI systems grouping people into particular categories and deeming humans as highly predictable creatures, perhaps causing some perception in the population that there is very little sense of unique individual expression. Imagine a state of constant government and private actor surveillance to support this society. Perhaps the E.U. took the right approach in enacting its constitution with a broad privacy right (followed by the GDPR to further it) as such strong privacy rights seem a meaningful safeguard regarding rapidly advancing technology. These protections serve as a barrier to mass collection of personal data and automated decision making that could create a society where many individuals might perceive they are mere indistinct cogs within a machine.

b. Eavesdropping/Surveillance Has Been and Always Will Be an Issue

In 1890, Warren and Brandeis identified the issue of eavesdropping. Eavesdropping or surveillance is certainly an issue that will remain with humanity in perpetuity. Hacking or eavesdropping of private information has existed throughout human history (e.g., consider Caesar Ciphers of

[83] Molly Killeen, *German Constitutional Court Strikes Down Predictive Algorithms for Policing*, EURACTIV (Feb. 20, 2023) https://www.euractiv.com/section/artificial-intelligence/news/german-constitutional-court-strikes-down-predictive-algorithms-for-policing/ [https://perma.cc/PR5H-RU3K]; *see also* In re: Xarelto (Rivaroxaban) Products Liability Litigation, 2016 WL 3923873, at *13 (E.D. La., 2016) ("[The German Constitution contains a "right to informational self-determination."); for a general discussion of this German constitutional right and others, *see* Russell A. Miller, *A Pantomime of Privacy: Terrorism and Investigating Powers in German Constitutional Law*, 58 B.C. L. REV. 1545 (2017).

antiquity),[84] certainly including the period of 1890 through today, such as decrypting wartime communications during World Wars I and II. Interestingly, the first financially motivated electronic hacking occurred in 1862 where a stockbroker eavesdropped a telegraph message for insider trading purposes.[85] For many decades in the 1900s, telephones were very easy to tap, which was frequently done by law enforcement or private investigators investigating adultery or other issues. By 1965, however, one author notes that society seemed to accept wiretapping for national security as a necessary evil but perceived that its use for ordinary law enforcement was an abuse of power.[86]

Various examples of overreaching government surveillance are provided below to illustrate the need for strong information privacy protection from government actors.

The U.S. government has long been an antagonist of the privacy of American citizens. The mass data-collection after the September 11 terror attacks, leaked by Snowden is one modern example.[87] The Red Scare and Japanese-American internment targeted individuals after data collection.[88] United States intelligence groups surveilled civil rights and women's rights movements and organizations of the 1960s; the government initially justified this surveillance as a necessary evil for national security purposes, which eventually gave way to civil rights concerns.[89]

Marginalized communities, particularly communities of color, are disproportionately affected by these surveillance efforts, not only because these neighborhoods are overpoliced, but because physical privacy may be less accessible in low-income areas.[90]

The data collection practices of Immigration and Customs Enforcement ("ICE") are particularly offensive to privacy concerns. With minimal oversight, ICE utilizes social media, driver's license and DMV

---

[84] Caesar Cipher, PRACTICAL CRYPTOGRAPHY, http://practicalcryptography.com/ciphers/caesar-cipher/#:~:text=The%20Caesar%20cipher%20is%20one,become%20C%2C%20and%20so%20on [https://perma.cc/LR2M-AF8W] (last visited Mar. 6, 2023).

[85] April White, *A Brief History of Surveillance in America*, SMITHSONIAN MAGAZINE (April 2018), https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399/ [https://perma.cc/KWJ6-HSK3].

[86] *Id.* ("[By 1965, the normative political position in the United States was that wiretapping for national security was a necessary evil, whereas wiretapping in the service of the enforcement of criminal law—in, say, tax evasion cases or even in Mafia prosecutions, which was a big priority among American law enforcement starting in the 1960s—was outrageous and an abuse of power.").

[87] Volini, *supra* note 49, at 351; White, *supra* note 85.

[88] Barry Friedman, *Lawless Surveillance*, 97 N.Y.U. L. REV. 1143, 1159 (2022).

[89] *Id.*

[90] Dana Khabbaz, *Unmanned Stakeouts: Pole-Camera Surveillance and Privacy After the Tuggle Cert Denial*, YALE L. J. 105, 107-08 (2022).

data, and even home utilities to surveil.[91] After 9/11, ICE began tapping databases held by private data brokers, as well as state and local bureaucracies.[92] Perhaps most disturbing is the way in which ICE exploits vulnerability by leveraging people's trust in institutions such as state and local agencies, the DMV, even people's need for basic utilities such as water, gas, and electricity.[93]

Other agencies employ the same caliber of intrusive technology. The Department of Homeland Security's Fast Attribute Technology ("FAST") is able to identify who is safe to fly, and who is not, in real-time, based on behavior and mannerisms.[94] AI has exponentially empowered automated license plate readers ("ALPRs") by allowing any camera to become a license plate reader.[95] Law enforcement is developing an all-encompassing system of geolocation services by partnering with private vendors to purchase license plate readers and then exchanging their hoard of data with other government agencies.[96] A 2020 New York Civil Liberties report detailed that even privileged and confidential attorney-client communications are illegally recorded by contractors working for the government.[97]

On the world stage, the Snowden leaks put a spotlight on the United States' surveillance of civilians. One such program, Project Prism, collected direct communications sent to and from specificized targets, including email, phone communications, and search histories.[98] The revelations of the Snowden leaks led to distrust from European allies, and ultimately, in 2020, the European Court of Justice invalidated the E.U.-U.S. Privacy Shield program. The program allowed participating U.S. organizations to import data from the E.U., concerning E.U. subjects. The invalidation was a direct result of the invasiveness of U.S. privacy practices and concerns E.U. residents' data privacy was not protected from the U.S. government's gaze. The European commitment to prioritizing privacy

---

[91] Nina Wang, Allison McDonald, Daniel Bateyko & Emily Tucker, *American Dragnet: Data-Driven Deportation in the 21st Century*, CTR. ON PRIV. & TECH. (May 10, 2022), https://americandragnet.org [https://perma.cc/YFY7-AN7D]. ICE uses facial recognition technology to search the driver's license photographs of 1 in 3 (32%) of all adults in the U.S. Additionally, the agency uses driver's license data of 3 in 4 (74%) adults to track the movements of cars in cities home to nearly 3 in 4 (70%) adults.

[92] *Id.*

[93] *Id.* ICE obtained the new address of 3 in 4 (74%) adults when connecting the gas, electricity, phone or internet in a new home.

[94] Friedman, *supra* note 88, at 1154.

[95] *Id.*

[96] *Id.*

[97] Volini, *supra* note 49, at 360-61.

[98] *Id.* at 354.

prompted the E.U. and U.S. to agree to the Trans-Atlantic Data Privacy Framework, which addresses the concerns raised by the Court of Justice in 2020.[99]

In 2021, the Fourth Circuit ruled the Baltimore Police Department's ("BPD") aerial surveillance program unconstitutional.[100] BPD contracted with a private company to fly planes equipped with wide-angle cameras over Baltimore, for six months, twelve hours a day, with the purported purpose of solving criminal investigations.[101] The court in holding the program a violation of the Fourth Amendment and an invasion of people's reasonable expectation of privacy prohibited BPD from accessing data collected through the program.[102] It should be noted this is the same sort of technology and data collection practice used to surveil protected First Amendment assembly, such as Black Lives Matter protests.[103]

The above examples show that there is no shortage of government surveillance. Other parts of this article likewise reference private entity surveillance, such as online tracking without consent. It's important to look at both private entity and government surveillance because as noted in Part III below, the government can work with private entities to abuse privacy.

7. Privacy By Design Is a New Concept

Communication technologies tend to proliferate without privacy in mind and then are redesigned for privacy. In the 1890s, telegraphs were presumably easy to tap, literally tapping into the wire (hence, the term wiretapping persists today with regard to any electronic eavesdropping).[104] As noted above, telephone systems were likewise open for many years, making it easy for local police, private detectives and others to eavesdrop at will. This was a source of discomfort in society. As noted above, while there was some acceptance of eavesdropping for national security, widespread eavesdropping for domestic law enforcement created discomfort. For many years, the open nature of telephones supported a low expectation of privacy and the associated third party doctrine, which has been gradually eroding in recent years given that people now expect or

---

[99] U.S.-EU Trans-Atlantic Data Privacy Framework, CONGRESSIONAL RESEARCH SERVICE https://crsreports.congress.gov/product/pdf/IF/IF11613 [https://perma.cc/7PDA-PEP4].

[100] *Federal Appeals Court Rules Aerial Surveillance Program is Unconstitutional*, ACLU (June 24, 2021), https://www.aclu.org/press-releases/federal-appeals-court-rules-baltimore-aerial-surveillance-program-unconstitutional [https://perma.cc/PME9-GAWW].

[101] *Id.*

[102] *Id.*

[103] *Id.*

[104] Peter Tsai, *Security History: A Timeline of Early Electronic Eavesdropping*, SPICEWORKS (June 5, 2017), https://community.spiceworks.com/topic/1995160-security-history-a-timeline-of-early-electronic-eavesdropping [https://perma.cc/4L34-ARJC].

demand that a third party entity holding their emails or other data will not share the data with others absent some procedure such as a warrant or court order.[105]

Just like early telephones, much of the internet's early development was geared toward an open transparent system, requiring new technologies to redesign its function to provide privacy.[106] A major example of privacy retrofitting is that HTTP connections were very common until the Electronic Frontier Foundation in 2016 campaigned browser providers to use HTTPS (the "S" standing for secure). In my prior work, I describe these and other common protocols in some level of detail. Without going into great detail here, HTTP involves transmitting data with no encryption whatsoever such that all transmitted data is visible to an eavesdropper. HTTPS, in contrast, encrypts much of the transmitted data making it far more difficult for an eavesdropper to view the data.[107] In my prior work, I analogized HTTP to sending data on a postcard where the data (i.e., the message) is visible to anyone. I next analogized HTTPS to placing the data (i.e., the message) inside of an envelope, meaning an eavesdropper could see the sender/recipient info but not the encrypted data.[108]

The GDPR, effective May 2018, provided a concept of privacy and security by design and default for development of new IT products and services.[109] This GDPR requirement is a helpful concept to combat the natural human instinct to get a system up and running first before giving

---

[105] For discussion reflecting the erosion of the third-party doctrine, *see* Harvey Gee, *Last Call for the Third-Party Doctrine in the Digital Age After Carpenter?*, 26 B.U. J. SCI. & TECH. L. 286, 288–89 (2020) (noting that in Carpenter v. United States (2014) "the Supreme Court reframed the third-party doctrine by limiting and departing from a long tradition of deference paid to the [third-party] doctrine" and further questioned: "During this time of Big Data policing and aggressive policing, we need to ask ourselves some important questions about the government's use of surveillance technology. Do we want to live in a world where the government continuously tracks the location of our cell phone or smartphone, and knows about every online click and scroll we make, and when we make it? Do we mind that the Federal Bureau of Investigation and Immigration and Customs Enforcement routinely probes state driver's license databases with facial recognition technology in their investigations? Do we want to allow police departments to secretly use less than perfect and unprecedented facial recognition software in real-time video surveillance footage streaming from stores, buildings, streets, and police body cameras? Whatever happened to the Fourth Amendment's prohibition against unreasonable searches and seizures, and the warrant requirement?").

[106] The internet was initially designed by the military as a secondary communication method, and thus, may have initially contemplated privacy, but its subsequent development by universities and then the private sector largely ignored privacy, triggering redesign efforts upon spotting privacy issues. One source describes the NSA as discouraging the development of built-in encryption for the civilian used internet. *Id.*

[107] See Volini *supra* note 49, at 320-26.

[108] *Id.*

[109] Commission Regulation 2016/679, 2016 O.J. (LI 19) [GDPR] at Art. 25, available at https://eur-lex.europa.eu/eli/reg/2016/679/oj [https://perma.cc/XQY3-7VQT].

any thought to privacy or security, which can be observed historically with regard to many vulnerable technologies.[110] Implementing a broad federal right against information privacy abuse from government and private actors could further push the U.S. legal system closer to a privacy and security by design system.

8. Cybersecurity Did Not Exist in 1890, and Modern Tech Law Often Assesses Historical Physical World Concepts

a. More Data Can Be Hacked

Obviously, the concept of cybersecurity did not exist in 1890. Confidential or sensitive information, from 1890 to many years thereafter, was on paper and perhaps stored in a safe if it was especially sensitive. In 1890, there were certainly laws in place that would inhibit a government or private actor from invading one's home or cracking one's safe to access such information. Today various state and federal laws exist to prohibit hacking of personal information, such as the federal Computer Fraud and Abuse Act (CFAA) and its parallel state law cousins,[111] along with HIPAA and GLBA, concerning health and financial data, which both have express privacy and security rules. Also, state breach notification laws typically provide a broad duty to safeguard personal information.[112]

Two key differences between 1890 and today are that (1) an individual possesses arguably much more personal data on her computer(s) or third party platforms than would be present in an 1890s diary and (2) all of this personal data may be compromised by a remote bad actor thousands of miles away. Such hacking could have various motivations, commonly financial or identity theft, but other motivations exist.[113] Today,

---

[110] In addition to early telephone systems, various examples exist of launching new systems without privacy/security in mind. *See* Alison DeNisco Rayome, *Report: 40% of IT Security Leaders Don't Change Default Admin Password*, TECHREPUBLIC (Nov. 7, 2017), https://www.techrepublic.com/article/report-40-of-it-security-leaders-dont-change-default-admin-passwords/ [https://perma.cc/94H5-MFH5] ("A whopping 40% of IT security professionals said they don't employ the basic best practice of changing a default admin password.").

[111] *See e.g.*, the Illinois crime of computer tampering discussed in *People v. Janisch*, 966 N.E.2d 1034 (Ill. App. Ct. 2012).

[112] *See e.g.*, Data security, IL ST CH 815 § 530/45 ("A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.").

[113] *See* Samuel Chng, et al., *Hacker types, motivations and strategies: A comprehensive framework*, 5 COMPUTS. IN HUM. BEHAVIOR REPORTS (2022). Some motivations include: curiosity; financial; notoriety; revenge; recreation; ideology; and sexual impulses. *Id.* at 3. While not always exact, hackers often fit one (or more) of the following archetypes: Professionals, Petty Thieves, and Digital Pirates—varied levels of skill, all working to further criminal enterprise; Cyberpunks—low to medium skillset, wreaking havoc for fun; Insiders—disgruntled current or former-employees abusing access;

data is far more frequently stored electronically than on paper, and there is much more data available about an individual.[114]

b. Physical World Analogies

Interestingly, when assessing modern electronic privacy issues, courts often have to assess precedent addressing historical physical world concepts. For example, courts are currently split on whether compelling a defendant to disclose his computer password is a testimonial act under the Fifth Amendment.[115] They also often must assess Supreme Court rationale on how compelled disclosure of information can be like "telling an inquisitor the combination to a wall safe, [and] not like being forced to surrender the key to a strongbox."[116]

Comparison to physical world concepts is a helpful tool for lawyers and courts to assess modern technology issues given the challenge or impossibility of quickly understanding such technologies.[117] Given that analogies are by definition imperfect, however, criticisms of a particular physical world analogy would seem to arise fairly often. That being said, analogies will likely continue to serve as helpful analytical tools as attorneys will continue to struggle with understanding the under-the-hood mechanics of IT relative to privacy.

Hacktivists—hackers furthering a political agenda; Nation States—hackers working for a foreign government to destabilize or disrupt another nation; Online Sex Offenders—cyber predators and pedophiles. *Id.* at 4.

[114] *See, e.g.*, Riley v. California, 573 U.S. 373, 386 (2014) (noting that "[c]ell phones, however, place vast quantities of personal information literally in the hands of individuals" when distinguishing a cell phone search from a physical search).

[115] For a general discussion, see Kirstyn Watson, *Under Digital Lock and Key: Compelled Decryption and the Fifth Amendment*, 126 PENN ST. L. REV. 577 (2022).

[116] U.S. v. Hubbell, 530 U.S. 27, 43 (2000) (*quoting* Doe v. U.S., 487 U.S. 201, 210 (U.S. 1988) at FN 9: We do not disagree with the dissent that "[t]he expression of the contents of an individual's mind" is testimonial communication for purposes of the Fifth Amendment. *Post,* at 2352, n. 1. We simply disagree with the dissent's conclusion that the execution of the consent directive at issue here forced petitioner to express the contents of his mind. In our view, such compulsion is more like "be[ing] forced to surrender a key to a strongbox containing incriminating documents" than it is like "be[ing] compelled to reveal the combination to [petitioner's] wall safe").

[117] For example, in an amicus brief which I co-authored with Professor Karen Heart, we compared passive network scanning to simply standing on a public sidewalk looking at a building for open windows and we compared criminal network penetration as crawling into the open window without permission. Brief Of Karen Heart And Anthony Volini Of Ciplit As Amici Curiae In Support Of Respondent, Nathan van Buren v. United States of America, No. 19-783 (Sep. 2, 2020) https://www.supremecourt.gov/DocketPDF/19/19-783/151963/20200902140330536_19-783_Brief_Amici_Heart_and_Volini_CIPLIT.pdf [https:perma.cc/M8Zf-JZ25].

c. Privacy and Security Issues Often Overlap, But Are Distinct Concepts

As noted above, various statutes require security of personal data. Thus, the relationship between privacy and security is fairly obvious.

While privacy and security are typically overlapping complementary concepts, they are also distinct. For example, an organization could have the strongest cybersecurity controls available (e.g., encryption, firewalls, multi factor authentication, etc.), but still have enormous privacy exposure if it is collecting massive amounts of personal data in violation of one or more statutes or unlawfully disclosing such data to third parties. Therefore, today, it's helpful to separately assess privacy and security. This seems very different from 1890 where a person may have simply assessed privacy and security together, keeping private papers in her bedroom or perhaps a safe (or an attorney keeping client paperwork secure). The issue today of assessing IT security risks regarding personal data seems far more complicated than locking papers in a safe. Likewise, assessing privacy risks relative to unlawful collection or disclosure seems more complicated.

B. Auto-Feedback: Publication of Junk Spurs Creation of More Junk

Warren and Brandeis prophetically referenced the harm wrought by such invasions confined "to the suffering of those who may be the subjects of journalistic or other enterprise . . . The supply creates the demand. Each crop of unseemly gossip, thus harvested, becomes the seed of more, and, in direct proportion to its circulation results in a lowering of social standards and of morality."[118] Today, the massive proliferation of junk content, driven by money, is still arguably harmful to society. For example, society might be less likely to trust a legitimate, true news story given the presence of so much false news.[119] Also, the proliferation of false content invites conspiracy theories, which can generate an unhealthy overblown distrust of government and others. The result is that massive proliferation of junk content creates a more confused society.

A major similarity between 1890 and today is the goal of attracting readers to a page in order to expose them to advertisements. Viewing a web page is the modern equivalent of viewing a newspaper page. Accordingly, the same financial temptation to publish false, misleading, or scandalous

[118] Warren & Brandeis, *supra* note 1, at 196.

[119] Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1785 (2019) (describing the "liar's dividend," a concept where a liar is able to deny the truth of a story and referencing that "recent years have seen mounting distrust of traditional sources of news").

content persists. While publishing junk content persists, a key change today is the ability to track who has read particular content so that the platform continues to feed the same type of content to the user. According to the movie, *The Social Dilemma*, this tracking of content readership can have a polarizing effect on society in the realm of politics. For example, if advertisers observe an individual gravitates toward right-leaning content, they will continue to push similar content to her, resulting in a biased unbalanced newsfeed. Likewise, a left leaning individual may have a biased newsfeed of left leaning content. The biased information feeds thus exacerbate the already existing polarization on political issues. Accordingly, the particular problem with targeted junk is that it seems to increase polarization in society.[120] *The Social Dilemma* discusses this principle very well.[121] When a system detects that a user is drawn to a particular type of content and continues to feed her similar content, the result is that each user might be exposed to only one viewpoint or perspective, and the repeated exposure to the same perspective might amplify the user's adherence to that perspective.[122] A common goal of continually feeding targeted junk may involve keeping that user's eyes on the screen for as long as possible to expose that user to ads on the screen. Traditional newspapers had the same goal: publication of a hot story would keep consumers' eyes on the page to expose them to ads in the paper. So, just as in 1890, the temptation exists for a publisher to push misleading or patently false information in order to generate ad revenue.

1. Disinformation and Free Speech

Large scale disinformation is a legitimate concern given the ability of the Internet to effect large scale good or harm to society. The concern over disinformation harm apparently may be stimulating a movement toward restriction of free-speech rights. It seems antiquated to express the view "I disagree with what you are saying, but I defend your right to say it."[123]

---

[120] Frank Fagan, *Systemic Social Media Regulation*, 16 DUKE L. & TECH. REV. 393, 415 (2017-2018)(noting how social media tends to increase polarization, describing in part "network-selection behavior is entirely rational and helps explain why social networks systemically exhibit high levels of herding and polarization").

[121] THE SOCIAL DILEMMA (Exposure Labs 2020).

[122] For a variety of video lectures concerning algorithmic amplification of biases and other amplification problems *see* The Social Dilemma, *The Dilemma*, https://www.thesocialdilemma.com/the-dilemma/ [https://perma.cc/GV77-A2QG]; *see also* Tom Stafford, *How Liars Create the 'Illusion of Truth,'* BBC (Oct. 26, 2016), https://www.bbc.com/future/article/20161026-how-liars-create-the-illusion-of-truth [https://perma.cc/AP7F-DSN5] (discussing the impact of repetition on belief).

[123] *See* Young v. American Mini Theatres, Inc., 427 U.S. 50, 63 (1976) ("A remark attributed to Voltaire characterizes our zealous adherence to the principle that the government may not tell the citizen what he may or may not say. Referring to a suggestion that the violent overthrow of tyranny

Instead, private platform censorship is common, which may carry with it both positive and negative consequences as free speech law evolves.[124]

To combat the spread of false and harmful information, some might propose that private platforms should continue to police user content to prevent dissemination of false or undesirable speech. A private platform is likely not bound by the First Amendment, and thus, arguably has the right to police content. However, with a majority of adult Americans on Facebook, and a likely large concentration of working Americans on LinkedIn,[125] an alternative argument that social media is a necessity for users and might be treated as more akin to a public forum where free speech should not be silenced.[126] Given that the online world and physical world are increasingly merged together, careful thought should be given on how to appropriately safeguard free speech, even unpopular speech, to preserve a free society while at the same time stopping efforts to incite violence. Perhaps a high point for free speech was in 1977 when Jewish attorneys advocated for Nazis to march in Skokie, Illinois.[127] This was clearly an effort to protect First Amendment rights for highly offensive speech, perhaps based on an understanding that a fascist government would restrict offensive speech while a democratic government should not. Today feels different in that the private platform argument seems to favor censorship of undesirable or perhaps hateful speech and many Americans seem supportive of this trend.

Given free speech concerns, perhaps a better approach to combat mass distribution of false content might involve focusing on commercial actors regularly engaged in spreading such content, rather than focusing on individuals attempting to share their views. It seems that large scale commercially motivated disinformation campaigns may have contributed to

might be legitimate, he said: 'I disapprove of what you say, but I will defend to the death your right to say it.'").

[124] *See, e.g.*, Tzu-Chiang Huang, *Private Censorship, Disinformation and the First Amendment: Rethinking Online Platforms Regulation in the Era of a Global Pandemic*, 29 U. MICH. TECH. L. REV. 137 (2022).

[125] Pew Research Center estimated that in 2021 nearly 70% of adult Americans had used Facebook and 28% had used LinkedIn. John Gramlich, *10 Facts about Americans and Facebook*, PEW RESEARCH CENTER (Jun. 1, 2021), https://www.pewresearch.org/short-reads/2021/06/01/facts-about-americans-and-facebook/ [https://perma.cc/2ABF-WW4B].

[126] For a general discussion reflecting these conflicting principles, *see* Edward Mehrer III, *Freedom of Speech in the Age of Information and Misinformation*, 48 U. DAYTON L. REV. 65, 67 (2022) (proposing a "necessity for either: the Supreme Court to expand the public forum doctrine to apply to those social media platforms with a substantial market power, or Congress to amend Section 230 of the CDA to combat private viewpoint discrimination--especially on the basis of political matters").

[127] *See* David Goldberger, *The Skokie Case: How I Came to Represent the Free Speech Rights of Nazis*, ACLU (Mar. 2, 2020), https://www.aclu.org/issues/free-speech/rights-protesters/skokie-case-how-i-came-represent-free-speech-rights-nazis [https://perma.cc/Q7NA-CFPY].

Facebook's current practice of censoring private individuals, thereby reducing their online freedom of expression within their social circles.[128] That being said, stopping the flow of widespread misinformation would seem to require stopping dissemination by individual users, so there is no easy solution

2. Reducing Disinformation By Requiring Opt-in Consent?

The question then is how to reduce the creation of large-scale commercial misinformation at its source, rather than punishing individual users for disseminating the false content. Misinformation is typically created for commercial purposes, and false content that is likely to generate a strong emotional response, whether positive or negative, is more likely to go viral and generate revenue.[129] One possible mechanism to reduce misinformation is to require commercial actors to obtain opt-in consent from users before tracking engagement with the content.[130] Presumably, the vast majority of users would not opt-in, thereby potentially decreasing the financial incentive to generate the false content in the first place.

For example, commercial actors benefit from tracking user preferences and demographics with regard to views of their content.[131] If social media platforms required opt-in consent by default before such tracking could occur, then this might significantly deter the auto-feedback of junk content. In other words, most users would likely avoid opting in to low privacy settings. Essentially, if a publisher of junk is unable to detect whether user John Smith likes junk article #1, then the publisher is less likely to deliver similar junk article #2 to John Smith.

The problem with this proposal of following the GDPR's requirement of opt-in consent is that the entire business model of many platforms within the U.S. involves default settings that are not this protective of privacy, as targeted online ads are a multibillion dollar industry in the U.S.[132]

---

[128] The censorship is commonly referred to as Facebook jail. Kirsten Grind, *Inside 'Facebook Jail': The Secret Rules that Put Users in the Doghouse*, WALL STREET JOURNAL (May 4, 2021), https://www.wsj.com/articles/inside-facebook-jail-trump-the-secret-rules-that-put-users-in-the-doghouse-11620138445 [https://perma.cc/K8WH-C64Q].

[129] See Adam Mosseri, *Working to Stop Misinformation and False News*, FACEBOOK (Apr. 7, 2017) https://www.facebook.com/formedia/blog/working-to-stop-misinformation-and-false-news [https://perma.cc/3VY5-4QQWF] (discussing disruption of economic incentives as a key strategy to reduce misinformation).

[130] Opt-in consent involves affirmatively checking a box. *See* discussion *infra* Section D.2.

[131] *See, e.g.*, Tanya Kant, *Identity, Advertising, and Algorithmic Targeting: Or How (Not) to Target Your "Ideal User", MIT COLL. COMPUTING (Aug. 10, 2021), https://mit-serc.pubpub.org/pub/identity-advertising-and-algorithmic-targeting/release/2 [https://perma.cc/9KRE-6E6G].*

[132] In fact, using these US-developed settings in Europe has caused liability for Meta (Facebook). On September 2, 2022, Ireland's Data Protection Commission imposed one of the largest fines under the General Data Protection Regulation (G.D.P.R.) against Meta for its treatment of children's data on

Accordingly, social media platforms and other organizations may lobby strongly against privacy legislation requiring the opt-in consent generally required by the European Union's General Data Privacy Regulation.[133] Thus, a concern is that new legislation will likely continue to follow an opt-out model, and the goal may be to placate consumers by providing legal rights that might only be exercised by tech savvy consumers willing to spend time on their privacy settings, allowing big tech to continue profiting from the majority of consumers who do not read the fine print.[134]

3. Tech Platforms Misleading Consumers to Profit From Personal Information

One problem with the opt-out consent practice in the U.S. is that consumers do not spend time reading lengthy privacy policies and then make the decision of whether to opt-out of certain privacy settings.[135] Social media or other platforms tend to placate consumers with a false sense of privacy, while continuing to maximize revenues from acquiring personal information, using any available loopholes in the agreement. A famous example involves Google informing the public that they "don't sell your personal information to anyone."[136] This statement appeared technically true because Google was not selling personal data directly to third parties.[137] However, the statement likely misled consumers because they didn't understand that Google collected payments from third party advertisers for Google to direct ads to Google users with particular demographics collected by Google.[138] In another case, a court held that

Instagram, investigating Instagram in 2020 for making the accounts of children between the ages of 13 and 17 set to public by default, and for allowing teenagers with business accounts to make their email addresses and phone numbers public. Facebook alleged that it had updated these settings.

Adam Satariano**,** *Meta Fined $400 Million for Treatment of Children's Data on Instagram*, N.Y. TIMES (Sept. 5, 2022), https://www.nytimes.com/2022/09/05/business/meta-children-data-protection-europe.html [https://perma.cc/3CEE-ZUEY].

[133] *See* discussion *infra* Section D.2.

[134] Bennett Cyphers, Gennie Gebhart & Hayley Tsukayama, *Tech Lobbyists Are Pushing Bad Privacy Bills. Washington State Can, and Must, Do Better,* ELEC. FRONTIER FOUND. (Mar. 6, 2020), https://www.eff.org/deeplinks/2020/03/tech-lobbyists-are-pushing-bad-privacy-bills-washington-state-can-and-must-do [https://perma.cc/WK7L-DF7L].

[135] Solove, *supra* note 81, at 10.

[136] Bennett Cyphers, *Google Says it Doesn't 'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits it*, ELEC. FRONTIER FOUND. (Mar. 19, 2020), https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and [https://perma.cc/TZW9-2237].

[137] *Id.*

[138] *Id.* For example, Google can "[use] data to build individual profiles with demographics and interests, then lets advertisers target groups of people based on those traits."

Google misled consumers about its cookie tracking practices.[139] In another instance, Google was forced to pay a large settlement with forty state attorney generals for allegedly misleading of consumers with respect to location tracking.[140]

One does not need to look too hard to find other instances of tech platforms ignoring privacy or other legal rights in favor of maximizing growth with data collection, especially in the early development of those platforms. For example, in the early days of Facebook a nineteen-year-old Mark Zuckerberg is reported to have had the following conversation:

> Zuck: Yeah so if you ever need info about anyone at Harvard
>
> Zuck: Just ask.
>
> Zuck: I have over 4,000 emails, pictures, addresses, SNS
>
> [Redacted Friend's Name]: What? How'd you manage that one?
>
> Zuck: People just submitted it.
>
> Zuck: I don't know why.
>
> Zuck: They "trust me"
>
> Zuck: Dumb fucks.[141]

In a similar vein of ignoring rights of others, YouTube in its early days was alleged to have blatantly disregarded copyrights in favor of growth.[142]

The point of the above Google/Facebook/YouTube vignettes is that tech platforms often favor revenue and growth over privacy or other legal rights because the consumer data is so valuable, and these examples reflect such tendencies. Generally, it seems many organizations that are trying to grow often overlook either intentionally or accidentally any variety of legal requirements until they are forced to change their practices.

---

[139] FTC, *Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser,* FEDERAL TRADE COMMISSION (Aug. 9, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented-privacy-assurances-users-apples [https://perma.cc/UA4K-GMB3]; *See also* In re Google Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125 (3d Cir. 2015).

[140] Cecilia Kang, *Google Agrees to $392 Million Privacy Settlement With 40 States*, N.Y. TIMES (Nov. 14, 2022), https://www.nytimes.com/2022/11/14/technology/google-privacy-settlement.html [https://perma.cc/9K93-FWAA].

[141] Laura Raphael, *Mark Zuckerberg Called People Who Handed Over Their Data "Dumb F****",* ESQUIRE (Mar. 19, 2018), https://www.esquire.com/uk/latest-news/a19490586/mark-zuckerberg-called-people-who-handed-over-their-data-dumb-f/ [https://perma.cc/YW2L-8W8L].

[142] Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 518-19 (S.D.N.Y. 2010).

Certainly, regulatory fines and private lawsuits will push tech platforms toward stronger privacy for consumers. However, during this privacy evolution, tech platforms may still continue to favor revenue and absorb fines and civil damages as a cost of doing business. Perhaps statutes with the harshest penalties might be avoided (e.g., TCPA and BIPA)?[143] Regarding such harsh penalties, it will be interesting to see whether and to what extent courts might be willing to reduce certain damages under such statutes where defendants argue they are oppressive and unconstitutional.[144]

C. Tort Laws Continue to be Insufficient to Protect Privacy[145]

Warren and Brandeis noted that privacy has some superficial resemblance to the law of slander, libel, and defamation, but noted these areas only address damage to reputation and "extend[] the protection surrounding physical property to certain of the conditions necessary or helpful to worldly prosperity."[146] They further noted that the law does not generally award compensation to "mere injury to the feelings."[147] As discussed previously, feelings and privacy are linked, and it would seem today that a variety of privacy tort claims would fail if based on insubstantial emotional harm without any economic damages.

Also, tort claims may fail if they appear barred by another law. For example, some websites, such as cheatingreport.com,[148] invite site visitors to anonymously post defamatory content about individuals (e.g., cheating, drug use, etc.) and avoid liability by using Section 230 of the Communication Decency Act as a shield and portraying themselves as

---

[143] *See* Telephone Consumer Protection Act, 47 U.S.C. § 277(b)(3)(B)(providing statutory damages of at least $500 per violation); Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/20 (providing that a prevailing party can recover from "a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater").

[144] For example, in Wakefield v. ViSalus, Inc., 51 F.4th 1109, 1125 (9th Cir. 2022), the Ninth Circuit remanded to the district court the issue of whether an aggregate TCPA award of $925,220,000 was severe and oppressive and, if so, by how much the cumulative award should be reduced.

[145] *See* Deidré Keller, *Copyright to the Rescue: Should Copyright Protect Privacy?*, 20 UCLA J.L. & TECH. [i] (2016) for an in depth discussion on these issues.

[146] Warren & Brandeis, *supra* note 1, at 197.

[147] *Id.*

[148] *Removal*, CHEATING REPORT, https://www.cheatingreport.com/removal/ [https://perma.cc/2TWV-YVWG] (including the text, "We are protected by the Communications Decency Act or 'CDA'. In a nutshell, we don't publish the content but rather our users submit articles and we simply approve them. The only thing we look for when approving or denying a submission is if it violates federal or state laws. We don't fact check and we don't check for copyrighted images or text. If you have a complaint with an article it can be removed via a court order or by providing us with information that violates federal or state law. We also will remove a post due to revenge p**n (but we don't allow that type of material either, so . . . shouldn't ever happen). Other than that, that's pretty much it. You can't name us in a complaint, if you do, we won't be held liable in court. We're not the publishers . . . ").

merely neutral conduits of information.[149] For example, a disgruntled ex-boyfriend might anonymously post defamatory content about his ex-girlfriend. While using the CDA as a shield, some of these platforms might offer to remove the content if the victim pays a fee and may also earn advertising revenue from generating traffic to the site.

A similar situation occurred with mugshots. Illinois, and other states,[150] outlawed websites from charging fees for removing published online mugshots from arrests.[151] Prior to such legislation, these sites appeared protected from tort liability, claiming the mugshot publications fell under the protection of news reporting.

Besides the concept of privacy torts being barred by other laws, one author has also observed that a desire to reduce tort liability can actually diminish privacy:

Tort law can pressure property owners, employers, and consumer product manufacturers into engaging in more surveillance. Tort law can pressure colleges, employers, and others into more investigation of students', employees', or customers' lives. Tort law can pressure landlords, employers, and others into more dissemination of potentially embarrassing information about people. Tort law can require people to reveal potentially embarrassing information about themselves. Technological change is likely to magnify this pressure still further. Yet this tendency has gone largely undiscussed.[152]

Returning to the CDA shielding privacy abuse, Congress could contemplate amendments to the CDA that would inhibit commercially motivated privacy abuses akin to online extortion of individuals in the mugshot or defamation contexts. But, perhaps a simpler solution is enacting a broad federal right of protection from information privacy abuse, which could be used to invalidate use of the CDA as a shield for privacy abuse. This concept of a broad express constitutional privacy right

---

[149] *See* Patricia Spiccia, *The Best Things in Life Are Not Free: Why Immunity Under Section 230 of the Communications Decency Act Should Be Earned and Not Freely Given*, 48 VAL. U. L. REV. 369 (2013).

[150] *See Mug Shots and Booking Photo Websites*, NATIONAL CONFERENCE OF STATE LEGISLATURES, https://www.ncsl.org/technology-and-communication/mug-shots-and-booking-photo-websites [https://perma.cc/W57E-3L62] (describing various states that prohibit sites from charging a fee for mugshot removal).

[151] See 815 Ill. Comp. Stat. 505/2QQQ (generally outlawing the business practice of soliciting money for removal of online mugshots).

[152] Eugene Volokh, *Tort Law vs. Privacy*, 114 COLUM. L. REV. 879, 881 (2014).

overriding a statute can be observed in California case law, a concept discussed again in Part III below.[153]

D. The Concept of Consent: 1890 and Today

1. An Author's Right to Publish Content or Keep it Private

Regarding consent, Warren and Brandeis discussed an individual's right to choose which thoughts she wishes to publish versus those she wishes to keep private: "[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,"[154] and "he can never be compelled to express them (except when upon the witness-stand) . . . generally retain[ing] the power to fix the limits of the publicity which shall be given them."[155] Expanding on this concept, they wrote "[t]he same protection is accorded to a casual letter or an entry in a diary and to the most valuable poem or essay, to a botch or daub and to a masterpiece. In every such case the individual is entitled to decide whether that which is his shall be given to the public. No one has the right to publish his productions in any form, *without his consent*."[156]

Certainly, an individual's rights today regarding what writings she would like to publish seems generally similar to 1890 (but consent to online collection and sharing of personal information today seems a very different issue).

2. Consent for Collecting and Sharing Personal Information

The collection of private information harvested from an individual and shared among advertisers or data brokers is certainly a key issue related to consent. Today, a major difference between the U.S. and Europe is that, as referenced previously, the E.U. generally requires opt-in consent for data collection, while the patchwork of laws within the U.S. generally require merely opt-out consent.[157] Opt-out consent generally involves a pre-checked box, where a user needs to uncheck the box in order to ensure privacy (e.g., prevent sharing of personal data with others). In contrast, the GDPR generally requires opt-in consent for collection and sharing of

---

[153] *See* Am. Acad. of Pediatrics v. Lungren, 940 P.2d 797, 831 (Cal.1997) (finding that a parental notice statute in the abortion context violated California's constitutional right to privacy).

[154] Warren & Brandeis, *supra* note 1, at 198.

[155] *Id.* at 198.

[156] *Id.* at 199 (emphasis added).

[157] *See* Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338; California Consumer Privacy Act of 2018, CAL. CIVIL CODE §§ 1798.100 - 1798.199.100; and American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

personal data, where the user is conspicuously presented with the question of whether she agrees to data collection and sharing.

While laws within the U.S. have been influenced by GDPR, it seems questionable whether the U.S. would ever move toward an opt-in system given the high value of personal data and the lobbying power of tech platforms when new privacy laws are created.[158] Further, just as tech platforms are economically addicted to personal data, American consumers might be addicted to receiving free or low cost products or services in exchange for their data.[159] All that being said, a broad privacy law could contemplate an opt-in system akin to Europe. Considering improved consent mechanisms seems worthwhile as Professor Solove has recently described consent as often a legal fiction given that "[i]ndividuals are often pressured or manipulated, undermining the validity of their consent," or are ill-equipped to understand what particular algorithms will do with their personal data.[160] He discusses that the E.U. approach to consent is far superior to the U.S. system in terms of promoting privacy, but notes it still has its problems. Solove recommends that the law embrace (continue to embrace?) some amount of personal decision making and autonomy regarding their data combined with strong guardrails to protect against harms.[161]

Given the economic addiction to personal data in the U.S., we will continue to see an interesting game play out where tech platforms attempt to placate consumers with a false sense of privacy while exploring ways to continue profiting from personal data.[162] In some instances, platforms could collect data without consent by conceivably bypassing consumer privacy controls, essentially ignoring an instruction from the consumer not to track her activities. For example, Apple faced an allegation in 2022 that its devices continue to track user activity even when the user has selected to

---

[158] See Hayley Tsukayama, *Virginia's Weak Privacy Bill is Just What Big Tech Wants*, EFF (Feb. 25, 2021), https://www.eff.org/deeplinks/2021/02/virginias-weak-privacy-bill-just-what-big-tech-wants [https://perma.cc/WG8N-2WKP] (asserting that a Virginia privacy bill was authored by an Amazon lobbyist).

[159] See also Solove, *supra* note 81, at 20, for a description of the internet as presenting a grand bargain to people - free goods and services in exchange for personal data, citing Chris Jay Hoofnagle and Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price,* 61 UCLA L. REV. 606, 606 (2014).

[160] Solove, *supra* note 81, at 2.

[161] Solove*, supra* note 81*,* at 5-6.

[162] Ashley Belanger, *Facebook Users Sue Meta for Bypassing Beefy Apple Security to Spy on Millions*, ARS TECHNICA (Sep. 22, 2022), https://arstechnica.com/tech-policy/2022/09/lawsuits-say-meta-evaded-apple-privacy-settings-to-spy-on-millions-of-users/ [https://perma.cc/8ZZM-UT5F].

turn off such tracking.[163] Likewise Facebook has faced an allegation that it sidestepped Apple's privacy protections by directing Facebook users to its own in-app browser rather than Apple's default browser that had the privacy protections.[164] According to one source, "[a]fter Apple updated its privacy rules in 2021 to easily allow iOS users to opt out of all tracking by third-party apps, so many people opted out that the Electronic Frontier Foundation reported that Meta lost $10 billion in revenue over the next year."[165] Thus, it would seem that Facebook needed to take some action to gain back some of the $10 billion in lost annual revenue from Apple's privacy protection, apparently by bypassing Apple's privacy protection.

Certainly, another concern is covert tracking by platforms outside of the U.S. or E.U..[166] The popular app Tik-Tok, for example, allegedly tracks users even while they're not using the app, and while regulators will certainly attempt enforcement against such platforms, it's conceivable that it might be challenging to get many such platforms to submit to U.S. or E.U. jurisdiction with regard to privacy practices.[167] Granted Tik-Tok has such a large international presence, it appears willing to submit to U.S. or E.U. jurisdiction; although smaller entities in some parts of the world may not submit to U.S. or E.U. jurisdiction.

In other instances, a platform might make privacy settings difficult to navigate.[168] Further, an organization could disclose that it doesn't share personal data with third parties with an exception for affiliates, meaning an assortment of commonly owned organizations can share the data and track

---

[163] Thomas Germain, *Apple Is Tracking You Even When Its Own Privacy Settings Say It's Not New Research Says*, GIZMODO (Nov. 8, 2022), https://gizmodo-com.cdn.ampproject.org/c/s/gizmodo.com/apple-iphone-analytics-tracking-even-when-off-app-store-1849757558/amp [https://perma.cc/5YAU-VCSR].

[164] Belanger, *supra* note 165; see also Bailey Schulz, *Facebook Sued Over Allegations It Sidestepped Apple's Privacy Protections to Collect User Data*, USA TODAY (Sept. 22, 2022), https://www.usatoday.com/story/tech/2022/09/22/facebook-meta-lawsuit-apple-privacy-data/8080826001 [https://perma.cc/EL5D-WRQQ].

[165] Belanger, *supra* note 165.

[166] Thomas Germain, *How TikTok Tracks You Across the Web, Even If You Don't Use The App*, CONSUMER REPORTS (Sep. 29, 2022), https://www.consumerreports.org/electronics-computers/privacy/tiktok-tracks-you-across-the-web-even-if-you-dont-use-app-a4383537813/ [https://perma.cc/DA7E-Y67R].

[167] See Ryan Browne, *TikTok Could Face a $29 Million Fine in the UK for Failing to Protect Kids' Privacy*, CNBC (Sep. 26, 2022), https://www.cnbc.com/2022/09/26/tiktok-may-face-29-million-uk-fine-for-failing-to-protect-kids-privacy.html [https://perma.cc/MJY2-L3XG].

[168] See Matthew Keys, *A Brief History of Facebook's Ever-changing Privacy Settings*, MEDIUM (March 21, 2018), https://medium.com/@matthewkeys/a-brief-history-of-facebooks-ever-changing-privacy-settings-8167dadd3bd0 [https://perma.cc/9E59-K8NA] (noting that Facebook has a history of delivering confusing privacy settings).

activity across multiple platforms, and the consumer might not understand the data sharing that she has consented to.

The business model of profiting from personal data seems fairly unworkable in the E.U. given the GDPR's protections. For example, a $414 million (390 million euros) fine was levied against Meta in 2022, after European Union regulators found the company had illegally forced users to accept personalized ads.[169] It's possible that Meta read the tea leaves in recent years, with its name change and pursuit of its new business model,[170] potentially realizing that profiting from personal data might be unsustainable should U.S. privacy rights become increasingly GDPR–like.

Accordingly, a broad federal privacy law that requires opt-in consent and privacy by default,[171] akin to the GDPR, would be one solution to inhibit the various privacy abuses. Given the enormous lobbying power of tech platforms and multibillion dollar online economy based on personal data, it would seem that informed consumers would have to push hard for such a fundamental change in online U.S. privacy protection. Accordingly, a broad constitutional protection from information privacy abuse might be more easily attained than requiring opt-in consent.

E. Copyright Law Is Still Insufficient To Protect Privacy

As a reminder, a central observation of this article is that in 1890 and today various areas of law are inadequate to protect privacy (hence, a broad express privacy right is needed). Warren and Brandeis' observations on copyright law's inability to protect privacy circa 1890 still seems very much on point today.

---

[169] Adam Satariano, *Meta's Ad Practices Ruled Illegal Under E.U. Law*, N.Y. TIMES (Jan. 4, 2023), https://www.nytimes.com/2023/01/04/technology/meta-facebook-eu-gdpr.html [https://perma.cc/RVJ6-PAVS] (noting Ireland's data privacy board, Meta's primary EU regulator (Meta is headquartered in Dublin), determined the lengthy terms-of-service agreement impermissibly put users to a choice between allowing collection of their data for personalized ads, or using the social media services at all).

[170] Gemma Ryles, *Facebook's Decision to Change Its Name to Meta Explained*, TRUSTED REVIEWS (NOV. 1, 2021), https://www.trustedreviews.com/news/facebooks-decision-to-change-its-name-to-meta-explained-4176812 [https://perma.cc/87GN-G3QE] ("Mark Zuckerberg, the founder of Facebook, claimed that the renaming was to signal that the company was branching out and was linked to more than one product."); *see also* Mike Isaac, *Facebook Renames Itself Meta*, N.Y. TIMES (Nov. 10, 2021), https://www.nytimes.com/2021/10/28/technology/facebook-meta-name-change.html [https://perma.cc/9RX3-C7JP] ("At the same time, renaming Facebook may help distance the company from the social networking controversies it is facing, including how it is used to spread hate speech and misinformation.").

[171] Council Regulation 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, art. 25. ("GDPR").

They discussed how unlike copyright law, where the value of the copyright is to profit from publication, privacy concerns the peace of mind or relief to prevent any publication at all. So, they discuss how a privacy right does not seem to fit within property law.[172]

Warren and Brandeis opined when "[a] man records in a letter to his son, or in his diary, that he did not dine with his wife on a certain day,"[173] no one should have the right to publish this information to the world, even if obtained rightfully.[174] This seems an interesting parallel to Senator Dick Durbin's questions addressed to Mark Zuckerberg:

Mr. Zuckerberg, would you be comfortable sharing with us the name of the hotel you stayed in last night?" Durbin asked. "Um, uh, no," Zuckerberg replied.

"If you messaged anybody this week, would you share with us the names of the people you messaged?" asked Durbin. "Senator, no, I would probably not choose to do that publicly here," said Zuckerberg. "I think that may be what this is all about: your right to privacy—the limits of your right to privacy, and how much you give away in modern America in the name of, quote, connecting people around the world," added Durbin. "A question, basically, of what information Facebook is collecting, who they're sending it to, and whether they ever asked me in advance my permission to do that.[175]

Warren and Brandeis identified privacy issues regarding publishing *contents* of a letter versus publication of a list of letters identifying sender and recipient without the contents.[176] A list of letters identifying to and from information versus the actual contents of the letters relates directly to the modern concept of routing information, which is sometimes described as metadata, versus content (e.g., routing information might involve which websites a person visited or which telephone number an individual sent a text to, while content would be the words used in an email or a text

[172] Warren and Brandeis, *supra* note 1, at 200-201.

[173] *Id.* at 201.

[174] *Id.*

[175] *Durbin Questions Facebook CEO Mark Zuckberg*, SENATOR DICK DURBIN, (Apr. 10, 2018) https://www.durbin.senate.gov/newsroom/press-releases/durbin-questions-facebook-ceo-mark-zuckerberg [https://perma.cc/Y4US-ZHEN].

[176] Warren & Brandeis, *supra* note 1, at 201.

message).[177] Courts have noted that such metadata can reveal significant details of someone's life.[178]

Warren and Brandeis pointed out the shortcoming of copyright law in that it would prevent reproduction of the works but not a description of the works.[179] This copyright principle still operates today.

Warren and Brandeis also described the shift in copyright law in that it had expanded to protect writings without regard to their pecuniary value or merit. They contemplated the possibility of future profits if someone later becomes famous, but noted that the law did not protect this scenario of the possibility of future profits under property law.[180]

Today, it's still accurate that property law, including copyright law, is largely ineffective to protect personal information.[181] Perhaps it's also true today that a small amount of personal information about one individual (e.g., biographic information combined with shopping preferences) might have a relatively small amount of commercial value. However, aggregated personal data of thousands or millions of consumers certainly has a much greater value. Thus, Warren and Brandeis' reference to a diary entry of whether a husband and wife dined together on a particular day could be very valuable for restaurant marketing, particularly if the information included data on where a large number of people dined on a particular date and what foods or beverages they enjoyed.

In another scenario, if an anonymous bad actor posted a picture or video of a victim in some embarrassing or defamatory manner, the victim might not be the copyright owner of the picture or video. For this reason, other theories outside of copyright would need to be explored, such as various privacy torts or use of likeness statutes provided that the platform of the abusive content is not protected by Section 230 of the Communications Decency Act.

---

[177] *See* United States v. Moalin, 973 F.3d 977, 991 (9th Cir. 2020) (describing metadata as including "comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number . . .)").

[178] *Id.* ("According to the NSA's former general counsel Stewart Baker, '[m]etadata absolutely tells you everything about somebody's life. . . . If you have enough metadata you don't really need content.'")

[179] Warren & Brandeis, *supra* note 1, at 201–202.

[180] *Id.* at 204.

[181] For a general discussion of copyright law's continuing shortcomings with protecting privacy, *see* Deidre Keller, *Copyright to the Rescue: Should Copyright Protect Privacy?*, 20 UCLA J.L. & TECH. 1 (2016); for a general discussion of how ownership of personal data does not seem adequate as a legal mechanism for personal data protection, *see* Tanith L. Balaban, *Comprehensive Data Privacy Legislation: Why Now is the Time*, 1 CASE W. RES. J.L. TECH. & INTERNET 1, 20–21 (2009).

F. Contract and Fiduciary Law Is Likely Still Insufficient To Protect Privacy

Warren and Brandeis noted cases from the 1800s that recognized breach of implied contract and breach of trust as a way to have liability or justify injunction as an alternative to property law theories.[182] Warren and Brandeis observed that "[the] process of implying a term in a contract, or of implying a relationship of trust, . . . is nothing more nor less than a judicial declaration that public morality, private justice, and general convenience demand the recognition of such a rule. . . ."[183]

Warren and Brandeis observed that legal theories based on breach of contract or breach of trust require some relationship between the parties, and oftentimes a breach of privacy involves strangers who have no relationship to create contractual or fiduciary rights. In discussing new advances in photography allow taking pictures surreptitiously,[184] they noted that the doctrines of implied contract and trust are thus inadequate where the photographer and publisher are strangers. They observed the law of tort must be resorted to, and they embraced a right to an "inviolate personality" from a torts perspective.[185] Certainly today, privacy tort law and even criminal privacy laws have evolved to capture privacy harms from surreptitious recordings.[186]

Warren and Brandeis also discussed trade secret law as inadequate to protect privacy because trade secret misappropriation claims typically involve some relationship between the parties, a relationship not present with surreptitious recordings.[187] As a side note, I would add there is a slight parallel between one aspect of trade secret law and privacy: it's well settled that allowing publication of a trade secret, such as through failure to maintain reasonable efforts at secrecy, can compromise trade secret protection. In a similar vein, a person publicizing personal information on a certain topic may compromise his ability to maintain privacy on that topic.[188]

Warren and Brandeis summed up that the rights of privacy don't fit squarely with rights from contract or special trust.[189] Thus, the principle

---

[182] Warren & Brandeis, *supra* note 1, at 208–09.

[183] *Id.* at 210.

[184] Warren & Brandeis, *supra* note 1, at 211.

[185] *Id.*

[186] Carol M. Bast, *Privacy, Eavesdropping, and Wiretapping Across the United States: Reasonable Expectation of Privacy and Judicial Discretion*, 29 CATH. U. J. L. & TECH 1, 1 (2020) (discussing civil and sometimes criminal consequences that may be available under various relevant laws).

[187] Warren & Brandeis, *supra* note 1 at 212.

[188] *See infra* Hulk Hogan/Terry Bollea discussions.

[189] Warren & Brandeis, *supra* note 1 at 213.

protecting personal writings and products of the intellect or emotions, while insufficient to protect privacy, might seem more germane to privacy than contract or fiduciary law.

G. Publication of Information That is Newsworthy or of General Interest May Still Override Privacy Interests

Warren and Brandeis observed a legal principle that endures to this day: a "right of privacy does not prohibit publication of matter which is of public or general interest" discussing the qualified privilege of comment and criticism on matters of public and general interest and noting the difficulties of applying such a rule.[190] One somewhat modern case reflecting this principle involved a leaked sex tape of Terry Bollea (known professionally as Hulk Hogan), where a court refused to enjoin Gawker Media from continuing to post a sex tape featuring wrestler Hulk Hogan on its website.[191] Essentially, Gawker's First Amendment rights trumped the wrestler's right of privacy given that Hogan, a public figure, had previously published commentary on his sex life.[192]

Warren and Brandeis in 1890 provided a principle consistent with this ruling: "There are persons who may reasonably claim as a right, protection from the notoriety entailed by being made the victims of journalistic enterprise. There are others who, in varying degrees, have renounced the right to live their lives screened from public observation."[193] As Warren and Brandeis discussed, someone running for public office would certainly seem to fit this principle as well, as details of her private life might become a matter of general interest in terms of the public deciding whether to vote for her.

Warren and Brandeis noted another enduring principle, "[t]he general object in view is to protect the privacy of a private life,"[194] but the right to privacy is not invaded where the information is necessary to maintain or defend a suit.[195] Certainly today, where private information is relevant to claims or defenses in litigation, it is subject to discovery.[196]

---

[190] *Id.* at 214.

[191] Gawker Media, LLC v. Bollea, 129 So.3d 1196, 1200-01 (Fla. Dist. Ct, App. 2014).

[192] *Id.*

[193] Warren & Brandeis, *supra* note 1, at 215.

[194] *Id.* at 215.

[195] *Id.* at 216.

[196] *See* 65 Cal.Rptr.3d 456, 468, 154 Cal.App.4th 1233, 1251 (Cal. App. 3 Dist. 2007) noting that even information subject to California's constitutional right to privacy may be discoverable: "the person seeking discovery of material protected by the constitutional right to privacy 'has the burden of making a threshold showing that the evidence sought is 'directly relevant' to the claim or defense.'" *citing Harris v. Superior Court* (1992) 3 Cal.App.4th 661, 665, 4 Cal.Rptr.2d 564.

III. A PATH FORWARD

A. Enacting a Broad and General Right to Information Privacy

Given privacy concerns increasing as technology advances, stronger legal protections are desirable as neither government nor businesses can be trusted to respect privacy. As noted above, the natural tendency for businesses is to favor profits over privacy interests. Likewise, government agencies, particularly law enforcement agencies, have a natural priority to detect and prosecute terrorism and other crimes more so than focusing on individual privacy rights. The Legislative and Judicial branches can intervene to keep these tendencies in check. Regarding consumer privacy, the FTC has been pushing for a broad privacy law since 2000, and a former FTC director of consumer protection has noted that Congress's failure to act has relinquished privacy leadership to Europe and California and, like Professor Solove, has noted that many existing statutes have overreliance on an ineffective notice and consent approach to privacy protection.[197] Thus, a new approach is needed.

A path forward might involve enactment of a broad express federal right of protection against information privacy abuses committed by government or private actors, either with or without a private right of action.[198] With enough support, perhaps such a law might take the form of a constitutional amendment,[199] which would of course be arduous to enact,[200] but the benefits could be significant. Less preferably, a broad statutory right

---

[197] Jessica Rich, *After 20 years of debate, it's time for Congress to finally pass a baseline privacy law*, Brookings (Jan. 14, 2021), https://www.brookings.edu/blog/techtank/2021/01/14/after-20-years-of-debate-its-time-for-congress-to-finally-pass-a-baseline-privacy-law/ [https://perma.cc/DH6L-76NS]

[198] California's constitutional privacy protection extends to both private and government actors as noted in Saleh v. Nike, Inc., 562 F.Supp.3d 503, 524 (C.D. Cal. 2021): "Article I, section 1 of the California Constitution declares privacy an inalienable right of the people of California. Cal. Const. Art. I, § 1. The right, in many respects broader than its federal constitutional counterpart, protects individuals from the invasion of their privacy not only by state actors but also by private parties.'' (*citing* Leonel v. Am. Airlines, Inc., 400 F.3d 702, 711 (9th Cir. 2005)).

[199] Shaun G. Jamison, *Creating a National Data Privacy Law for the United States*, 10 CYBARIS INTELL. PROP. L. REV. 1, 33 (2019) (suggesting a constitutional amendment but noting the difficulties in enacting one) (citing *Constitutional Amendment Process*, NATIONAL ARCHIVES) (last viewed March 7, 2023), https://www.archives.gov/federal-register/constitution [https://perma.cc/G2PB-TUFX].

[200] *See The Amendment Process*, NATIONAL ARCHIVES https://www.trumanlibrary.gov/education/three-branches/amendment-process [https://perma.cc/78P8-QMTC] (describing the amendment process as "very difficult and time consuming: A proposed amendment must be passed by two-thirds of both houses of Congress, then ratified by the legislatures of three-fourths of the states") and *see* Drew Desilver, *Proposed Amendments to the U.S. Constitution Seldom Go Anywhere*, PEW RESEARCH CENTER (Apr. 12, 2018), https://www.pewresearch.org/fact-tank/2018/04/12/a-look-at-proposed-constitutional-amendments-and-how-seldom-they-go-anywhere/ [https://perma.cc/7DX2-QTUX].

could be pursued.[201] Such a broadly defined law might be useful to fill gaps not addressed by existing laws, such as cases where claims under California's constitutional right to privacy survived dismissal while various other claims failed.[202] It would seem worthwhile to explore E.U. cases where broadly defined rights in the E.U.'s constitution, or national laws within the E.U., have protected information privacy.[203] Likewise, it may be helpful to explore case law from California and various other states having express constitutional privacy protection, assessing whether and to what extent a broad state constitutional right supported plaintiffs' claims where other statutory or common law claims were not available.[204]

Regarding broad scope, a constitutional guarantee against "information privacy abuse" would be flexible language requiring judicial interpretation much like the flexible language seen in the Bill of Rights/First through Tenth Amendments (e.g., the Eighth Amendment's prohibition of "cruel and unusual punishment" or the Fourth Amendment's prohibition of "unreasonable searches and seizures"). In contrast, the Eleventh through Twenty Seventh Amendments tend to have more concrete language (e.g., the Twenty-Sixth Amendment guaranteeing the right to vote to persons eighteen years of age or older or the Thirteenth Amendment's general abolition of slavery or involuntary servitude). It would seem then that an information privacy amendment would simply express what many

---

[201] Granted, a broad statutory right might create potential conflicts with other statutes and thus interpretation challenges. *See* Steve R. Johnson, *When General Statutes and Specific Statutes Conflict*, 57 ST. TAX NOTES 599 (Jul. 12, 2010), https://ir.law.fsu.edu/articles/304 [https://perma.cc/BZ53-TTWV] (discussing interpretation of conflicting statutes, such as more recent statutes overriding prior statutes, but more specific statutes outweighing general statutes); further, amending the FTC Act to broadly protect privacy might not be as efficient given the FTC's jurisdictional limitations and other issues. *See* Robert Gellman, *Can Consumers Trust the FTC to Protect their Privacy*, ACLU, (Oct. 25, 2016), https://www.aclu.org/news/privacy-technology/can-consumers-trust-ftc-protect-their-privacy [https://perma.cc/SX4Z-2YU3].

[202] *See* In re Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125 (3d Cir. 2015) (ruling that dismissal of a variety of federal and state claims was appropriate but that plaintiffs' California Constitutional privacy claim should survive dismissal); *see also* In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589 (9th Cir. 2020) (affirming the district court's dismissal of the SCA, breach of contract, and breach of implied covenant claims, but ruling that Plaintiffs adequately pleaded their remaining claims (e.g., California Constitutional invasion of privacy claim and common law intrusion upon seclusion)).

[203] Killeen, *supra* note 83.

[204] *See* David A. Carrillo, Stephen M. Duvernay, Rodolfo E. Rivera Aquino & Brandon V. Stracener, *California Constitutional Law: Privacy*, 59 SAN DIEGO L. REV. 119, 121 (2022) (asserting that the strength of the California Constitution's privacy protection has weakened over time, noting that "voters intended the new constitutional privacy right to shield personal privacy and guard against the unnecessary collection or misuse of private information. But while technological advances since 1972 have only sharpened [privacy] concerns, California courts have moved constitutional privacy doctrine backward").

courts in various contexts might imply from the Bill or Rights and/or the Fourteenth Amendment.

In 1890, Warren and Brandeis observed that privacy is an important right and then they essentially created an implied right to privacy given the gaps in existing laws that failed to squarely address it . Today, the U.S. legal system has the same gap: there is no broad, general, express right to information privacy. As a result, in past decades, state and federal statutes have sprung up in a variety of sectors in an effort to fill this gap. Today it would make sense to take a cue from Europe and have an express broad privacy right equivalent to the E.U.'s constitution. This would certainly create greater harmonization with Europe, which might be helpful for facilitating data transfers between the United States and E.U.. And, perhaps a broad privacy right could exist as a central rule upon which other rules are built (and potentially reduce the need for additional detailed statutes if particular harms could be addressed by such a broad constitutional right). It would be interesting to see whether a broad right might inspire courts to limit the ability of one entity, or affiliated entities, from holding too much personal data if a court were to rule this creates too much potential for abuse.

Regarding the lesson from 1890 that new technology advances create new privacy issues, it seems likely that AI proliferation will create new and unforeseen privacy harms, a broad gap-filling law would seem helpful for courts to restrict new privacy harms without waiting for Congress to react and then negotiate compromises with states on issues such as enforcement and preemption.[205] With a broad constitutional right, courts could at least restrict egregious privacy abuses with an injunction against commercial or private actors, while various state laws could provide additional remedies. Furthermore, state lawmakers could consider whether violating such a constitutional right should support a private right of action under state law.

Making such a federal right express rather than implied would avoid the problem of strict constructionist judges refusing to infer or imply an information privacy right in the wake of the *Dobbs* decision. Thus, a flexible and general broad right of federal protection from information privacy abuse might provide an optimal, flexible baseline for courts and regulators to quickly restrict new privacy abuses while allowing states to enact their own parallel legislation.

---

[205] Marissa Wong, *Revising U.S. Privacy Laws: New Laws are Required to Fill in the Gaps of Current and Proposed Legislation to Account for New Technologies and Future Emergencies*, 16 BROOK. J. CORP. FIN. & COM. L. 305 (2021) (noting in reference to past privacy legislative efforts, "the inability of the political parties to agree on the issues of preemption and private right of action").

1. Applying a Broad Right to Hypothetical Facts

Assume I recently visited a home in a subdivision in a small town. The homeowner informed me that his neighborhood had a license plate scanner and that my license plate information had been sent to the local police department to check whether my vehicle was stolen. Assume the relevant jurisdiction does not have any particular license plate privacy laws.[206] Returning to the concept of feelings, I might not feel that this is necessarily a privacy abuse. Certainly, homeowners in this neighborhood may have a legitimate desire for security. If the police department simply checked my plate against a list of stolen plates and then immediately deleted my information, this would not seem to abuse my privacy. On the other hand, if the police department shared my information, such as the date, time, location, or identity, with other parties to create a large database for warrantless access by law enforcement and private actors to track location data at multiple points in time throughout a broad geographic region for law enforcement or commercial purposes, such mass surveillance would seem abusive.[207] Given Professor Solove's observation that the U.S. legal system's default rule is that a privacy practice is generally permissible if not expressly prohibited by law, it's possible that certain government or private parties might not be liable for any harm depending on the facts.

Mass license plate scanning technology evokes Warren and Brandeis's comments on new technologies for recording images and sounds bringing new privacy harms. The ability to collect detailed location data and store it for months or years seems to invite information abuse. Further, given that the information is captured from public places, classic legal tests such as reasonable expectation of privacy may require stretching to fit the abuse.[208] Also, the involvement of various private entities collecting and sharing the data likely creates difficulties with Fourth Amendment application even where law enforcement later uses this publicly derived information. For example, some sources allege that law enforcement agencies continue to purchase location data from private entities, which would circumvent the

---

[206] *See, e.g.*, Kimberly Winbush, Annotation, *Use of License Plate Readers*, 32 A.L.R.7TH ART. 8 (2017) (listing case references of license plate scanner issues in various jurisdictions).

[207] . . . and arguably runs afoul of the Fourth Amendment.

[208] *See, e.g.*, United States v. Ellison, 462 F.3d 557 (6th Cir. 2006) (holding that a motorist had no privacy interest in information contained in a license plate number). However, the ACLU has been actively protesting government mass surveillance of license plates. *See, ee.g.*, *You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements*, ACLU (Jul. 2013), https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf [https://perma.cc/FBV6-Y8Q5].

warrant requirement for location data established by the Supreme Court in *Carpenter v. United States,* 138 S. Ct. 2206 (2018).[209]

This raises a question of how the law might efficiently address the above license plate situation. In some situations, existing laws might not adequately address the particular privacy abuse. For example, existing laws may be inadequate where Fourth Amendment protection appears unavailable relative to some private actor conduct. Waiting for states or Congress to enact a detailed license plate statute to address the particular harm would seem inefficient and might essentially allow privacy to be abused until the statute is enacted. Alternatively, a broad and general federal guarantee against information privacy abuse would allow courts to efficiently restrict clear abuses.

A broadly defined right would seem to have some advantages over detailed statutory schemes. For example, as discussed earlier, various statutes have implemented a notice and consent approach to privacy, which Solove argues has become ineffective (and as noted above might be completely moot regarding AI applied to publicly available data). As another example, various statutory definitions of personal information may become out of date and in need of revision especially where data traditionally considered public data might be shown to abuse privacy.[210] A detailed statute would certainly be helpful from a public notice standpoint of prohibited versus permissible conduct, but a broader law prohibiting information privacy abuse would seem more flexible to adapt to new harms that are very clearly an abuse of privacy and not adequately addressed by dated statutory language. On one hand, tech platforms might lobby against a broad right against information abuse and take issue with the lack of specifics. On the other hand, tech platforms might seem very disingenuous lobbying against a broad right against "abuse" of personal information (with courts determining the standard for "abuse"). All that being said,

---

[209] Bennet Cyphers, *How Law Enforcement Around the Country Buys Cell Phone Location Data Wholesale*, ELEC. FRONTIER FOUND. (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/how-law-enforcement-around-country-buys-cell-phone-location-data-wholesale [https://perma.cc/6CFM-UTQ9] (discussing various law enforcement agencies purchasing a license with a vendor that provides location data); Freddy Martinez, *Police Quietly Obtain Private Location Data with a Checkbook and Not a Warrant*, PROJECT ON GOV'T OVERSIGHT (Oct. 11, 2022), https://www.pogo.org/analysis/2022/10/police-quietly-obtain-private-location-data-with-a-checkbook-and-not-a-warranthttps://www.pogo.org/analysis/2022/10/police-quietly-obtain-private-location-data-with-a-checkbook-and-not-a-warrant [https://perma.cc/G35G-ZGR4] (alleging instances of law enforcement purchasing location data without a warrant post-*Carpenter*).

[210] As one example, *see Nevada Amends Data Security Law to Expand Definition of "Personal Information"*, NORTON ROSE FULBRIGHT: DATA PROTECTION REPORT (June 16, 2015), https://www.dataprotectionreport.com/2015/06/nevada-amends-data-security-law-to-expand-definition-of-personal-information [https://perma.cc/YC2J-MSH8] (noting Nevada broadening its statutory definition for greater consistency with other states).

given that privacy and feelings are connected, the average person might be able to perceive or feel whether a particular practice is a serious abuse of information privacy without the need for detailed statutory guidance. Regarding egregious privacy abuse, the words of Justice Stewart are fairly on point, "I know it when I see it."[211]

2. A Broad Right Could Override Other Statutes

Finally, a broad constitutional right might potentially override statutes or common law protections used in a manner that are clearly abusive of individual privacy (e.g., as noted earlier, a California case found a particular statutory provision violated California's constitutional privacy right[212]). As noted, Section 230 of the Communications Decency Act has been used as a shield for conduct that seems abusive of privacy.[213] A federal constitutional right could similarly invalidate privacy abuses otherwise supported by Section 230 or other lawlaw. A broad privacy law could also be more effective than piecemeal legislation targeting specific commercial activities that profit from harming individual privacy without any substantial justification. For example, perhaps enactment of the Illinois mugshot law may have been unnecessary if a broad constitutional privacy right existed at the time that would allow a court to rule that charging fees for mugshot removal was a privacy abuse more so than mere publication of newsworthy content.

3. A Broad Information Privacy Right Would Avoid the post-Dobbs Potential for Judicial Refusal to Imply Such a Right

Warren and Brandeis essentially defined privacy as a new area of law by implying its existence from existing law. In contrast, The Supreme Court in 2022 refused to imply a decisional privacy right in the context of abortion, which raises the possibility of future refusals to imply i*nformation*

[211] A phrase used by Justice Stewart in connection with his observation that a certain motion picture did not appear to be hard core pornography: "I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description; and perhaps I could never succeed in intelligibly doing so. But I know it when I see it, and the motion picture involved in this case is not that." Jacobellis v. Ohio, 378 U.S. 184, 197 (1964).

[212] As an example of this concept, the California Supreme Court found a California parental consent statute in the abortion context violated the California Constitutional right to privacy. Am. Acad. of Pediatrics v. Lungren, 940 P.2d 797, 831 (Cal. 1997).

[213] Mary Graw Leary, *The Indecency and Injustice of Section 230 of the Communications Decency Act*, 41 HARV. J. L. & PUB. POL'Y 553, 573 (2018) (observing that "overbroad interpretation [of Section 230] has left victims of online abuse with no leverage against site operators whose business models facilitate abuse") (quoting Danielle Citron & Benjamin Wittes, *The Internet Won't Break*, 86 FORDHAM L. REV. 401, 404 (2017)).

privacy rights.[214] Justice Kavanaugh's opinion that *Dobbs* will not affect issues outside of the abortion context invites skepticism.[215] For example, the dissent questioned the majority's statement that *Dobbs* will not affect other precedent outside of the abortion context by explaining "[r]ights can contract . . . because whatever today's majority might say, one thing really does lead to another."[216] The dissent expressed concern that *Dobbs* might pave the way for states to determine rights to contraception (and I would imagine other issues outside of reproductive rights). In 2023, the City of Chicago advanced the reasoning of *Dobbs* in a federal suit concerning mandatory vaccinations.[217] Thus, post–*Dobbs* I am doubtful that the decision will have no impact on other areas of law, and I am wary of the tendency that loss of one right might lead to loss of other rights.

When it comes to information privacy and its place among other liberty rights, a broad general question to consider is what life in a free society should look like. A free society requires a government that protects citizens and provides law and order[218] while also allowing various personal freedoms.[219]

When a sufficient quantity of individual rights are present within a society, it might be perceived as a free society. Alternatively, where individual rights are substantially restricted, the society may be viewed as not free. Some have argued that society must continually battle with the

---

[214] But, curiously, the dissent discussed that the majority's textual approach is flawed in that "marriage" is mentioned nowhere in the Constitution's text, yet marital freedom from government interference is considered [as an implicit right] within the Fourteenth Amendment's reference to liberty.

[215] Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2309 (2022) ((*"*First is the question of how this decision will affect other precedents involving issues such as contraception and marriage—in particular, the decisions in Griswold v. Connecticut, 381 U.S. 479, 85 S. Ct. 1678, 14 L.Ed.2d 510 (1965); Eisenstadt v. Baird, 405 U.S. 438, 92 S. Ct. 1029, 31 L.Ed.2d 349 (1972); Loving v. Virginia, 388 U.S. 1, 87 S. Ct. 1817, 18 L.Ed.2d 1010 (1967); and Obergefell v. Hodges, 576 U.S. 644, 135 S. Ct. 2584, 192 L.Ed.2d 609 (2015). I emphasize what the Court today states: Overruling Roe does not mean the overruling of those precedents, and does not threaten or cast doubt on those precedents.")..").

[216] *Id.* at 2332 (Breyer, Sotomayor and Kagan, JJ., dissenting). *See also* David Schultz, Commentary, *Is Any Precedent Safe Now? The Impact of Dobbs on Other Rights*, 2022 WL 2721325 (noting that *Dobbs* may have an impact on other rights outside of abortion, such as voting and marriage rights).).

[217] Caleb Drickey, *Chicago Says Dobbs Decision Forecloses Vax Challenge*, LAW360 (Feb. 9, 2023, 4:37 PM), https://plus.lexis.com/newsstand#/law360/article/1574573 [https://perma.cc/SPT4-Q2S5] (describing that in 2023 the City of Chicago "urged a federal court to end a group of municipal employees' challenge to the city's COVID-19 vaccine mandate, telling the court that the repeal of Roe v. Wade meant the workers could no longer claim their right to bodily autonomy was arbitrarily infringed upon")..").

[218] *See* Daron Acemoglu & James A. Robinson, *The Narrow Corridor: States, Societies, and the Fate of Liberty*, at xii (2019) ("[L]iberty must start with people being free from violence, intimidation, and other demeaning acts.")..").

[219] *Id.* ("("People must be able to make free choices about their lives and have the means to carry them out without the menace of unreasonable punishment or draconian social sanctions.")..").

government to preserve individual freedoms as there is a natural tendency for governments to grow in power and restrict individual rights for law enforcement or other purposes.[220] It would seem then if one were to view our legal system as a battle between society and government/commercial forces, regarding the liberty interest of privacy, then a broad privacy law would assist society in that battle for rights.

The Court's reluctance to imply a privacy right within the constitutional guarantee of liberty in *Dobbs* increases the probability of the Court delegating information privacy rights to the states. This certainly remains to be seen on a case-by-case basis; however, the ruling in *Dobbs* likely makes it easier for the Court to defer to state legislatures on privacy issues. Alternatively, *Dobbs* might not have a significant impact on many information privacy issues because it addressed a unique and divisive issue, involving whether abortion terminates life or a potential life, while a general desire for information privacy rights would seem far less divisive. If so, the Supreme Court may be less likely to defer to states on less divisive issues concerning information privacy.

Dobbs may have the effect of decreasing surveillance privacy rights if states attempt to exercise jurisdiction in criminalizing out of state abortions. Prior to *Dobbs*, I had no opinion on whether the substantial reduction of financial privacy within the United States was problematic, but I considered that a lack of financial privacy is certainly problematic in countries ruled by an authoritarian regime (a lack of financial privacy could be abused by an overreaching authoritarian government).[221] Now, post *Dobbs*, I am concerned that states could exploit financial transaction data to convict its residents of paying for abortions. Another related concern is that technology provides the ability for strong surveillance, and the question is whether and when such surveillance capability should be used.[222] A highly

---

[220] Similarly, see Ronald Reagan, Address at the Goldwater Presidential Campaign: A Time for Choosing (Oct. 27, 1964) (transcript available at Ronald Reagan Presidential Library & Museum), https://www.reaganlibrary.gov/reagans/ronald-reagan/time-choosing-speech-october-27-1964 [https://perma.cc/8ESZ-A7CK] ("No government ever voluntarily reduces itself in size. Government programs, once launched, never disappear. Actually, a government bureau is the nearest thing to eternal life we'll ever see on this earth!"). https://www.reaganlibrary.gov/reagans/ronald-reagan/time-choosing-speech-october-27-1964)

[221] One could argue that one purpose of the PATRIOT Act, with its Bank Secrecy Act amendments,, was to augment the government's money laundering investigation powers using terrorism concerns as the justification. In theory, a reduction in financial privacy might not be harmful to society. However, financial transparency could be abused by an overreaching government that disapproves of particular political or religious donations, for example.

[222] Frankie Vetch, *Women are the Primary Targets of Iran's Surveillance State,* CODA STORY. (Sep. 13, 2022), https://www.codastory.com/newsletters/iran-surveillance-women/ [https://perma.cc/8LPA-U5V8].

surveilled society is characteristic of rule by an authoritarian regime. Even with safeguards in place, such as warrants for investigating footage after a crime occurs, questions arise of whether and to what extent such technology should be installed in the first place, how much data should be collected, how long should it be stored, etc. I have previously argued that a society has greater freedom where it allows some crimes to go undetectable (essentially applying Blackstone's ratio to privacy), and thus, fewer implementations or surveillance tech might be valued from that standpoint.[223] Also as noted previously within the Smollett prosecution discussion, Westin offered a similar argument in the 1960s that detection of serious crime (e.g., terrorist activity) is essential for stability in society.[224] A key question is whether conduct that is legal in one state but illegal in another should be considered a serious crime, justifying invasive long arm discovery of data. Perhaps the answer might be no when applying a broad constitutional information privacy right?

4. Privacy and Out of State Abortions

If a state banning abortion wishes to criminalize its residents for out of state abortions, the privacy implications are staggering.[225] While Justice Kavanaugh's concurring opinion predicts that criminalization of an out of state abortion should not be possible given the constitutional right to travel, the matter might not be this simple.[226] For example, a state can theoretically pursue a murder charge for a murder of a resident committed outside of the state.[227]

What electronic information could be readily discoverable with or without a subpoena or warrant? Privacy experts warn that popular period-tracking apps could be mined for data, either by subpoena or sale to a third-

---

[223] *See* Volini, *supra* note 49, at 359-60 ("Just as the Blackstone ratio principle favors constitutional protections that allow ten guilty people to go free rather than allowing one innocent person suffer, individual privacy rights could arguably favor fairly unsurveillable encrypted communications at the risk of not detecting various criminal activity.").").

[224] Westin, s*upra* note 48.

[225] A state could conceivably justify jurisdiction for an out-of-state abortion, "reaching anyone involved with the killing of a 'living, distinct' resident of a state with an abortion ban." *See* David S. Cohen, Greer Donley & Rachel Rebouché, *The New Abortion Battleground*, 123 COLUM. L. REV. 1, 32 (2023) (describing various gaps in the general rule against extraterritorial application of criminal law that could be exploited to prosecute out-of-state abortions).

[226] *Dobbs*, 142 S. Ct. at 2309.

[227] *See* Shana Druckerman, Nikki Battiste & Edward Lovett, *Honeymoon 'Killer': Gabe Watson Breaks Silence on Details of Wife's Death*, ABC NEWS (Feb. 29, 2012), https://abcnews.go.com/US/honeymoon-killer-gabe-watson-breaks-silence-details-wifes/story?id=15819106 [https://perma.cc/8AUE-7QZ5].

party, as to whether a woman is even considering abortion.[228] This scenario extends beyond menstrual health and wellness apps. As a woman sits in the waiting room of an abortion clinic, scrolling social media, or playing a game, these apps could be recording her location data.[229] State governments could potentially obtain a warrant for emails, internet searches, and financial transaction information.

Abortion-supportive states, as well as the pro-choice Biden administration, have snapped into action to ensure access to reproductive care, which necessarily implicates protecting privacy rights.[230] California has taken the most aggressive stance in terms of data privacy, recently banning California based platforms from complying with out of state warrants targeting abortion.[231] Given the interstate legislative fights that might ensue post-*Dobbs*, it would seem that a broad privacy law ensuring information privacy rights may be desirable to maintain privacy of abortions in jurisdictions where abortion is legal (and perhaps such a privacy right might reduce potential legal battles between states). And, of course, states wishing to prosecute out-of-state abortions might oppose a constitutional information privacy amendment that might protect discovery of such extraterritorial abortions.

---

[228] Rina Torchinsky, *How Period Tracking Apps and Data Privacy Fit into a Post*-Roe v. Wade *Climate*, NPR (June 24, 2022), https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps [https://perma.cc/8LF3-9J6Z].

[229] *Id.*

[230] Cohen, *supra* note 225, at 43 (stating that Massachusetts, California, Connecticut, Delaware, New Jersey, and New York have all passed interstate shield laws, limiting the liability of those seeking, or individuals assisting those seeking, abortion related services and Illinois and the District of Columbia have similar bills pending). On the federal side, two weeks after the decision in *Dobbs* was handed down, President Biden signed an executive order protecting access to reproductive health care services. Relevant here, the order specifically addressed 1) protecting consumers from privacy violations by directing the Chair of the Federal Trade Commission to "consider taking steps to protect consumers' privacy when seeking information about and provision of reproductive health care services"; and 2) protect sensitive health information by directing the Secretary of Health and Human Services "to consider additional actions, including under the Health Insurance Portability and Accountability Act (HIPAA), to better protect sensitive information related to reproductive health care." *FACT SHEET: President Biden to Sign Executive Order Protecting Access to Reproductive Health Care Services,* THE WHITE HOUSE (July 08, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/08/fact-sheet-president-biden-to-sign-executive-order-protecting-access-to-reproductive-health-care-services/ [https:perma.cc/DZ4R-PWSG].

[231] Brian Fung & Clare Duffy, *California Bars Tech Companies from Complying with Other States' Abortion-related Warrants*, CNN BUSINESS (Sept. 29, 2022), https://www.cnn.com/2022/09/29/tech/california-tech-abortion-warrant-ban/index.html [https:perma.cc/U7KQ-VZPQ].

CONCLUSION

Based on the above discussion, it would seem worthwhile to explore a broad express federal right of protection against information privacy abuse. Further, in considering the path forward, contemplating the history of privacy and information technology from 1890 would seem helpful to assess how the law could best protect against unknown future privacy harms.

Privacy law within the United States would benefit tremendously from a broad overarching federal right to information privacy that would protect against abuses instigated by government actors, private actors, or two such parties working together. Such a right would provide a variety of benefits and might ideally take the form of a constitutional amendment. Such an amendment should focus entirely on information privacy rather than decisional privacy to have the greatest chance of enactment given the enduring divisiveness of the abortion issue. The lesson from comparing 1890 to today is that technology continually evolves at a rapid pace, and the law struggles to catch up to new privacy harms brought by new tech. Accordingly, today it would seem helpful to make express the broad privacy right that Warren and Brandeis needed to imply from existing law in 1890, especially if modern courts become reluctant to imply a broad information privacy right post *Dobbs v. Jackson*. One benefit of a broad information privacy right is judicial protection from new information privacy abuses without as much need to wait for state or federal congress to respond with piecemeal legislation. A related benefit is that it seems difficult or impossible to craft a detailed statute that would provide broad protection from unknown future privacy harms. Instead, the flexibility of express constitutional protection seems preferable. Other benefits of such a constitutional right include increasing harmonization of United States privacy law with Europe and empowering courts to override laws that might otherwise shield information privacy abuses.