UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 19 | Issue 1 Article 1

1-1-2018

Health Privacy and (Lack Of) Legal Protections In a Technology-Driven Economy

Mystica M. Alexander

Cheryl Kirschner

Patrick A. Sholten

David J. Yates

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 19, ISSUE 1: OCTOBER 2017

HEALTH PRIVACY AND (LACK OF) LEGAL PROTECTIONS IN A TECHNOLOGY-DRIVEN ECONOMY

Mystica M. Alexander, Cheryl Kirschner, Patrick A. Scholten, David J. Yates*

Applying the perspectives of law, technology, and economics, this article explores the privacy concerns arising from the ability of search engines and web domain owners to indiscriminately track an individual's health-related internet searches. Using the hypothetical example of a forty-year-old woman diagnosed with high cholesterol who turns to Google to begin gathering data about her condition and her treatment options, this article discusses the many ways in which technology can be used to gather, store, aggregate, and track an unsuspecting user's health-related searches as she surfs the web for information. From an economic perspective, financial incentives abound for those who conduct business by compiling these various bits of information on consumers through their internet activities. Having laid this foundation, this article then explores what legal protections exist under current privacy law to protect computer users from such intrusions. Finding a distinct lack of protection in the law, this article concludes with a recommendation that Congress take legislative action targeted specifically at protecting such health-related inquiries.

* Mystica Alexander is an Associate Professor of Law and Taxation at Bentley University. Cheryl Kirschner is a Senior Lecturer of Law at Babson College. Patrick Scholten is an Associate Professor of Economics at Bentley University. David Yates is an Associate Professor of Computer Information Systems at Bentley University. The authors thank Christina Zandri and William Wiggins for their assistance with this project.

INTRODUCTION

Consider this scenario: Pamela, a forty-year-old female, is informed by her doctor that she has high cholesterol and is at high

risk for coronary artery disease. If she is like many other individuals in today's world, she will soon log on to her computer to conduct Google or other internet searches[1] using terms such as "women and high cholesterol," "cholesterol-lowering drugs," and "coronary artery disease" to learn more about her new health concern. As she searches, there is a high likelihood that her queries are being tracked.[2] Due to advances in tracking technologies and data mining capabilities, simply conducting searches increases the probability that these searches can be traced back specifically to her.[3] Early tracking capabilities, such as cookies, were used as benign text files placed on users' computers to facilitate information transfers, such as keeping track of items in an online shopping cart.[4] Newer, more intrusive, third-party tracking technologies place files on or send a script to users' computers.[5] These trackers are designed to gather information on website users' behaviors across internet domains.[6] And although third-party tracking is often fragmented and messy, data mining and data warehousing can improve the quality of this tracking data by connecting it to additional information gathered, such as a user's IP address, location, name, or associations in their social

---

[1] *See* Ryan W. White & Eric Horvitz, *Experiences with Web Search on Medical Concerns and Self Diagnosis*, AMIA ANN. SYMP. PROC. 696 (finding that "wealth of medical information on the Web makes it convenient for non-experts to conduct their own diagnosis and healthcare assessment based on limited knowledge of signs, symptoms, and disorders.").

[2] *See* Greg R. Notess, *Tracking Your Search History*, ONLINE (Mar./Apr. 2006), http://www.infotoday.com/online/mar06/OnTheNet.shtml (explaining that the personalization enabled by consumer tracking in search engines "offers the opportunity to build user loyalty by more effectively targeting advertising and search results. The personalization features include such options as saving URLs, archiving pages, organizing saved results into folders, blocking specific sites, and recording a search history.").

[3] *See* Jonathan R. Mayer & John C. Mitchell, *Third-Party Web Tracking: Policy and Technology,* PROC. 2012 IEEE SYMP. ON SECURITY & PRIVACY 413, 415 (2012), http://cyberlaw.stanford.edu/files/publication/files/trackingsurvey12.pdf.

[4] *See* David M. Kristol, *HTTP Cookies: Standards, Privacy, and Politics*, 1 ACM TRANSACTIONS ON INTERNET TECH. 151, 152–54 (2001).

[5] *See* Mayer & Mitchell, *supra* note 3, at 421.

[6] *See id*. at 415.

networks.[7] This aggregated information is then purchased by companies that use the information gleaned from online activity to effectively sort individuals by certain characteristics, customize goods and services, and even engage in price discrimination.[8]

Given today's technology, such a consequence is more than just a mere possibility. Consider, for example, a change Google made to its privacy policy in June of 2016. As part of the company's plan to create more robust consumer profiles, Google "asked users to accept a new policy that would allow them to more easily see—and delete—the information Google holds about them."[9] This included giving Google permission to combine information on the individual's Google searches and email with information on the individual's browsing history.[10] This new policy marked a drastic departure from Google's nearly ten-year-old policy of separating data from search, email, and its DoubleClick business (DoubleClick is a subsidiary of Google that develops and provides Internet advertising delivery services).[11] In December of 2016, two U.S. privacy advocacy groups filed a complaint against Google with the Federal Trade Commission ("FTC") in response to this policy change.[12] In their complaint, the privacy advocates alleged that

> Google took affirmative steps to conceal and downplay the significance of this transformational change that eliminated the barrier between the data that Google gathers from cookies that track users' behavior and the personal information that Google holds from its users' accounts. Google induced users to accept the change to its privacy policy by cloaking it in an offer to enable 'new features' that purport to provide

---

[7] *See id*.

[8] *See* Joseph Turow, Lauren Feldman & Kimberly Meltzer, *Open to Exploitation: America's Shoppers Online and Offline*, *A Report from the Annenberg Public Policy Center of the University of Pennsylvania* (2005) (suggesting that it is "a complex mix of ignorance and knowledge, fear and bravado, realism and idealism that leaves most internet-using adult American shoppers open to financial exploitation by retailers.").

[9] Natalia Drozdiak & Jack Nicas, *Google Privacy-Policy Change Faces New Scrutiny in EU*, WALL ST. J. (Jan. 25, 2017), https://www.wsj.com/articles/oracle-expresses-concern-to-eu-over-google-privacy-policy-1485263548.

[10] *See id.*

[11] *See id.*

[12] *See id.*

> 'more control' over users' personal information. Unsuspecting users accepted Google's offer in droves.[13]

Such actions beg the question of whether a normal citizen like Pamela should have a reasonable expectation of privacy as she surfs the web to gather information about high cholesterol. If so, what is the extent of reasonable privacy protection?

To begin, many scholars have noted the difficulty in defining "privacy."[14] Fundamentally, "the desire for privacy is an innate aspect of human nature. For that reason, many have found that the most productive and credible way of justifying privacy is as a natural right aspect of human dignity."[15] Some philosophy scholars have argued that "there is no overarching concept of privacy but rather several distinct core notions that have been lumped together."[16] Some have defined privacy in freedom-based terms:

> [t]he right to privacy is an integral part of our humanity; one has a public persona, exposed and active, and a private persona, guarded and preserved. The heart of our liberty is choosing which parts of our lives shall become public and which parts we shall hold close.[17]

Others have attempted to clarify this murky area by defining three categories or "clusters" of privacy: spatial privacy (involving a person's solitude and freedom from physical invasion), decisional privacy (involving the freedom to make certain decisions without interference), and informational privacy (involving the ability to determine the conditions under which others receive information about oneself).[18] While these spheres are not "sharply separate," they are helpful distinctions for

---

[13] Complaint, Request for Investigation, Injunction, and Other Relief at 2 (Dec. 16, 2016), http://www.consumerwatchdog.org/resources/ftc_google_complaint_12-5-2016docx.pdf.

[14] Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1088 (2002).

[15] Samuel P. Winch, *Moral Justifications for Privacy and Intimacy,* 11 J. MASS MEDIA ETHICS 197, 198 (1996).

[16] Adam D. Moore, *Privacy: Its Meaning and Value*, 40 AM. PHIL. Q. 215, 215 (2003).

[17] Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 235 (Minn. 1998).

[18] Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy,* 39 SAN DIEGO L. REV. 843, 845 (2002).

discussing possible privacy protection schemes.[19] Our analysis is limited to informational privacy.

In light of the increasing potential of technology to infringe upon an individual's informational privacy, especially with regard to health-related information, and the potential economic implications of such infringement, this paper explores the legal protections of an individual's right to privacy and proposes legislative action to limit industries' abilities to continue indiscriminate tracking and aggregation of individual health-related information. Part I of this Article provides a discussion of the technological possibilities and realities of the 21st century, and how technologies are used to gather, sort, aggregate, and store user information. Part II offers a description of the economic motivations behind the tracking and collection of user data. Advances in technology have given rise to new online intermediaries, such as online advertisers and price aggregating and comparison sites, that create and use platforms to add user value and create exploitative profit opportunities. However, these activities have significant implications for consumer privacy. Part III traces the legal history of user data protection and examines the current state of protection at both the federal and state levels. Part IV considers whether the tracking and aggregation of user information in the context of health-related issues should be subject to special scrutiny. Moreover, the section asks whether the current methods for tracking, collecting, and storing health-related user search inquiries violates the spirit, if not the letter, of the privacy protections provided by the Health Insurance Portability and Accountability Act ("HIPAA"). Part V concludes that industry self-regulation alone is not adequate to protect against abuses of user informational privacy and proposes federal legislation limiting the ability of third-party trackers to gather and aggregate health-related data.

[19] Jerry Kang, *Information Privacy in Cyberspace Transactions,* 50 STAN. L. REV. 1193, 1203 (1998).

I. THE EVOLUTION OF ONLINE TRACKING TECHNOLOGY AND ITS INCREASING IMPOSITION ON PRIVACY

How a business initially obtains a user's information should be a key factor when considering the potential privacy harms of commercial data aggregation and analysis.[20] Arguably, there is a distinction among a user's privacy expectation in information voluntarily given, such as on a survey, transactional information a company gleaned from an online purchase, and data collected about a user's online searches, such as in the opening scenario.

A. First-Party Tracking and Consumer Privacy

Most website owners *directly* collect, track users' behaviors, and store personal identifiable information ("PII") and non-personal identifiable information ("Non-PII") on visitors using different mechanisms. According to the National Institute of Standards and Technology, [P]II is:

> any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.[21]

---

[20] A fascinating point of law tangentially related to the topic of this article is whether and to what extent the government is permitted to access and use information voluntarily transmitted by a business about a citizen. In *United States v. Miller,* Justice Powell wrote for the majority:

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

425 U.S. 435, 443 (1976), *superseded by statute*, Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 (1978).

[21] Erika McCallister et al., *Guide to Protecting the Confidentiality to Personally Identifiable Information (PII)*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Apr. 2010), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

In contrast, non-PII is data that cannot be solely utilized to identify or trace a person.[22] Traditionally, examples include device IDs, IP addresses, and cookies; however, the distinction between PII and non-PII has become increasingly blurred.[23] This is the essence of first-party tracking: a website (Internet domain) owner directly collects information on everyone visiting their website. In this context, "first-party" refers to which organization or website is doing the tracking and "tracking" refers to the mechanism used to collect the user information. In the context of Pamela, the forty-year-old woman diagnosed with high cholesterol, her internet search would result in Google storing a small text file, called a "first-party cookie," on her computer that uniquely identifies her browser or her device, distinguishes it from other users, and identifies how she interacted with the Google search engine.[24] Here, Google is the first party, and its tracking mechanism is the cookie it places on Pamela's computer. By tracking and identifying users, website owners create and update user profiles.

The most elementary form of first-party tracking occurs when a user creates a profile through a user account with a website owner

---

[22] *See* Mark H. Rosenbaum, *Identifying Unethical Personally Identifiable Information (PII) Privacy Violations Committed by IS/IT Practitioners: A Comparison to Computing Moral Exemplars* (Feb. 2015) (unpublished doctoral dissertation, Nova Southeastern University), http://nsuworks.nova.edu/gscis_etd/29.

[23] *See* Massimiliano Pappalardo, *Personal Data or Non-Personal Data That Is the Question! The Different Interpretations of ECJ and Italian Supreme Court*, (Oct. 2016), https://www.lexology.com/library/detail.aspx?g=804ce9b8-dfa5-4c67-bbf7-4cc3e087c2f8. Note, PII is a term used primarily within the United States, whereas the term personal data is the European equivalent to PII, with some caveats. The EU directive 95/46/EC defines personal data as:

> Article 2(a): 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31, 2(a).

[24] Google Analytics, *Google Analytics Cookie Usage on Websites*, https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage (last visited Sept. 17, 2017).

and logs into their account to access that website. As part of the account set-up process the website owner may ask for various pieces of information, such as name and contact information, and when users voluntarily reveal this identifying information, tracking related to such disclosures is *explicit*. For example, our forty-year-old woman may have voluntarily created a Google account and may have been signed into it when she conducted an internet search for "women with high cholesterol." By providing her name, date of birth, gender, mobile phone number, email address and location, Google will give her access to other services it offers and will provide a secure, more personalized experience. Information disclosures such as these permit users to gain access to additional content or website features in exchange for personal (or clickstream) information that website owners can use.[25]

While personal online profile accounts or profiles permit explicit first-party tracking, there are many examples of website owners that use *implicit* first-party tracking mechanisms. These commonly-used computer browser-based tracking mechanisms include: 1) Hypertext Transfer Protocol ("HTTP") cookies,[26] 2) Internet Protocol ("IP") address identification,[27] and 3) browser fingerprinting.[28]

While the Internet is a networking infrastructure consisting of networks of networks, the Web—or World Wide Web—is the

[25] Clickstream information is a series of mouse clicks made while accessing one or more websites. *See* Randolph E. Bucklin & Catarina Sismeiro, *Click Here for Internet Insight: Advances in Clickstream Data Analysis in Marketing*, 23 J. INTERACTIVE MARKETING 35, 35–37 (2009).

[26] David Kristol & Lou Montulli, *HTTP State Management*, *Request for Comments* (Oct. 2000), https://www.ietf.org/rfc/rfc2965.txt.

[27] Client IP addresses are logged as part of standard practice by web servers so that Internet domain owners know basic information about clients who have accessed content hosted on their servers. When combined with other information in a standard log entry, e.g. a timestamp, a reverse DNS lookup of the IP address, the client TCP port number, the identity of the client device can be determined. For a description of a standard log entry, *see* the *World Wide Web Consortium* (W3C) Extended Log File Format, https://www.w3.org/TR/WD-logfile.html.

[28] Peter Eckersley, *How Unique Is Your Web Browser?*, INTERNATIONAL SYMPOSIUM ON PRIVACY ENHANCING TECHNOLOGIES SYMPOSIUM 1, 1–18 (Jul. 2010).

protocol for accessing information (websites) over the Internet. The Hypertext Transfer Protocol (HTTP) is the dominant application layer protocol for data communication over the Web. Originally, HTTP was designed as a stateless protocol; meaning that each user's request to a website is treated independently of previous requests from the same user.[29] The implication is that websites and their applications cannot track user configuration settings or retain transaction information between sessions or web pages. This feature of the HTTP protocol severely limits the potential usefulness of the World Wide Web and the Internet. For example, a stateless protocol would preclude a website from remembering what an online shopper had added to their shopping cart.

To overcome the stateless feature of HTTP, websites send and store small text data files, called HTTP cookies, on a user's computer via the internet browser while a user is browsing.[30] HTTP cookies were designed to maintain state information between a user and websites she has visited, such as remembering items added to a shopping cart in an online store and browsing activities across pages maintained by a website owner. In addition to maintaining state information, HTTP cookies remember other pieces of information that a user may have entered on a website owner's pages like passwords and credit card numbers.[31] Cookies play an important role in how modern websites work. Their management of state by the web browser and web server provides a convenient and reliable way of remembering things such as where a user left off the last time she visited a site and any user preferences.[32] To maintain state information, a website "sets" a cookie in a user's browser. The information encoded in the cookie, the use of the cookie by the website owner, and the ability to link the cookie with other information all generate privacy concerns.[33]

---

[29] *See* Ray Fielding, Jim Gettys, Jeff Mogul, Henrik Frystyk, Larry Masinter, Paul Leach & Tim Berners-Lee, *Hypertext Transfer Protocol—HTTP/1.1*, *Request for Comments* (Jun. 1999), https://www.ietf.org/rfc/rfc2616.txt.

[30] *See* Kristol, *supra* note 4, at 153.

[31] *Id*. at 155.

[32] *Id*.

[33] *Id*.

Two common types of first-party HTTP cookies are session cookies and persistent cookies.[34] A session cookie is a temporary text file that is removed from the computer user's cache memory when the web browser closes. The purpose of a session cookie is to store state information only while a user visits a website. In regards to consumer privacy concerns, session cookies are the most benign first-party tracking technology since they are deleted once the browser session is terminated and are not used for tracking over time or across websites. In contrast, a persistent cookie is a small text file placed on a computer that remains in a browser's data storage so that the cookie communicates its information to the website upon every visit. Persistent cookies expire either on a specific date or after a specific length of time.[35] The enduring nature of persistent cookies enables users to remain logged into a website for a period of time and store information on behalf of the website owner. It also permits a website to track a user's behavior while visiting the pages on its website. Despite the upside of facilitating interactions and improving users' experiences, persistent cookies are more invasive in terms of privacy since websites can learn about users' behavior and potentially use that information in ways that could be harmful to the consumer.[36] While users can set browser settings to disable cookies or easily remove them from their computers, a new class of cookies has been developed that cannot easily be deleted.[37]

---

[34] *See* Nicholas C. Zakas, *HTTP Cookies Explained*, NCZONLINE (May 5, 2009), https://www.nczonline.net/blog/2009/05/05/http-cookies-explained/ (last visited Sept. 17, 2017). By default, "a cookie has a lifespan of a single session. A session is defined as finished when the browser is shut down, so session cookies exist only while the browser remains open." *Id*. For a cookie to persist on a client device after a browser is shut down, the default behavior can be modified by setting an expiration date and time for a cookie, which specifies when the cookie "may be deleted by the browser." *Id*. Therefore, a persistent cookie is stored on the client device until it expires.

[35] MDN TECHNOLOGIES, *HTTP Cookies*, https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies (last visited Sept. 17, 2017).

[36] *See infra* Part II.

[37] This new class of cookies is called evercookies or zombie cookies that are persistent and cannot be (easily) deleted. *See* Jacqui Cheung, *Zombie Cookie Wars: Evil Tracking API Meant to Raise Awareness*, ARS TECHNICA (Sept. 22,

Browser fingerprinting and Internet Protocol ("IP") address tracking are two other commonly used implicit, first-party tracking mechanisms, which differ from HTTP cookies in that they are stateless.[38] Unlike persistent cookie technology that can be used to identify and track users' online behavior over time on a particular website, browser fingerprinting relies on a combination of user's browser and computer configuration that the website can retrieve with each visit.[39] Individually, the identifiers within a "fingerprint" are incapable of identifying a specific individual. However, the personal-identification power is derived from examining these identifiers collectively. The chance that two individuals have the exact same settings and specifications is only one in several million individuals.[40] Browser fingerprinting is viewed as the most invasive violation of consumer privacy because: 1) it is virtually impossible for users to detect; 2) it is difficult to prevent; and 3) it is semi-permanent.[41] Although not as invasive as browser fingerprinting, IP address tracking is another first-party tracking mechanism that facilitates individual- or household-level identification and tracking, and it can be technically difficult for lay users to prevent. Each computer or router connects to the Internet using an Internet Service Provider ("ISP"), who assigns

---

2010), https://arstechnica.com/business/2010/09/evercookie-escalates-the-zombie-cookie-war-by-raising-awareness/.

[38] Browser fingerprinting and IP address tracking can also be used as third-party tracking technologies. *See* NPR Staff, *Online Trackers Follow Our Digital Shadow by "Fingerprinting" Browsers, Devices*, NPR (Sept. 16, 2016, 5:58 PM), http://www.npr.org/sections/alltechconsidered/2016/09/26/495502526/online-trackers-follow-our-digital-shadow-by-fingerprinting-browsers-devices.

[39] The collected information is extensive and typically includes: browser type and version, the computer operating system and version, screen resolution, supported fonts, plugins, time zone, language, font preferences, and sometimes other hardware configurations. *See* Lance Cottrell, *Browser Fingerprints, and Why They Are So Hard to Erase*, NETWORK WORLD (Feb. 17, 2015, 6:22 AM), https://www.networkworld.com/article/2884026/security0/browser-fingerprints-and-why-they-are-so-hard-to-erase.html.

[40] This statistic suggests that browser fingerprinting is a highly successful individual-identifying mechanism. *Id.*

[41] *Id.*

each computer or router a unique IP address.[42] By itself, an IP address does not contain any personally identifiable information; however, a website can identify a user's IP address, which can reveal the user's geographical region.[43] The implication is that a website can, with some degree of accuracy, link an IP address to an individual user.[44]

B. Third-Party Tracking

In contrast to first-party tracking technologies, the common elements of third-party tracking technologies are twofold: 1) the mechanism is initiated by a party other than the website owner and 2) the technologies can identify, collect, store, and aggregate personal and non-personal information about a user over time and across websites. Third-party tracking technologies can be used when a website partners with an advertising network to populate blank ad-space or partners with an analytics company to better understand users' behaviors. Pamela may visit a website to research the health implications of her high cholesterol and encounter an advertisement that relies on third-party tracking technology to deliver the advertisement based on certain personally identifiable and non-personally identifiable user information, for example, her age, gender, browsing history, or search history.

There are many different third-party tracking technologies. Broadly, these are categorized as "stateful" and "stateless" technologies. Stateful third-party tracking technologies, such as

---

[42] PRIVACY RIGHTS CLEARINGHOUSE, *Online Privacy: Using the Internet Safely*, PRC, https://www.privacyrights.org/consumer-guides/online-privacy-using-internet-safely (last visited Sept. 6, 2017).

[43] There are two possible weaknesses in an ISP assignment of IP addresses: 1) ISPs' privacy policies vary considerably and may disclose an individual's or a household's IP address and 2) ISPs assign IP addresses based on geographical location and the specificity of that assignment varies with ISP. *Id*.

[44] *Why IP Tracking Is a Bad Idea*, AD EXCHANGER (Jul. 30, 2010, 12:09 AM), https://adexchanger.com/the-debate/why-ip-tracking-is-a-bad-idea/ (discussing a 2010 test that revealed the ability of IP addresses to accurately identify about thirty percent of U.S. households).

third-party cookies, use a variety of technologies, including many of which fall under the umbrella term of supercookies.[45]

Like a first-party cookie, a third-party cookie is a small file residing on a website user's computer that identifies personal and non-personal information. However, unlike a first-party cookie, the origin of the third-party cookie is a website other than where a user is currently visiting. For example, if Pamela visits an information content provider's website, like WebMD.com, and encounters an advertisement for a cholesterol-lowering drug, like Repatha, and she clicks on the advertisement and is redirected to a non-WebMD.com website, then a third-party cookie may have been used in the redirection process. A third-party cookie was likely used to help identify (based on her personally identifiable and non-personally identifiable information) with what advertisement to populate the ad space on WebMD.com, and where to redirect the user as she clicked on the ad. Third-party cookies have the benefit of maintaining a stateful relationship with the user and the first party, thereby permitting third parties to identify, collect, store, and aggregate information about specific users over time and across different websites.[46]

Some types of supercookies place small files on a user's computer to facilitate communication with websites using Adobe Flash or HTML5 local storage.[47] These cookies can store a user's preference information, retrieve saved data from a supercookie-enabled application, or track users' behavior across time and websites.[48] Supercookies can be automatically recreated after a user deletes them by storing the information in multiple locations

---

[45] Jose Pagliery, "*Super cookies" Track You, Even in Privacy Mode*, CNN TECH (Jan. 9, 2015, 10:03 AM), http://money.cnn.com/2015/01/09/technology/security/super-cookies/.

[46] Mayer & Mitchell, *supra* note 3, at 415.

[47] Flash cookies also are called local shared objects (LSOs). *Id*. at 421.

[48] John Naughton, *When the Cookies Crumbled, So Did Your Web Anonymity*, GUARDIAN (Oct. 4, 2014, 7:05 PM). https://www.theguardian.com/technology/2014/oct/05/cookies-crumbled-internet-anonymity.

on the user's computer, which is more invasive than other standard HTTP cookie technologies.[49]

Clearly, "an abundance of data, inexpensive processing power, and increasingly sophisticated analytical techniques drive innovation in our increasingly networked society."[50] Indiscriminate data collection from online user behavior can be collected and used in many ways. As discussed in this section, types of data collection fall into two categories, first-party tracking and third-party tracking, with some overlap between the two distinctions. Many different tracking mechanisms, however, are used by both types of tracking. Although the use of data collected via tracking is often aligned with users' interests, data gathered during online activity are also used to target sponsored content like online advertisements as well as unsponsored content like related web pages.

Independent of the type of tracking technology used is a general lack of transparency and understanding between websites and users. A Pew Research survey in 2013 asked Americans to respond "true" or "false" to the following question: "When a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users." About 50 percent of survey respondents incorrectly answered, believing the statement was "true."[51] Beyond the lack of user understanding of websites' privacy policies, there is also an increasing lack of transparency between what users are giving up in exchange for accessing the information or services hosted by a website, especially in the realm of consumer privacy regarding health information. To access information or services for "free," users unknowingly give up personal and non-personal information, which can lead to the creation of detailed user profiles over time.

---

[49] *Understanding Other Online Tracking,* FED. TRADE COMM'N CONSUMER INFO. (June 2016), https://www.consumer.ftc.gov/articles/0042-online-tracking#Understanding_Other_Online_Tracking.

[50] THE WHITE HOUSE, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 4 J. PRIVACY CONFIDENTIALITY 95, 99 (2012).

[51] Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RES. CTR. (Dec. 4, 2014), http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/.

Beyond user identification, it is also important to understand how websites owners use personal and non-personal information to further their economic objectives.

II. THE ECONOMIC MOTIVATIONS OF UNINHIBITED TRACKING AND DATA COLLECTION

In 1961, Nobel Laureate George Stigler wrote "[o]ne should hardly have to tell academicians that information is a valuable resource: knowledge *is* power. Any yet it occupies a slum dwelling in the town of economics. Mostly it is ignored . . . ."[52] In the half-century since, a burgeoning literature has led to significant developments in the field of information economics.[53] There are many legitimate reasons for web property owners to gather, aggregate, and use personally identifiable and non-personally identifiable information about a site visitor, and the law is well-settled that such information can be valuable, confidential information protected by trade secret law.[54] Businesses may want to identify and refine target markets; learn about and predict future spending and inventory needs; improve and track advertising effectiveness; offer complimentary discounts personalized to a consumer;[55] offer coupons designed to encouraged consumers to switch to a competing brand; increase volume of consumers buying store brands or higher-profit-margin items; track timing of purchases to assess staffing needs; develop individualized profiles for more effective introduction of new or complementary products; design products more likely to be successful; and/or engage in a host of other business strategies and decisions.[56] While many consumers might not object to their personal and non-personal information being collected to further business interests or to enhance their shopping experiences, many consumers would likely

---

[52] *See, e.g.*, George J. Stigler, *The Economics of Information*, 69 J. POL. ECON. 213 (1961).

[53] Joseph Stiglitz, *Information and Economic Analysis: A Perspective*, 95 ECON. J. 21, 23–24 (1985).

[54] Brian Yeh, CONG. RESEARCH SERV., R43714, PROTECTION OF TRADE SECRETS: OVERVIEW OF CURRENT LAW AND LEGISLATION 2 (2016).

[55] In this section, we interchangeably use the terms "consumers" and "users."

[56] Yeh, *supra* note 54.

feel differently if data collection and use had a negative impact on them economically. Does or should a consumer's right to informational privacy vary according to how the data about her is being used or to the nature of the interaction between all individuals involved in an interaction? What are the economic implications of consumer online data gathering for both businesses and consumers?

Our understanding of how information impacts economic agents' behavior and market outcomes is significantly richer today than forty years ago. We have a better understanding of how 1) economic agents transmit and receive private information to mitigate market and non-market uncertainty and 2) asymmetrically informed economic agents impact market efficiency and outcomes.[57] Information can serve as an efficient coordination mechanism to match economic agents on two sides of an exchange, improve market efficiency and reduce transaction costs.[58] The impact of asymmetrically informed economic agents on market and non-market environments also has been widely studied.[59] Recent technological innovations have given economic agents on all sides of market interactions greater opportunities to collect, store, and transmit information and have led to more indiscriminate data collection.[60] This market activity, combined with health care legislation in the United States, provides an opportunity to explore the economic value of health information.[61]

---

[57] Stiglitz, *supra* note 53, at 29–30.

[58] Muriel Niederle, Alvin Roth & Tayfun Sonmez, *Matchingversi (Forthcoming in The New Palgrave Dictionary of Economics* 11).

[59] Stiglitz, *supra* note 53; Antonio Cordella, *Transaction Costs and Information Systems: Does IT Add Up?*, 21 J. INF. TECH. 195 (2006).

[60] Ben Rosen, *EU Court Slams Indiscriminate Data Collection, Opening Challenge to British Cyber Law*, CHRISTIAN SCI. MONITOR (Dec. 21, 2016), http://www.csmonitor.com/Technology/2016/1221/EU-court-slams-indiscriminate-data-collection-opening-challenge-to-British-cyber-law.

[61] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,181, 53,254 (Aug. 14, 2002) (to be codified at 16 C.F.R. pt. 160 and 164); *see also* Technical Corrections to the Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,944 (Dec. 29, 2000) (to be codified at 16 C.F.R. pt. 160 and 164).

Rapid innovation in internet technology has created a vast global network of voluntarily interconnected autonomous computer networks built on the Internet Protocol suite: Transmission Control Protocol and Internet Protocol ("TCP/IP").[62] The Internet continues to fundamentally change the ways that individuals acquire and transmit information, connect socially and at work, shop for goods and services, and consume entertainment.[63] Our interconnected world has created significant economic opportunities for information content providers and other intermediaries that create platforms to connect individuals and organizations on both sides of market and non-market interactions.[64] An implication of the autonomous characteristics of the Internet is that it operates without a central governing body.[65] Each constituent network, web property owner, and intermediary platform operator sets its own privacy policies.[66] The pace of advances in internet technology, especially in the area of tracking technologies like those described in sections I.A and I.B, have

[62] The TCP/IP protocol is the standard set of communications protocols that permit users on different computer networks to transmit and receive information. The suite specifies how data is packaged, addressed, transmitted, routed, and received. *See* Vinton Cerf & Robert Kahn, *A Protocol for Packet Network Intercommunication*, 5 IEEE TRANSACTIONS ON COMM. 637 (1974).

[63] INTERNET SOCIETY, THE INTERNET OF THINGS: AN OVERVIEW – UNDERSTANDING THE ISSUES AND CHALLENGES OF A MORE CONNECTED WORLD (Oct. 2015), http://g3ict.org/download/p/fileId_1031/productId_340.

[64] Examples of market-based interactions include: 1) videogame platforms (such as Sony PlayStation, Microsoft X-Box, Nintendo) that act as intermediary between gamers (platform buyers) and game developers; 2) payment card operates act as intermediaries between cardholder (buyer of goods and services) and merchants who accept the intermediaries' payment platform to settle transactions; and 3) online auctions sites (such as eBay) that match buyers and sellers of goods and services. Examples of non-market interactions include: 1) social media sites (such as Facebook) who connect two or more individuals in social contexts and 2) dating platforms that match individuals looking for relationships. *See* Jean-Charles Rochet & Jean Tirole, *Platform Competition in Two-Sided Markets*, 1 J. EUR. ECON. ASS'N 990, 992 (2003).

[65] JOVAN KURBALIJA, AN INTRODUCTION TO INTERNET GOVERNANCE (5th ed. 2012).

[66] Norman Bowie & Karim Jamal, *Privacy Rights on the Internet: Self-Regulation or Government Regulation?*, 16 BUS. ETHICS Q. 323, 330 (2006).

outpaced social norms and legal structures in terms of acceptable practices, especially in the field of privacy.[67]

Markets consisting of intermediaries that create and operate platforms designed to directly connect two (or more) parties in market and non-market interactions are called two-sided (or multi-sided) markets.[68] The literature on two-sided markets refines the research examining demand-side scale economies; the notion is that a good or service's value to one individual depends on the number of other users.[69] The two-sided market literature examines how distinct users of an intermediary's economic platform confer network effects on one another by facilitating direct interaction between the distinct users.[70] Online advertising, price aggregating, and comparison sites are examples of two-sided, or multi-sided, markets.[71]

---

[67] Vivek Wadhwa, *Laws and Ethics Can't Keep Pace with Technology*, MIT TECH. REV. (Apr. 15, 2014), https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/.

[68] Rochet & Tirole, *supra* note 64, at 990.

[69] Demand-side scale economies are also identified as network effects or network externalities. The classic example of a product exhibiting demand-side scale economies is the telephone: the value of telephones is a function of the number of other individuals with a telephone. *See* S.J. Liebowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy,* 8 J. ECON. PERSP. 133, 133–136 (Spring 1994). Demand-side scale economies can be positive or negative. Congestion is an example of a negative network externality: the value of the good or service is less valuable as users' consumption increase. A positive feedback loop, or bandwagon effect, is an example of a positive network effect: the value of a good or service increase as buyers' consumption increases.

[70] The network effects in two-sided markets can be both same-side and cross-side effects, and either positive or negative. *See* Andrei Hagiu, *Strategic Decisions for Multisided Platforms*, MIT SLOAN MGMT. REV. (Dec. 19, 2013), https://tribunecontentagency.com/article/strategic-decisions-for-multisided-platforms/ (explaining that the network effects in two-sided markets can be both same-side and cross-side effects, and either positive or negative).

[71] Rochet & Tirole, *supra* note 64, at 991–92.

A. An Introduction to Online Tracking Technologies and Advertising: How Personal and Non-Personal Information Is Exchanged for "Free" Health-Related Internet Content

According to comScore's MediaMetrix®, an American media and data analytics company, ranking "fifty-six of the top 100 websites based on page views in February 2008 presented advertising," suggesting that online advertising is a significant source of revenue for many web property owners.[72] In 2016, many of the same web property owners remain on comScore MediaMetrix's Top 50 Properties and likely continue to derive significant revenue from advertising.[73] In 2008, the only directly health-related web property on comScore's Top 100 list was AthenaHealth.com (ranked 88).[74] WebMD[75] Health ranked 33rd on comScore's Top 50 Properties list in February 2016 with over twenty-eight million unique visitors from desktop devices.[76]

Online advertising consists of intermediary operators of platforms designed to coordinate the matching problem of delivering advertisers' messages to many potential consumers. There is no single mode or form of online advertising.[77] Indeed, online advertising can take the form of email campaigns, search

---

[72] David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy*, 23 J. ECON. PERSP. 37, 37 (2009).

[73] *comScore Ranks the Top 50 U.S. Digital Media Properties for February 2016*, COMSCORE (March 21, 2016), https://www.comscore.com/Insights/Rankings/comScore-Ranks-the-Top-50-US-Digital-Media-Properties-for-February-2016 (listing websites and their ranks based on the number of unique viewers).

[74] Evans, *supra* note 72 at 41. iVillage.com: The Women's Network also provides some health-related content relevant to primarily women, but also provides much broader media content of interest to women.

[75] WebMD is an online content provider that publishes health news and information to the public. *See generally What We Do for Our Users*, WEBMD, http://www.webmd.com/about-webmd-policies/about-what-we-do-for-our-users (last updated April 29, 2014); *Advertising Policy*, WEBMD, http://www.webmd.com/about-webmd-policies/about-advertising-policy (last updated June 9, 2016); *Privacy Policy*, WEBMD, http://www.webmd.com/about-webmd-policies/about-privacy-policy (last updated Dec. 30, 2016).

[76] *See* comScore, *supra* note 73 (noting that this number rises to 72.5 million unique visitors/viewer from both desktop and mobile devices).

[77] Evans, *supra* note 72, at 38.

engine marketing, social media marketing, or display ads.[78] While advertisers are eager to deliver messages, consumers vary considerably in their willingness to receive online advertising.[79] Thus, effectively targeting online advertisements requires website owners to attract a large number of potential consumers with a wide variety of behavioral patterns to best leverage the variety of advertising delivery techniques.[80]

Many display-ad online advertising platform models exist. Website owners that deliver content directly can publish advertising with their content and act as an intermediary connecting advertising suppliers—like an advertising agency—to potential consumers. This is an example of the website owner using first-party tracking technologies to understand its users' behavior on its own web pages. In this scenario, website owners typically source advertisements from an advertising agency's servers and display ads alongside the website owner's content. This is an example of a two-sided market.[81]

More complex display-ad models exist and include different economic agents. For example, display-ad space may be allocated via auction using an ad exchange, which is a technology platform that hosts advertising inventory from multiple ad networks and facilitates real-time bidding between buyers and sellers for display ads.[82] Specifically, when a user visits a web property owner's pages, a user's personal and non-personal information and a request to fill a blank ad space are then transferred to the publisher's ad server.[83] The user's information and ad-space-for-sale offer are submitted to supply-side ad servers, and the user's

---

[78] *See id*. at 39–40 (analyzing revenues of different online advertising formats).

[79] *See id*. at 39 ("Nevertheless, certain features of the 'online advertising ecosystem' have become clear. On one side of the business are advertisers that want to reach consumers. On the other side are consumers who may or may not be receptive to receiving advertising messages.").

[80] *See id*.

[81] *See id.* at 38.

[82] INTERNET ADVERTISING BUREAU, *How an Ad is Served with Real Time Bidding (RTB) – IAB Digital Simplified*, YOUTUBE (June 19, 2014), https://www.youtube.com/watch?v=-Glgi9RRuJs.

[83] *Id.*

information is submitted to a data-management platform where it is connected to demographic information, such as previous purchase behavior and other information used by advertisers.[84] The user's information and ad-space offer are bundled into an offer, returned to the supply-side platform, and sent to an ad exchange.[85] Then the ad exchange submits the offer on demand-side platforms.[86] Bidders on the demand-side platforms—typically acting on behalf of ad agencies—receive the bundled ad offer supplied by the web property owner and supply-side server and decide how much to bid for the ad space.[87] According to the Internet Advertising Bureau, the demand-side platform has about ten milliseconds to respond to an offer.[88] Once the winning bid is accepted through the ad exchange, both parties are notified of the transaction, and the ad exchange sends the ad link back through the supply-side platform to the web property owner's ad server and ultimately to the user's browser.[89] In this process, a web property owner uses personal and non-personal information about the user accessing its pages; this is an example of third-party tracking technology.[90]

To examine the manifestation of online advertising, let us revisit Pamela's situation. Her internet search about high cholesterol might lead her to the popular information content provider WebMD, depicted in Figure 1.

---

[84] *Id*.
[85] *Id*.
[86] *Id*.
[87] INTERNET ADVERTISING BUREAU, *supra* note 82.
[88] *Id*.
[89] *Id*.
[90] *The Murky World of Third Party Web Tracking*, MIT TECH. REV. (Sept. 12, 2014), https://www.technologyreview.com/s/530741/the-murky-world-of-third-party-web-tracking/.

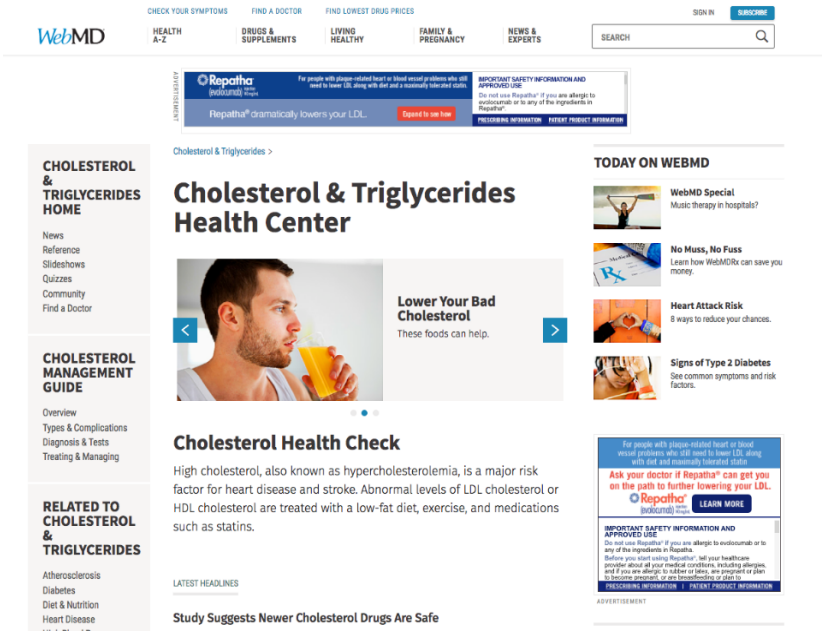

Figure 1: Screenshot of WebMD's Cholesterol and Triglycerides Health Center Content Page[91]

The page contains lots of useful information on high cholesterol, triglycerides, and other health-related content. Under the "Cholesterol Health Check" section is a statement of the health ramifications of high cholesterol and general treatments for abnormal levels of cholesterol.[92] WebMD also provides links to "Latest Headlines" and "Top Stories" related to cholesterol and other health-related content under the "Today On WebMD."[93] To fund this content at no cost to consumers, WebMD sells advertising space alongside the free content.[94] For example, in Figure 1, the LDL-lowering cholesterol statin Repatha® is advertised in two locations on the page.[95] How WebMD's pages source the advertising may have significant implications on health-related consumer privacy.

---

[91] *Id.*
[92] *See* fig. 1.
[93] *See id.*
[94] *See id.*
[95] *See id.*

One possibility is that WebMD is a first-party advertiser and sources its own advertising directly from advertisers. Under this scenario, WebMD directly interfaces with advertisers and avoids advertising through other intermediaries. While WebMD may collect personal and non-personal information, the information is not connected to third-party demographic data nor linked to an individual user. Instead, the WebMD pages populate advertising based on the personal and non-personal user information it collected from the user's account profile and with first-party tracking tools as a user views WebMD's health-related content and pages.[96]

Another possibility is that WebMD could source its advertising through an ad exchange, which is a third-party intermediary that uses a technology platform to facilitate buying and selling of online advertising from multiple ad networks.[97] Prices for these ads are determined through an auction using a bidding process.[98] When WebMD offers to sell an ad space, it bundles the ad offer along with consumer information and submits it to the ad exchange.[99] Third-party advertisers can use the user's personal and non-personal information along with third-party tracking technologies to identify the demographics of the ad recipient (consumer of content) with high probability and connect this information search to the ad recipient.

---

[96] *WebMD Privacy Policy*, WEBMD (Sept. 16, 2017), http://www.webmd.com/about-webmd-policies/about-privacy-policy.

[97] The major ad exchanges include: AppNexus, AOL's Marketplace, DoubleClick (a subsidiary of Google since 2008), Microsoft's Ad Exchange, OpenX, Rubicon Project Exchange, and Smaato. WebMD places no restrictions on the types of advertising in which it can engage. *Advertising Policy*, WEBMD, http://www.webmd.com/about-webmd-policies/about-advertising-policy. Since ad exchanges are a form of third-party tracking, this is a possibility, (last visited Sept. 16, 2017). *Third-Party Ad Server,* KNOW ONLINE ADVERTISING, http://www.knowonlineadvertising.com/advertisingdictionary/third-party-ad-server/ (last visited Sept. 17, 2017).

[98] *Ad Exchange Auction Model*, DOUBLECLICK, https://support.google.com/adxbuyer/answer/6077702?hl=en (last visited Sept. 17, 2017).

[99] *See WebMD Privacy Policy*, *supra* note 96 (explaining the technical details of how a blank ad space gets populated using the ad exchange is described in the previous paragraphs).

A review of WebMD's Privacy Policy reveals that it may collect "personal and non-personal information."[100] These forms of information are used in a variety of ways, but include: "statistically analyze user behavior and activity" and "provide you and other people with similar demographic characteristics and interests with more relevant content and advertisements."[101] The policy also discloses that "[w]e [WebMD] may combine Personal and Non-Personal Information collected by WebMD about you, and may combine this information with information from external sources. Third parties may also use Non-Personal Information in order to display advertising that reflects the interests and preferences of our community."[102] Individuals who prefer that Personal Information not be used by WebMD can: 1) "opt out" of registering with the WebMD community; 2) set browser software to reject Cookies; or 3) "opt out" of Cookies advertisers by visiting the Network Advertising Initiative gateway opt-out site.[103]

A review of WebMD Network's Advertising Policy shows that it accepts advertising from third parties.[104] In addition to providing more general advertising guidelines around the discretion for determining types of advertising displayed and categories of advertisements it will knowingly exclude, WebMD specifies that it uses "Ads by Google" to source "[a]dvertisements that have been purchased by companies that want to have links to their websites appear adjacent to search results in response to specific terms."[105]

An important implication is that health-related information content providers produce and distribute health-related content that is "freely" available to users.[106] To generate revenue, content

---

[100] "Personal information" includes: an individual's name, address, telephone number, email address, and health information. *Id.* "Non-personal information" includes: cookies, web beacons, WebMD mobile device applications, and data from external sources. *Id.*

[101] *Id.*

[102] *Id.*

[103] *Id*.

[104] *See Advertising Policy, supra* note 75.

[105] *Id.*

[106] Some content may require the user to provide profile information in a user account. Thus, "freely" means there is no explicit monetary transaction, but the user does give up some personal information in exchange for the information

providers sell advertising and collect personally and non-personally identifiable information to improve the advertising targeting and efficiency.[107] While content providers and website owners often have explicit privacy and advertising policies, most users are likely unaware of how their personal and non-personal information is used.[108] Opt-out style privacy and advertising policies contribute to the sense of "freely" available content without fully understanding that personally identifiable and non-personally identifiable information implicitly is exchanged for health-related content and other goods and services on the Internet.[109]

B. Internet Technology and Economic Incentives: Price Discrimination

A firm with some degree of market power has an incentive to design price strategies that enhance its profitability. This often leads a firm to charge different prices for identical or seemingly identical goods and services in different markets, a practice known as price discrimination.[110] While multiple forms of price discrimination exist, traditionally the strategies are divided into three categories: 1) first degree—charging each consumer her reservation price;[111] 2) second degree—practice of posting a schedule of declining prices to consumers with different demand

---

content. *See* John Gallaugher, Pat Auger & Anat Barnir, *Revenue Streams and Digital Content Providers: An Empirical Investigation*, 38 INFO. & MGMT. 1, 7 (2001) (discussing the exchange of personal information for content in the context of "freely" available web content).

[107] *See* Evans, *supra* note 72, at 37–56.

[108] *See* Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW RES. CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ (discussing a Pew Research study finding that 47 percent of "Americans struggle to understand the nature and scope of data collected about them").

[109] *See id.*

[110] HAL R. VARIAN, *Price Discrimination*, *in* HANDBOOK OF INDUSTRIAL ORGANIZATION (Richard Schmalensee & Richard D. Willig eds., 1989).

[111] A "reservation price" is the upper limit on the price a consumer would pay for a good or service. *See* Ian Steedman, *Reservation Price and Reservation Demand,* 4 THE NEW PALGRAVE: A DICTIONARY OF ECONOMICS 5537–38 (1987).

but cannot associate buyers and their demand to permit buyers to self-select what to purchase; a classic example is a providing a menu of prices for different quantities or qualities; and 3) third degree—charging different prices to different consumer groups.[112] Each form of price discrimination varies in terms of profitability and information needed to implement the strategies.

Price discrimination is not a new practice and has been successfully and unsuccessfully implemented in both online and traditional markets. Airlines successfully engage in second-degree price discrimination in traditional markets by charging different prices for first-class and coach seats and by charging different prices for the same seat according to how far in advance a ticket is booked from its departure date.[113] In 1999, the Coca-Cola Company tested a variable-price Coke machine. Essentially, the Coca-Cola Company designed a vending machine that can adjust prices based on demand in current market conditions; for example, price adjustment could be positively correlated with the outside temperature or negatively correlated with the time of day and foot traffic.[114] Despite resting on sound economic principles, Coke's variable-price vending machine was met with public disdain as angry Coke drinkers voiced their opinions in Internet chat rooms and newspaper editorials around the world, which led Coke to abandon widespread adoption of the "innovation."[115]

As tracking technologies become increasingly sophisticated, online retailers increasingly are exploring and using different forms of price discrimination. Amazon, for example, uses first- and third-party tracking technologies to engage in price

---

[112] *See* MICHAEL R. BAYE, MANAGERIAL ECONOMICS AND BUSINESS STRATEGY 404–410 (5th ed. 2017).

[113] *See* Tejvan Pettinger, *Airline Price Discrimination*, ECON. HELP BLOG (Feb. 5, 2014), http://www.economicshelp.org/blog/7767/business/airline-price-discrimination/.

[114] Constance L. Hays, *Variable-Price Coke Machine Being Tested,* N.Y. TIMES (Oct. 28, 1999), http://www.nytimes.com/1999/10/28/business/variable-price-coke-machine-being-tested.html.

[115] David Leonhardt, *Why Variable Pricing Fails at the Vending Machine*, N.Y. TIMES (Jun. 27, 2005), http://www.nytimes.com/2005/06/27/business/why-variable-pricing-fails-at-the-vending-machine.html?_r=0.

discrimination.[116] When a consumer makes a purchase from Amazon or one of its affiliates, Amazon collects a name, address, email, phone number, credit card number, IP address, browser type, operating system, purchase history and other information and uses it in a variety of ways.

On the upside, Amazon has designed a platform that enables personalized shopping experiences for its customers by giving them the ability to create "wish lists," access other customer reviews for products, and recommend products through the "Recommended for You" feature, among other features.[117] Amazon's data-rich consumer database is the basis for Amazon's Advertising Platform, which connects advertisers to Amazon shoppers on Amazon's web properties as well as across the Internet and on mobile apps.[118] These are examples of second-degree price discrimination and, in general, appear to be designed to provide Amazon customers with a more personal experience.[119] Data collected using first-party tracking technologies, namely transactions and cookies, are the primary driver behind these personalized shopping experiences.

However, despite these upsides to consumers increasingly sophisticated tracking technologies facilitate the use of something closer to first-degree price discrimination, or dynamic pricing, based on personal and non-personal information. In September 2000, Amazon CEO Jeff Bezos admitted the company charged significantly different prices for the same DVDs in a "randomized price test."[120] More recently, lawsuits filed against Amazon alleged

---

[116] *See* Jakub Mikians et al., *Detecting Price and Search Discrimination on the Internet*, HOTNETS-XI PROCEEDINGS OF THE 11TH ACM WORKSHOPS ON HOT TOPICS IN NETWORKS, 80–82 (2012), https://dl.acm.org/citation.cfm?id=2390245.

[117] *Amazon Privacy Notice*, AMAZON.COM, https://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496#examples (last visited Sept. 17, 2017).

[118] *See id*.

[119] *See* Mikians et al., *supra* note 116, at 80–82.

[120] Anita Ramasastry, *Web Sites Change Prices Based on Customers' Habits*, CNN INT'L (June 24, 2005), http://edition.cnn.com/2005/LAW/06/24/ramasastry.website.prices/. At least one customer reported that Amazon offered a significantly lower DVD price after he deleted cookies identifying himself as a "regular" Amazon customer. *Id.* Bezos' admission of the "randomized pricing

that Amazon Prime's "free" shipping is not free since Amazon Prime members are charged high base prices to cover shipping costs.[121]

Notwithstanding pending litigation, there is nothing inherently illegal about Amazon's price discrimination efforts; firms in other markets have similar practices.[122] Most markets currently do not have restrictions on what personal and non-personal information can be collected and shared. An exception is how personal and non-personal health-related information is collected, stored, and shared as described in HIPAA. As explained more fully in Part IV, this raises the question whether the spirit, if not the letter of HIPAA, may be violated in markets using a two-sided platform, like a third-party ad exchange platform or other platforms using third-party tracking technologies.

Incentives for firms to engage in price discrimination may lead to health-related data collection, storage, aggregation, and sharing practices. For example, suppose our hypothetical patient, Pamela, decides in consultation with her doctor to treat her condition with a combination of diet, exercise, and medication. While browsing WebMD, Pamela saw an advertisement for Repatha, a drug that treats high cholesterol by lowering LDL. She mentions Repatha to her doctor, and they agree on the appropriate treatment for her specific case. To explore the cost of her proposed Repatha

---

test – 'mistake'" included: 1) a statement that Amazon would offer to refund the 6,896 high-paying customers the difference between the price paid and the lowest price during the period, an amount totaling about $21,377.60, *see id.*, and 2) that Amazon did not and never will use consumer demographic data as a basis for test prices, Michael J. Martinez, *Amazon Error May End Dynamic Pricing*, ABC NEWS (Sept. 29, 2016), http://abcnews.go.com/Technology/story?id=119399&page=1. Note, personal and non-personal information are different from consumer demographic data. *See id.*

[121] *See* Jennifer Abel, *Lawsuit Alleges Amazon Charges Prime Members for "Free" Shipping*, CONSUMER AFF. (Mar. 14, 2014), https://www.consumeraffairs.com/news/lawsuit-alleges-amazon-charges-prime-members-for-free-shipping-031414.html; Tricia Duryee, *Lawsuit Alleges Amazon Prime Third-Party Prices Are Inflated to Cover Shipping*, GEEK WIRE (Feb. 24, 2014), http://www.geekwire.com/2014/lawsuit-alleges-amazon-prime-third-party-prices-inflated-cover-shipping/.

[122] *See* John Spacey, *10 Examples of Price Discrimination*, SIMPLICABLE (Jan. 12, 2016), http://simplicable.com/new/price-discrimination.

treatment, Pamela visits www.GoodRx.com, which is a price comparison intermediary (price aggregator) that lists prices of different pharmaceutical retailers on its platform. As an intermediary, GoodRx provides price information on various firms for a broad variety of pharmaceutical products thereby facilitating transactions between potential consumers (in consultations with their doctors) and retail pharmaceutical sellers through the use of coupons on its platform.[123] Pharmaceutical consumers can use GoodRx for "free" to access drug price information and coupons.[124] GoodRx generates revenue by charging referral fees and selling advertising.[125]

A search for Repatha on www.GoodRx.com results in the webpage shown in Figure 2.

[123] *How GoodRx Works*, GOODRX, https://www.goodrx.com/how-goodrx-works (last visited Sept. 17, 2017). According to GoodRx's Privacy Policy, the company does not collect any personal information from users unless a visitor "register[s] to receive certain services," such as price alerts, coupons and discount cards. *Privacy Policy*, GOODRX, https://www.goodrx.com/privacy-policy (last visited Sept. 17, 2017). There are options that require a user to provide an email address, phone number, and/or name and mailing address. *Id.* GoodRx also uses cookie technology "[t]o collect, store and sometimes track information for statistical purposes to improve the service we provide." *Id.* Additional information collected with cookies includes: 1) locational information, 2) drug information accessed while visiting www.goodrx.com, and 3) third-party websites a user visited before accessing www.goodrx.com. *Id.* User information collected via cookies is retained for 30 days and is associated with the user's account information, if an account exists. *Id.* While GoodRx's cookies do not enable third parties to access personally identifiable information, visiting other websites may require the user to accept a third-party cookie. *Id.* GoodRx claims they do not control the use of any third-party cookies deposited from other websites, and "expressly disclaim[s] responsibility for information collected through them [third-party websites]." *Id.*

[124] *How GoodRx Works*, GOODRX, https://www.goodrx.com/how-goodrx-works (last visited Sept. 17, 2017).

[125] *Id.* There is no description that reveals whether GoodRx engages in first-party or third-party advertising practices.

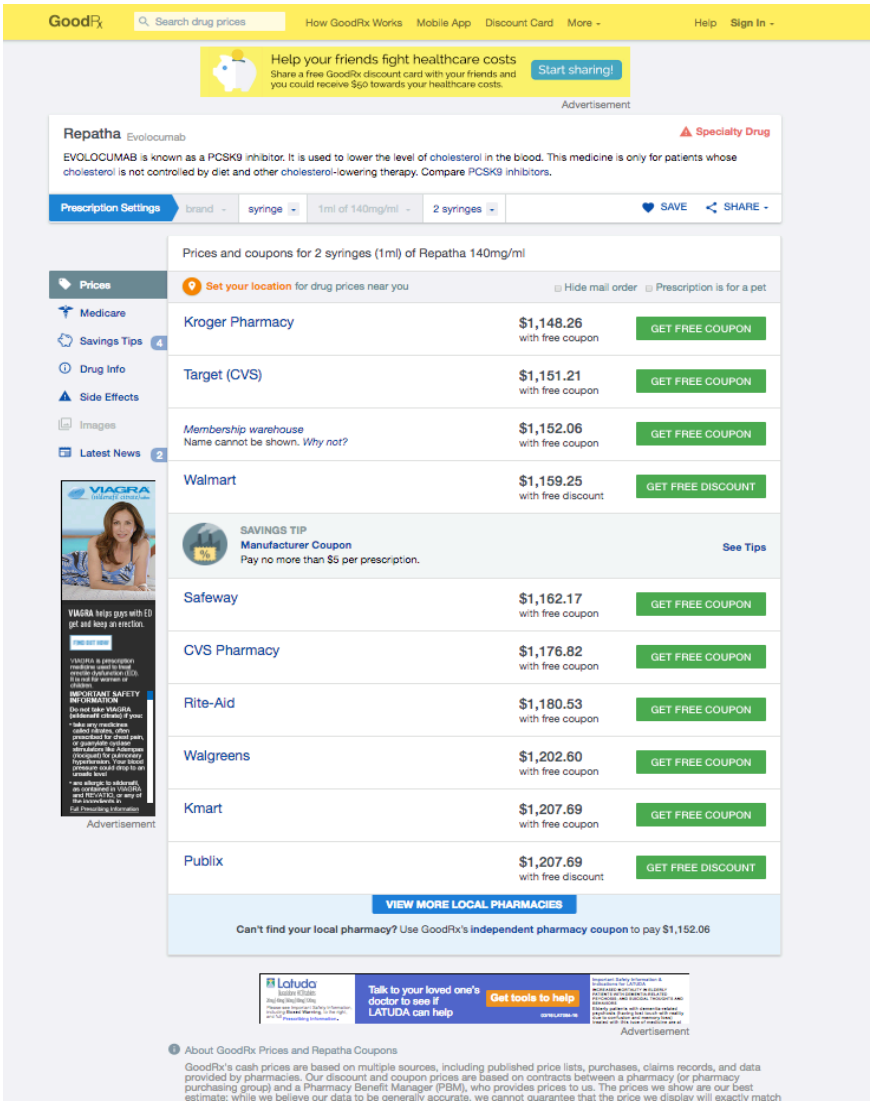

Figure 2: Screenshot of GoodRx's Webpage for Retailers' Prices and Coupons for the Cholesterol-Lowering Drug, Repatha

There are options for our 40-year-old woman to set her location by zip code and sign in to the GoodRx website. Doing either of these *could* permit the companies to charge different prices by zip code or based on other personally or non-personally identifiable

information.[126] A user entering neither piece of information results in a price range between $1,148.66 and $1,207.69 before discounts for two syringes (1 ml) of Repatha 140mg/ml. An open question is whether GoodRx permits pharmaceutical retailers to engage in any form of first-degree, price discrimination based on information collected from consumers on its website. That is, whether each consumer sees a different set of prices based on their personal and consumer information. GoodRx's current privacy policy suggests that information is not shared unless to facilitate a requested transaction.[127] However, the technology exists to engage in this behavior, and absent legislation that delineates boundaries on the management of this health-related information, consumers are left to rely on individual website's privacy policies, which can, and often do, evolve.

To reinforce the speculation that GoodRx has the technical capability to engage in price discrimination, consider the following. A 2016 NPR interview revealed how machine-based algorithms used by the Princeton Review resulted in significantly different online SAT course prices across the nation: prices ranging from $6,600 to $8,400.[128] Asians were almost twice as likely as non-Asians to be charged higher prices for the Princeton Review's online SAT preparation course.[129] Although it was unclear whether Asians were charged higher prices because they were Asian or because they lived in certain zip codes that are

[126] *Prices and Coupons for 2 Syringes (1ml) of Repatha 140mg/ml*, GOODRX, https://www.goodrx.com/repatha?drug-name=repatha (last visited Sept. 17, 2017). Currently, a review of four or five different zip codes does not suggest that individual retailers listing prices on GoodRx charge different prices; however, different retailers are available in different zip codes so the price range varies.

[127] *See Privacy Policy*, *supra* note 124.

[128] *ProPublica Reveals Discriminatory Pricing by Computer Algorithms,* NPR (Oct. 19, 2016, 4:27 PM), http://www.npr.org/2016/10/19/498582157/propublica-reveals-discriminatory-pricing-by-computer-algorithms.

[129] *See id*.

predominantly Asian, the Princeton Review indicated that the discrimination against Asians was not intentional.[130]

Independent of current industry practices, Parts I and II suggest that it is technologically feasible to indiscriminately collect personal and non-personal information. Furthermore, strong economic motivations exist to collect, store, aggregate, and transfer personal and non-personal information that can be linked back to other demographic information. The result: indiscriminate data collection can lead to health-related information being used to identify individuals. Moral and ethical issues aside, this type of indiscriminate data collection raises significant privacy concerns—especially in the realm of health-related information. In Part III, we explore whether there are legal protections available to protect unsuspecting users from this data collection, storage, aggregation, and sharing.

III. LEGAL PROTECTIONS OF INDIVIDUAL PRIVACY

Data aggregation of information obtained from a computer user's search history (as opposed to volunteering information or transactional data) arguably catches the consumer unaware. Would the consumer in the opening scenario be surprised to learn how her search for cardiac information was being used, or even that it was being used at all? While such information is valuable to businesses for ad-revenue generation, better ad targeting, or price discrimination as explained above, how far does and should the protection of business' economic interests go vis-a-vis consumers?

The United States has taken a rather ad hoc approach to data privacy. Those federal statutes that do exist target specific industries such as healthcare, communications, education, financial services, and online data collection regarding minors.[131] Aside from some enforcement actions by the FTC and a smattering of state laws, industry best practices shaped and enforced by company

[130] *Id*. It should be noted that although the Princeton Review seemed to draw lines for their zip code pricing in a way that encompassed primarily high-income areas, also included in this group were many low-income Asians areas. *Id.*

[131] THE WHITE HOUSE, *supra* note 50, at 6.

privacy officers and other privacy professionals are the primary influence of standards of privacy protection.[132]

A. The Historical Roots of Privacy Protection

The ancient, classical Greek[133] notion of privacy as a state of deprivation was turned on its head beginning during the Middle Ages[134] and gained momentum with the explosion of individual rights ideas developed by John Locke and others.[135] Political philosophers invoked the concept of private, as opposed to public, spheres of life "as a way to limit state power and to legitimate the concept of private property."[136] Such a public/private sphere differentiation had obvious and profound influences on the framers of the U.S. Constitution, evident in the wording of the Fourth Amendment: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated but upon probable cause . . . ."[137] The text of the Fourth Amendment embodies the two stated privacy concerns Constitutional framers had: (1) that Fourth Amendment privacy addresses rights of the *private citizen against government intrusion*; and (2) that Fourth Amendment privacy deals with limitations on *physical or spatial intrusion* by the government. While these remain an underpinning for modern-day privacy

---

[132] *Id.*

[133] Ironically, privacy in ancient civilizations was based on a "sense of impoverishment and exclusion," according to noted architectural historian Joseph Rykwert in his article *Privacy in Antiquity,* 68 SOC. RES. 29, 31 (2001). The Ancient Greeks thought that "service to the *polis* or city-state, was the highest calling." Winch, *supra* note 15, at 200. In fact, the word for privacy in Ancient Greek, *idion* (not coincidentally the root for *idiot*) "referred to that which separates one out from the unity of the community, the humanity of the polis." *Id*. at 201. Hannah Arendt noted: "the privative trait of privacy, indicated in the word itself, was all-important: it meant literally a state of being deprived of something . . . [a] man who lived only a private life who – like the slave – was not permitted to enter the public realm or . . . was not fully human." HANNAH ARENDT, THE HUMAN CONDITION 38 (2nd ed. 1958).

[134] Winch, *supra* note 15, at 200.

[135] David Gray, *Fourth Amendment Remedies as Rights: The Warrant Requirement*, 96 B.U.L. REV. 425, 450 (2016).

[136] *Id.*

[137] U.S. CONST. amend. IV.

rights, both notions of privacy and the corresponding privacy law have evolved considerably.

During the founding of the United States, privacy concerns centered on the individual's right to prevent intrusion by the government, not by other private individuals or businesses. Philosophical writings of the time evince this vein of thinking, revealing the natural reaction to an emergence from British imperial rule as well as with the general and long-standing historical division between "public" and "private" life. This was the backdrop for the Fourth Amendment's protection of individuals against unreasonable searches and seizures and its progeny recognizing a reasonable expectation of privacy.[138] In the landmark case *Katz v. United States,*[139] Justice Harlan stated in his concurring opinion that the Constitution protects people (not places) against unreasonable searches and seizures by a reasonable expectation of privacy, which involves two requirements: "first that a person ha[s] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[140] Indeed, the Fourth Amendment's "origin and history clearly show that it was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon other than governmental agencies."[141]

---

[138] For a thoughtful article evaluating and criticizing the "reasonable expectation of privacy" standard, *see generally* Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843 (2002). Among the flaws Professor Spencer points out are: reasonable expectations of privacy involve constantly-shifting expectations; it is subject to disproportionate influence by major businesses and powers; reasonable people could disagree as to their expectations of privacy; such disagreement could vary regionally, creating particular problems for the United States Supreme Court; and increased technological advancement can lead to a corresponding decrease in privacy. *Id.*

[139] Katz v. United States, 389 U.S. 347 (1967).

[140] *Id.* at 361.

[141] Burdeau v. McDowell, 256 U.S. 465, 475 (1921). Other cases have held that a private parties' wrongful search and seizure does not violate the Fourth Amendment and, therefore, does not deprive the government of using that evidence lawfully received by the private party. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 125–26 (1984); State v. Watts, 750 P.2d 1219, 1223, 1225 (Utah 1988) (finding that the informant was not acting as a government agent when he searched the defendant's premises, the Supreme Court of Utah

The extensive line of Fourth Amendment cases deciding what constitutes unreasonable search and seizure is of limited applicability here. While it is tempting to utilize definitions of (and glean examples of) reasonable expectations of privacy from these cases, potential privacy intrusions by the government are not analogous to potential privacy intrusions by business. The history behind and rationale for limiting governmental intrusion (and the accompanying harms to individuals and society) do not parallel the history, rationale, ethical considerations, or type of injury experienced by consumers when businesses profile their health-related data in detail based on online searches and the like. Statutes and cases decided in the context of consumer information provide far more relevant guidance.[142]

The historical development of the right to be free from certain types of non-governmental intrusion stems largely from the thoughtful and influential work *The Right to Privacy*.[143] Giving the modern reader an eerie sense of déjà vu, Warren and Brandeis reveal that their motivation and determination in writing an article to advance privacy theory was: technological advancement. Writing in 1890, they asserted that one justification for expanding certain privacy rights beyond situations where courts could identify breach of contract or breach of confidence/trust type theories was "now that modern devices afford abundant opportunities for the

---

upheld defendant's conviction). In *Jacobsen*, Federal Express personnel discovered a package that had been accidentally torn open by a forklift. 466 U.S. at 111. Upon examining the contents, consistent with written company policy and necessary for insurance purposes, they became suspicious and contacted the Drug Enforcement Administration. *Id.* The contents, it turns out, were cocaine. *Id.* The United States Supreme Court held that "federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as the result of private conduct." *Id.* at 126. In *Watts*, an unidentified informant met a police officer near the defendant's home and pointed out to the officer a shed located on the defendant's property and voiced suspicions as to the shed's use for the cultivation of marijuana. 750 P.2d at 1220. Upon returning to the premises with a warrant and finding no one home, police searched the shed and seized material which ultimately proved to be marijuana. *Id.*

[142] Lior Jacob Strahilevitz*, A Social Networks Theory of Privacy,* 72 U. CHI. L. REV. 919 (2005).

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

perpetration of . . . wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation."[144]

Much of this oft-cited article focuses on issues relating to the public revelation of facts or ideas which a person would expect to be confidential. In a general sense, Warren and Brandeis detailed the exact discomfort that many privacy advocates have complained of:

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.[145]

Since Warren and Brandeis' seminal article, rights to privacy protection against non-governmental individuals and entities have developed tremendously, at both federal and state levels.[146]

B. Federal Standards

At the federal level, some limited privacy protections are provided by statutory law and by the administrative efforts of the Federal Trade Commission ("FTC"). The FTC is an independent federal agency with the twofold mission of (1) consumer protection and (2) enhancing industry competition.[147] As part of its responsibilities, the FTC addresses a variety of practices that impact consumers, including those behaviors that may violate a consumer's lawfully protected privacy rights.[148] The FTC's goals in privacy work are "to protect consumers' personal information and ensure that consumers have the confidence to take advantage of the many benefits offered in the marketplace."[149]

---

[144] *Id.* at 211.
[145] *Id*. at 196.
[146] Irwin R. Kramer*, The Birth of Privacy Law: A Century Since Warren and Brandeis,* 39 CATH. UNIV. L. REV. 703 (1990).
[147] FED. TRADE COMM'N, *Privacy & Data Security Update,* 1 (2015), https://www.ftc.gov/reports/privacy-data-security-update-2015.
[148] *Id.*
[149] *Id.*

1. Federal Statutes

Congressional curtailment of businesses' use of consumer information has been driven largely by consideration of: (1) *who* is using the information and (2) *what* the information is *about*—financial, medical, videotape, etc. Major federal legislation relating to businesses' use of consumer information has been piecemeal, often targeting restrictions for one specific sector or industry such as those described below.

The Fair Credit Reporting Act of 1970 ("FCRA")[150] applies to consumer reporting agencies, permitting them to release a consumer report only to a court, to the consumer him/herself, or to a person the consumer reporting agency has reason to believe intends to use the information for specifically enumerated purposes (such as evaluating the consumer's creditworthiness for extending credit).[151] A consumer reporting agency's release of target marketing information to vendors violates the FCRA because such information is not necessary for lenders in their pre-screening process.[152]

The Gramm Leach Bliley Act ("GBLA") of 1999[153] mandates that financial institutions take appropriate safeguards "to insure the security and confidentiality of customer records and information."[154] For these purposes, "financial institutions" include but are not limited to: banks, savings associations, and insurance providers, as well as brokers, dealers, investment companies, and

---

[150] 15 U.S.C. § 1681 (2016).

[151] Other purposes include the review or collection of an account of the consumer's; employment purposes; underwriting insurance; eligibility for a license or other government-issued benefit for which investigation of the applicant's financial responsibility is legally mandated; review by current or potential investors valuing credit risks and obligations; a legitimate business need for the information in connection with a business transaction initiated by the consumer; or a legitimate business need to review whether a consumer continues to meet the terms of an existing account. *Id.* § 1681(b).

[152] In re Trans Union Corp. Privacy Litig., 326 F. Supp. 2d 893 (N.D. Ill. 2004).

[153] 15 U.S.C. § 6801 (2016).

[154] *Id.* § 6801(b)(1).

investment advisers under the jurisdiction of the U.S. Securities and Exchange Commission ("SEC").[155]

The Health Insurance Portability and Accountability Act ("HIPAA")[156] and its accompanying regulations promulgated by the Department of Health and Human Services[157] require that health care providers, administrators and employees of health care plans, healthcare clearinghouses and health insurance companies protect the privacy of individually identifiable health information.[158] HIPAA will be revisited and explored more fully in Part IV.

2. Regulatory Efforts

Since the 1990s, the FTC has been seeking ways to address privacy concerns regarding the data gleaned from individuals' Internet activities.[159] In its 2009 report, "Self-Regulatory Principles for Online Behavioral Advertising," the FTC advocated self-regulation of the industry.[160] In response, leaders in the advertising

---

[155] *Id.* § 6805(a).

[156] Health Insurance Portability and Accountability Act, Pub. L. No. 104–191, 110 Stat. 1998 (1996).

[157] D'Lisa Simmons, *Impact of HIPAA and the Privacy Rule*, HOUSTON LAWYER (May/June 2006), http://www.thehoustonlawyer.com/aa_may06/page20.htm. *See generally* 45 C.F.R. § 160.408 (2016).

[158] Interestingly, as argued in *The HIPAA Privacy Regulation – Troubled Process, Troubling Results,* a Special Report issued by Privacilla.org in April 2003, Congress "punted" on the issue of privacy protection under HIPAA:

> Congress . . . wondered aloud what privacy was and how it should be protected . . . [and] asked the Secretary of Health and Human Services to make recommendations to Congress about the privacy of individually identifiable health information [and then] told the Secretary of HHS to go ahead and write into law whatever the recommendations were if Congress did not act.

The HIPAA Privacy Regulation – Trouble Process, Troubling Results, Privacilla.org (Apr. 2003), http://www.privacilla.org/releases/HIPAA_Report.html.

[159] Courtney A. Barclay, *A Comparison of Proposed Legislative Data Privacy Protections in the United States*, 29 COMPUTER L. AND SEC. REV. 359, 360 (2013).

[160] FED. TRADE COMM'N, *Staff Report: Self-Regulatory Principles for Online Behavioral Advertising, Behavioral Advertising: Tracking, Targeting, and Technology* (2009), https://www.ftc.gov/sites/default/files/documents/reports/

industry proposed guidelines aimed at improving transparency and making consumers aware of privacy policies and opt-out tools.[161] Although industry leaders came together to discuss more transparent processes to protect consumers' privacy, progress was slow. The FTC expressed displeasure with the industry's slow pace toward reform and instead proposed in 2010 that a simple do-not-track mechanism be offered to consumers to allow consumers to easily opt out of data protection.[162] Earlier that year, the *Wall Street Journal* released an investigative series of articles, "What They Know," which examined the quickly-growing business of spying on consumers.[163] This series revealed that, on average, more than 60 pieces of tracking technology are installed on a user's computer by the most frequently used 50 websites.[164] This brought concerns of data privacy to national attention. Testifying before Congress in 2010, then-director of the FTC's Bureau of Consumer Protection David Vladeck told House members that "the Commission supports a more uniform and comprehensive consumer choice mechanism for online behavioral advertising."[165] Such an approach would essentially place a persistent cookie on a browser which would then alert websites visited whether the consumer consents to being tracked.[166] Although the FTC called on the industry, specifically the World Wide Web Consortium, to help design how Do Not Track would work, a final workable solution was never

---

federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

[161] Barclay, *supra* note 159, at 360.

[162] FED. TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, 66 (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

[163] Barclay, *supra* note 159, at 359.

[164] *Id.* at 359–60.

[165] FED. TRADE COMM'N, *FTC Testifies on Do Not Track Legislation* (Dec. 2, 2010), https://www.ftc.gov/news-events/press-releases/2010/12/ftc-testifies-do-not-track-legislation.

[166] *Id.*

achieved "despite years of meetings and thousands of emails."[167] Significantly, prominent members of the consortium group walked away from the Do Not Track efforts, citing frustration at the process.[168] For example, the Digital Advertising Alliance, a consortium of some of the biggest ad-technology companies, withdrew from the group in September 2013 complaining that the group was not capable of developing a workable solution.[169] Consumer Watchdog, a California-based advocacy group, also withdrew from the Digital Advertising Alliance in 2014, concerned that even if standards were developed, they would only be voluntary and would offer no incentive for online companies to comply with a consumer's Do Not Track request.[170] Although the group ultimately released a proposed set of rules in August 2015, this proposal was met with criticism from members of Congress and from third-party ad tech companies because the proposed rules created a double standard that permitted Internet publishers with direct consumer relationships, such as Google or Facebook, to track customer information, but imposed stricter privacy rules on third-party independent ad companies.[171] To date, none of the various pieces of Do Not Track legislation that were introduced in Congress have succeeded in becoming law.[172]

Even if industry standards were adopted, such action would not ensure industry compliance. Consider, for example, Google's actions in Canada. Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"), enacted in 2000, mandates that targeted advertising cannot be generated through the

---

[167] Dawn Chmielewski, *How 'Do Not Track' Ended Up Going Nowhere*, RECODE.NET (Jan. 4, 2016, 5:00 AM), http://www.recode.net/2016/1/4/11588418/how-do-not-track-ended-up-going-nowhere.

[168] *Id*.

[169] *Id.*

[170] *Id.*

[171] *Id*.

[172] Do Not Track Online Act of 2015, S. 2404, 114th Cong. (2015) (sponsored by Senator Richard Blumenthal, D–CT); Do Not Track Online Act of 2013, S. 418, 113th Cong. (2013) (sponsored by Senator John D. Rockefeller, D–WV); Do Not Track Online Act of 2011, S. 913, 112th Cong. (2011) (sponsored by Senator John D. Rockefeller, D–WV).

use of sensitive personal data.[173] Specifically, Canadian law Principle 4.3 states that "the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate."[174] Principle 4.3.6 states that "[a]n organization should generally seek express consent when the information is likely to be considered sensitive."[175] Sensitive personal data includes information about a person's health.[176] For information that is less sensitive, implied consent would generally be adequate.[177] In 2012, the Canadian Privacy Commissioner issued behavioral guidelines, stating that "[i]t is inappropriate for sensitive health information to be used in behavioral advertising."[178] On this point, Privacy Commissioner Chantal Bernier stated: "As Canadians spend more and more time online, they create a digital trail [clickstream data] that can reveal a great deal about a person. Organizations such as Google must ensure privacy rights are respected in this complex environment."[179]

Operating within Canada, Google's privacy policy explicitly stated that the company would not associate cookies with information about an individual's health, sexual orientation, religion, or race.[180] Despite this assurance, the Office of the Privacy Commissioner of Canada found that Google violated Canada's

---

[173] Susan Krashinsky Robertson, *Google Broke Canada's Privacy Laws with Targeted Health Ads, watchdog says*, GLOBE & MAIL (Jan. 15, 2014, 12:37 PM), http://www.theglobeandmail.com/technology/tech-news/google-broke-canadas-privacy-laws-with-targeted-ads-regulator-says/article16343346/.

[174] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 P. 7 (Can.).

[175] *Id.* at 48.

[176] *Id.*; *see also* PIPEDA Report of Findings #2014-001 (Jan. 14, 2014), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-001/.

[177] *Id*.

[178] NIRICO SYSTEMS, INC., *Google Breaks Privacy Laws in Canada By Using Sensitive Health Information*, https://www.nirico.com/google-breaks-privacy-laws-in-canada-by-using-sensitive-health-information/ (last visited Sept. 17, 2017).

[179] *Id*.

[180] *Id.*

privacy laws through its use of targeted online advertising.[181] The Office of the Privacy Commissioner began its investigation into Google's activities in response to a consumer complaint. A consumer who had searched for devices for sleep apnea noticed that even when he was on other sites, ads were popping up from Google's AdSense promoting similar devices.[182] If Google acted contrary to Canadian privacy laws and contrary to its own stated privacy policy, how much more skeptical should we be of a search engine's ability to respect privacy rights when the primary motivator is merely self-regulation?

In 2012, President Obama introduced the Consumer Privacy Bill of Rights "as a blueprint for privacy in the information age."[183] The purpose of this action was to offer consumers guidance on the expectations that companies and individuals handling consumers' personal information should meet.[184] He urged Congress to pass legislation codifying the Consumer Privacy Bill of Rights that would allow both the FTC and state attorneys general to enforce the rule's mandates.[185] The proposal also recommended a safe harbor provision that would allow companies to utilize their own company code of conduct as a means of compliance with the Consumer Privacy Bill of Rights, as long as such code was approved by the FTC.[186] Congress never enacted the Consumer Privacy Bill of Rights, and now with the change in administration, the bill has been moved off the Whitehouse.gov website and into the White House archives. These efforts were, however, a step in the right direction and will be revisited in Part V.

In October 2016, the Federal Communications Commission ("FCC") issued new rules that limited Internet service providers'

---

[181] Robertson, *supra* note 173; *see* ruling at PIPEDA Report of Findings #2014-001 (Jan. 14, 2014), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-001/.

[182] *Id.*

[183] THE WHITE HOUSE, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

[184] *Id*.

[185] *Id.*

[186] *Id.*

("ISPs") use of customer data.[187] The executive director of the Center for Digital Democracy called the rule adoption "the best day we've had on Internet privacy—commercial Internet privacy—maybe ever."[188] Under the new requirements, Internet providers had to obtain a user's consent before using information or sharing information with third parties.[189] The rules were designed to apply to Internet providers but not to other companies such as Google and Facebook.[190] As a result, critics of the new regulations complained that "[t]here is no lawful, factual, or sound policy basis to justify a discriminatory approach that treats ISPs differently from some of the largest companies in the Internet ecosystem that engage in similar practices."[191] In fact, in the first half of 2016, Facebook and Google combined accounted for 70% of online advertising, and together they were responsible for nearly all the 2016 growth in online advertising.[192] However, before the FTC's new rules could go into effect, they were repealed by Congress in March 2017.[193]

C. State Efforts

The federal government's piecemeal approach to consumer privacy and failure to provide comprehensive reform has led some to look to the states for online privacy protection. Some states have looked no further than their state constitution for consumer privacy protection. In some cases, state statutes or state common law help

---

[187] Brian Fung & Craig Timberg, *The FCC Just Passed Sweeping New Rules to Protect Your Online Privacy*, WASH. POST (Oct. 27, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/10/27/the-fcc-just-passed-sweeping-new-rules-to-protect-your-online-privacy/?utm_term=.7177ddc176dd.

[188] *Id.*

[189] *Id.*

[190] *Id.*

[191] *Id.*

[192] Hal Singer, *We Should Welcome Trump's Reversal of FCC Digital Privacy Rules*, FORBES (Feb. 2, 2017), http://www.forbes.com/sites/washingtonbytes/2017/02/02/how-many-regulators-does-it-take-to-protect-our-digital-privacy/#43d88de86d21.

[193] David Shepardson, *Trump Signs Repeal of U.S. Broadband Privacy Rules*, REUTERS (Apr. 3, 2017), http://www.reuters.com/article/us-usa-internet-trump-idUSKBN1752PR.

protect consumer privacy. We examine the relevant state landscape in this section.

1. State Constitutions

Beyond the Fourth Amendment federal constitutional protection of privacy from government intrusion, some states specifically provide a measure of privacy against private, non-government entities. California,[194] Hawaii,[195] and Illinois[196] guarantee privacy rights specifically in the text of their constitutions. Some other states' constitutions grant a right to privacy that applies only to state actions, such as Alaska,[197] Arizona,[198] Florida,[199] Louisiana,[200] and South Carolina.[201] Yet other

---

[194] CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").

[195] HAW. CONST. art. I, § 6 ("The right of the people to privacy is recognized and shall not be infringed without a showing of a compelling state interest . . . "); Op. Att'y Gen. No. 94–01 (1994) (revealing that one of the purposes intended by the Hawaiian legislature was to guard against "possible abuses in the use of highly personal and intimate information in the hands of the government *or private parties*.") (emphasis added).

[196] In *In re Minor*, the Supreme Court of Illinois noted that "[i]t is clear from the debates in the Sixth Illinois Constitutional Convention that . . . . [Illinois' constitutional right to privacy] was intended to protect an individual's privacy from invasions or injuries caused by another *nongovernmental* individual or company." *In re Minor*, 595 N.E.2d 1052, 1056 (Ill. 1992).

[197] *See Miller v. Safeway, Inc.*, 102 P.3d 282 (Alaska 2004) (holding that a grocery store clerk's right to privacy under the Alaska constitution had not been infringed because there was no state action).

[198] *See* Cluff v. Farmers Ins. Exchange, 460 P.2d 666, 669 (Ariz. 1969) (denying that the Arizona constitutional right to privacy gives rise to a private cause of action between private individuals); *see also* ARIZ. CONST ART. II, § 8 (right to privacy).

[199] FLA. CONST. art. I, § 23 ("Every natural person has the right to be let alone and free from governmental intrusion into the person's private life . . .").

[200] LA. CONST. art. I, § 5 ("Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy.").

[201] S.C. CONST. art. I, § 10 ("The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated, and no warrants shall issue but upon probable cause, supported by oath or affirmation, and

states' constitutions extend the right to privacy only to voter registration-related issues.[202]

Several California cases help illustrate the circumstances under which successful consumer privacy actions brought under state constitutional provisions against non-government parties. In *Pioneer Electronics v. Superior Court of Los Angeles County,*[203] the plaintiff bought an allegedly defective DVD player from Pioneer Electronics.[204] In seeking to bring suit on his own behalf and on behalf of others similarly situated, he asked through discovery request for identifying information about others who had complained about this particular DVD model.[205] Pioneer responded that it could not disclose the names because to do so would violate the California state constitutional right to privacy.[206] Ultimately, the California Supreme Court found no abuse of discretion in the trial court's order requiring Pioneer to convey information on the customers who had purchased its DVD players and held that requiring the customers to opt-out would be sufficient.[207] In its rationale, the court relied on a three-part test: (1) would the customers have expected their information to be confidential unless they affirmatively opted out; (2) was there serious invasion of privacy in releasing the information; and (3) the interests of the plaintiff in wanting to learn the data is weighed against the possibility of customers failing to receive the opt-out notice and objecting to the data's release.[208] In brief, the California state constitutional privacy provision only protects an individual's expectation of privacy against a serious invasion.[209]

In 2011, the California Court of Appeals re-visited the topic of consumer privacy rights under the California Constitution. In *Los*

---

particularly describing the place to be searched, the person or thing to be seized, and the information to be obtained").

[202] *See, e.g.,* ARK. CONST. amend. LI, § 6; WYO. CONST. art. VI, § 11.

[203] 150 P.3d 198 (Cal. 2007).

[204] *Id.* at 199.

[205] *Id.* at 200.

[206] *Id.*

[207] *Id.*

[208] *Id.* at 205–06.

[209] *Id.* at 207.

Angeles Gay and Lesbian Center v. Superior Court,[210] the court made a critical distinction between general consumer information (as in the DVD player customers) and health-related consumer data.[211] In that case, a health center servicing gay, lesbian and transgender people in Los Angeles accidentally administered bicillin C-R instead of bicillin L-A medication to about 663 patients who were suspected to have syphilis.[212] Some patients who had been treated with the wrong medication brought suit against the Center and during discovery requested a list of all the other patients who had been similarly treated with the wrong medication.[213]

Relying on the California Constitution's right to privacy, the California Appeals Court held that, in contrast to the *Pioneer* case, such a list could not be released.[214] Applying the test articulated in *Pioneer,* the court distinguished between health information and general consumer information[215] and stated:

> The class members' medical records are private . . . . [P]laintiffs have a reasonable expectation in the privacy of their medical information at the Center given the extremely sensitive nature of the information contained in them (sexually transmitted disease, possible HIV status, and sexual orientation) . . . [and] the proposed invasion here, namely, disclosure to a wide array of third persons in connection with the litigation, is serious in nature, scope and potential impact. Thus, we must balance the competing interests at stake here—the benefits of efficient litigation where disclosure does not require the class members' consent and class-wide recovery against the Center versus the class members' interest in controlling how this sensitive information is disseminated.[216]

In addition to the protection afforded under some states' constitutions, some states have enacted statutes affording privacy rights against non-governmental entities. For example, Massachusetts General Law provides that "[a] person shall have a right against unreasonable, substantial or serious interference with

---

[210] 125 Cal. Rptr. 3d 169 (2011).
[211] *Id.* at 184.
[212] *Id.* at 172.
[213] *Id*.
[214] *Id*. at 186.
[215] *Id.* at 184.
[216] *Id.*

his privacy."[217] In a class action suit, the plaintiffs' allegation in *Weld v. CVS*[218] that CVS drug store had violated the Massachusetts privacy statute through the use of sharing consumers' drug prescription data survived summary judgment.[219] The *Weld* case dealt with the legality of a direct mailing program established by CVS.[220] CVS sent targeted customers mailings which reminded them to fill prescriptions, informed them of new drugs that might be of interest to them, and encouraged them to discuss potential medical conditions with their doctors.[221] The letters stated the name of the drug manufacturer that funded that mailing.[222] CVS transferred all prescription information to a third party, Elensys, to handle the mailing logistics and Elensys in turn contracted with a company to physically send out the mailings.[223] The CVS/Elensys agreement contained strict confidentiality provisions.[224]

Almost immediately after the press began reporting on the program in February 1998, CVS terminated the program, presumably in response to significant negative publicity.[225] But CVS's Motion for Summary Judgment, decided in June 1999, survived on the count alleging violation of Massachusetts's privacy law.[226] In its decision, the court noted the plaintiffs' complaint about not just the *use* of the information CVS had about the plaintiffs, but also the systematic *searching* of the plaintiffs' prescription records.[227] Such a situation could constitute a violation

---

[217] MASS. GEN. LAWS ch. 214, § 1B (2016).
[218] No. 98-0897F, 1999 Mass. Super. LEXIS 261, at 1 (Mass. June 1, 1999).
[219] *Id.*
[220] *Id.* at 2.
[221] *Id.* at 3.
[222] *Id.*
[223] *Id.* at 5.
[224] *Id.* at 6.
[225] Rudolph A. Pyatt, *Ultimately, A Healthy Decision at Giant and CVS Pharmacy*, WASH. POST (Feb. 23, 1998), https://www.washingtonpost.com/archive/business/1998/02/23/ultimately-a-healthy-decision-at-giant-and-cvs-pharmacy/d96ffe44-b944-437e-874f-3d31593b94d5/?utm_term=.d587a5895e0d.
[226] *Weld*, 1999 Mass. Super. LEXIS 261, at 16.
[227] *Id.* at 14.

of privacy "that is both unreasonable and substantial or serious," as required under the Massachusetts privacy statute.[228]

Later, in 2007 a superior court in Massachusetts dismissed a plaintiff's claim in a similar case. In *Kelley v. CVS*,[229] CVS had an arrangement with Merck & Co., Inc. to mail letters that had been approved by Merck to CVS customers who had filled certain prescriptions.[230] CVS identified, based on prescription records, which customers should receive Merck's letters and then CVS again contracted Elensys (a third-party) to prepare and send letters to the identified customers.[231] The plaintiff filled a prescription for diabetes medication, received one such letter,[232] and sued for privacy rights violation.[233] In sustaining the defendants' motion for summary judgment on this count, the court found that there was no showing of substantial or serious interference with the plaintiff's privacy.[234] In part, this was because the plaintiff had already disclosed his diabetes condition to several people, making no secret of it.[235] In addition, Elensys received no information from CVS about the plaintiff's diagnosis or condition.[236]

2. State Common Law

States' approaches to common law invasion of privacy lack uniformity. Further complicating this area of law, some states' privacy legislation has preempted common law invasion of privacy claims.[237] Traditionally, courts have referenced the four types of invasion of privacy actions, in line with those identified by *Prosser* in *2d Restatement of Torts*: (1) unreasonable intrusion upon the seclusion of another; (2) appropriation of a person's name or

---

[228] *Id.*
[229] No. 98-0897-BLS2, 2007 Mass. Super. LEXIS 381 (Mass. Aug. 24, 2007).
[230] *Id.*
[231] *Id.*
[232] *Id.* at 2.
[233] *Id.* at 4.
[234] *Id.* at 5.
[235] *Id.* at 7.
[236] *Id.* at 6.
[237] *See* Weld, *supra* note 218, at 21 (stating that a tortious misappropriation claim "is probably preempted by" the Massachusetts privacy statute); *see also* MASS. GEN. LAWS ch. 214, § 1B (2016) (privacy statute).

likeness (3) publication of private facts; and (4) publication of facts which place a person in a false light. Some, but not all, states recognize all four types of privacy invasion.[238] A few jurisdictions, such as Massachusetts[239] and Maryland,[240] recognize a cause of action for negligent invasion of privacy, but others, like Michigan, require intent.[241] Of the four types, only unreasonable intrusion upon a person's seclusion and publication of private facts are potential candidates for invasion of *informational* consumer health privacy discussed here. "Publicity" in this context means "communicating the matter to the public at large or to so many persons that the matter must be regarded as one of general knowledge."[242] We examine cases involving online activity leading to the transfer of information to third parties and claims of intrusion on seclusion and public disclosure of private facts claims in this section.

Courts have distinguished facts that are private from those that are personal[243]; a fact must be "private" to succeed under an invasion of privacy claim. For purposes of invasion of privacy claims, matters of public record, such as name, address, date of birth and marriage, are not private.[244] In *Busse v. Motorola*[245] a

---

[238] Illinois, for example, recognizes all four types. Cooney v. Chi. Pub. Schs., 943 N.E.2d 23, 31–32 (Ill. App. Ct. 2010) (quoting Busse v. Motorola, Inc., 813 N.E.2d 1013, 1017 (Ill. App. Ct. 2004)). New York, however, recognizes only misappropriation as a basis for invasion of privacy claims. Gaeta v. Home Box Office, 645 N.Y.S.2d 707, 707 (N.Y. Civ. Ct. 1996).

[239] *See* Barnes v. Town of Webster, No. 04-2420, 2005 Mass. Super. LEXIS 480, at *3–4 (Mass. Oct. 11, 2005).

[240] *See* Bailer v. Erie Ins. Exchange, 687 A.2d 1375, 1380–81 (Md. 1997).

[241] In a class action suit, the medical records of a group of 159 patients accidentally became available on the internet and "Google's automated web crawler . . . indexed the information, thereby making it possible to find patient information through Google's search engine." Despite the fact that the disclosure involved patient medical information, the court ruled that there was no invasion of privacy because the disclosure was accidental. Doe v. Henry Ford Health System, 865 N.W.2d 915, 918 (Mich. Ct. App. 2014) *cert. denied*, No. 1509378, 2015 Mich. LEXIS 1995 (2015).

[242] Roehrborn v. Lambert, 660 N.E.2d 180, 184 (Ill. App. Ct. 1995).

[243] *Cooney*, 943 N.E.2d at 32.

[244] Busse v. Motorola, Inc., 813 N.E.2d 1013, 1018 (Ill. App. Ct. 2004). Other courts have concluded that names and addresses are not automatically

cellular phone customer brought a class action alleging, *inter alia*, that a cellular phone service company and others intruded on seclusion by transferring customers' names, addresses, birthdates, social security numbers, cellular phone numbers and other information to a private research firm for studying a possible link between cell phone use and mortality. In determining only the element of requiring that intrusion be upon *private* matters, the Appellate Court of Illinois held that none of the information transferred was in fact private.[246] In its interpretation of *Busse*, the court in *Cooney v. Chicago Public Schools* stated that the part of the distinction between personal information and private facts is that the latter are "facially embarrassing and highly offensive if disclosed."[247] Even household income, credit limits, credit card balances and credit purchase history is not necessarily "private" for purposes of an invasion of privacy claim of intrusion upon seclusion.[248]

Other courts have held that social security numbers are private[249] and that "[e]mployees' family matters, health problems, and sex lives" are "clearly private."[250] If the plaintiff's privacy claim is based on public disclosure of private facts, then it is also

---

considered public information. In *Weld*, the Massachusetts Superior Court held that plaintiffs who were drug store customers "have not similarly relinquished any expectation of privacy" in their names and addresses the way public school employees have. *Weld v. CVS Pharm.*, No. 98-0897F, 1999 Mass. Super. LEXIS 261, at *12 (Mass. June 1, 1999). The United States Supreme Court held that "[m]erely because [a fact] can be found in a public recor[d] does not mean that it should receive widespread publicity if it does not involve a matter of public concern." United States Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 763 n.15 (1989) (quoting W. Keeton, D. Dobbs, R. Keeton & D. Owens, Prosser & Keeton on Law of Torts § 117, p. 859 (5th ed. 1984)).

[245] *Busse*, 813 N.E.2d 1013.

[246] *Id.*

[247] *Cooney*, 943 N.E.2d at 32.

[248] Bovay v. Sears Robuck & Co., 994 N.E.2d 665, 677–78 (Ill. App. Ct. 2013).

[249] *Busse*, 813 N.E.2d at 1018; City of Kirkland v. Sheehan, No. 01-2-09513-7 SEA, 2000 WL 1751590, 7 (Wash. Super. Ct. May 10, 2001).

[250] Johnson v. Kmart Corp., 723 N.E.2d 1192, 1196–97 (Ill. App. Ct. 2000).

necessary to show that "the intrusion would be highly offensive or objectionable to a reasonable person."[251]

Although intrusion upon seclusion can occur in an informational setting, plaintiffs invoking this theory in the realm of consumer privacy have met little success, both in connection with online information and in more traditional informational settings. Several courts applying state law have held that the transfer of consumer information does not constitute an "intrusion" for purposes of invasion of privacy claims.[252] In one case, American Express rented information about cardholders spending habits.[253] Before doing so, it would "rank . . . cardholders into six tiers based on spending habits . . . [f]or example, a cardholder may be characterized as 'Rodeo Drive Chic' or 'Value Oriented.' To characterize its cardholders, defendants analyze where they shop and how much they spend, and also consider behavioral characteristics and spending histories."[254] In this case, the Appellate Court of Illinois decided that these actions did not rise to the level of "intrusion" for invasion of privacy purposes.[255]

Similarly, plaintiffs in *In re Trans Union Corp. Privacy Litigation* failed to show intrusion on seclusion when a business transferred consumer information to a third party.[256] There, the defendant was a large credit reporting agency in the business of assembling and evaluating consumer credit information and then selling reports to companies considering extending credit to the consumer. The defendant was also in the business of selling or leasing 'target marketing' lists to catalog retailers, publication subscription vendors, and others using both mail and telemarketing.[257] The marketing lists were compiled using the same database as the credit reporting division. The plaintiff attempted to

---

[251] *Busse*, 813 N.E.2d at 1017.

[252] In re Trans Union Corp. Privacy Litigation, 326 F. Supp. 2d 893, 901 (N.D. Ill. 2004); Dwyer v. American Express Co., 652 N.E.2d 1351, 1356 (Ill. App. Ct. 1995).

[253] Dwyer, 652 N.E.2d at 1352–53.

[254] *Id*. at 1353.

[255] *Id.*

[256] *Trans Union*, 326 F. Supp. 2d 893 at 902.

[257] *Id*. at 895–96.

distinguish *Dwyer* on the grounds that the *Dwyer* plaintiffs voluntarily disclosed information directly to the defendant, whereas *Trans Union* plaintiffs did not.[258] The court rejected the importance of this distinction, stating that plaintiffs disclosed information to third-party creditors who then lawfully transferred the information to the defendants. Further, the court stated, plaintiffs "do not and cannot allege that they were unaware that their creditors would pass this information on to Trans Union in the normal course of business."[259] While it may well be that plaintiffs knew or should have known that creditors would transfer their payment histories to credit reporting agencies, it does not follow that this knowledge equates to consent to any and all subsequent transfers of that information.

Neither the *Busse*, *Dwyer*, nor the *Trans Union* court makes any mention of the aggregation aspect of the plaintiff/consumer's information. The *Trans Union* court, in fact, seems unaware of the transformative power of aggregating data: "Nor are the *individual* pieces of information—names, addresses, particulars of cell phone use—facially revealing, compromising or embarrassing."[260] Indeed, individual pieces of information taken alone may have *de minimis* impact on privacy. However, does the analysis change when information is data-aggregated to the point where the original information recipient receives an entire profile that identifies a customer and discloses information about their behavior?

3. State Data Privacy Statutes

Frustrated by the failure of the federal government to provide comprehensive standards for data privacy protection, states have taken matters into their own hands, as the following representative examples indicate.

a. Broad Privacy Protections

---

[258] *Trans Union*, 325 F. Supp. 2d at 901–02. In the technology terms described in Part I, the plaintiffs were essentially arguing that this was data based on transactional information, not data voluntarily submitted, for example, by a survey.

[259] *Id.*

[260] Busse v. Motorola, Inc., 813 N.E.2d 1013, 1018 (Ill. App. Ct. 2004) (emphasis added).

Not surprisingly, California has been at the forefront of state efforts to protect consumer privacy. Established in 2000, the California Office of Privacy Protection was created to protect the privacy rights of consumers.[261] When budget cuts closed this office in 2011, a newly created Privacy Enforcement and Protection Unit with the Attorney General's office continued the defunct agency's privacy protection efforts.[262] This unit enforces both federal and state privacy laws.

In 2004, California enacted the California Online Privacy Protection Act of 2003,[263] making California the first state to require a commercial website to post a privacy policy that: (1) identifies for site users the categories of personally identifiable information ("PII") the site collects; (2) indicates the categories of third parties with whom the information is shared; (3) describes the process, if any, users can follow to view and edit the PII collected; and (4) specifies the process by which users will be notified of any material changes to the policy.[264] This law was updated in 2014 with two additional disclosure requirements. The first requires a website operator that collects PII about an individual to notify users how the website operator responds to "do not track" requests.[265] Second, the website must also disclose whether third parties are permitted to collect PII during the user's site visit.[266]

In 2015, Delaware followed suit and enacted an online privacy and protection almost identical to that of California.[267] In July 2016, regulations became effective in Delaware that offer to website operators optional safe harbor language that could be used

---

[261] SCOTT COOPER ET AL., STATE PRIVACY LAWS IN PROSKAUER ON PRIVACY 5-3 (Practicing Law Institute ed., 1st ed. 2010).

[262] Jennifer Archie, Kevin Boyle & Ghaith Mahmood, *California AG's Office Establishes Privacy Enforcement Unit*, LATHAM & WATKINS GLOBAL PRIVACY & SECURITY COMPLIANCE LAW BLOG (July 20, 2012), http://www.globalprivacyblog.com/privacy/california-privacy-enforcement-unit/.

[263] CAL. BUS. & PROF. CODE § 22575 (West 2004).

[264] *Id.* § 22575(b)(1)–(3).

[265] *Id.* § 22575(b)(5).

[266] *Id.* § 22575(b)(6).

[267] DEL. CODE ANN. tit. 6, § 1205C (2016).

to ensure compliance with the Delaware online privacy laws.[268] In addition, those regulations indicate that if a website operator has a privacy policy that complies with the requirements of the California Online Privacy Protection Act, the safe harbor will be satisfied.[269] The Delaware privacy statute's definition of "personally identifiable information" includes most commonly items such as name, address, social security number, and email address that independently or in combination with other identifiers could be personally identifiable.[270] But in its safe harbor regulations, greater clarity is offered in the description of the notification requirements for the kinds of information that the website might collect from a user, which include:

> Information about your device or computer, including your IP address, geolocation, browser type, browser version, device type, operating system, referring [site/service/application].
>
> Information about your visits to and use of the site/service/application, including how you use the site/service/application, such as describe the type of information—examples might include the timing, length, frequency, and pattern of use, and the pages, screens, or other displays of information looked at by the user.[271]

If our patient Pamela is to find any relief within the law, it appears that her relief is most likely to be found in a state privacy statute, such as that of Delaware, that contains specific language that addresses how to handle information collected online about a user.

b. Deceptive Trade Practice

All states have enacted some form of consumer protection law prohibiting deceptive trade practices, but there is variation in terms of extent of protections, enforcement mechanisms, and penalties for violations.[272] In some states, violations of a stated company privacy policy are within deceptive trade practice prohibitions.

---

[268] 6-100-104 DEL. ADMIN. CODE (2016).
[269] *Id.* § 5.0 (2016).
[270] DEL. CODE ANN. tit. 6, § 1202(c)(15) (2016).
[271] 6-100-104 DEL. ADMIN. CODE § 4.2.2 (2016).
[272] CAROLYN L. CARTER, NATIONAL CONSUMER LAW CENTER, A 50-STATE REPORT ON UNFAIR AND DECEPTIVE ACTS AND PRACTICES STATUTES (2009), http://www.nclc.org/images/pdf/udap/report_50_states.pdf.

Nebraska, for example, does not impose specific obligations on website in terms of what privacy protections must be provided to consumers, but under state law a website owner may be guilty of a deceptive trade practice if that operator "knowingly makes a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public."[273] Pennsylvania law contains a similar provision.[274] As per statute, a person commits a deceptive or fraudulent business practice if in the course of business such person, "knowingly makes a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public."[275]

c. ISPs and Confidentiality

In Nevada, Internet service providers are required to keep confidential "[a]ll information concerning a subscriber other than the electronic mail address of the subscriber, unless the subscriber gives permission, in writing or by electronic mail, to the provider of the Internet service to disclose the information."[276] Similarly, in Minnesota, subject to certain exceptions, ISPs may not "knowingly disclose personally identifiable information concerning a consumer of the Internet service provider."[277] If the disclosure is incidental to the ordinary course of business of the ISP, disclosure may be permissible[278] as is a disclosure made with the consent of the user.[279] Minnesota law defines personally identifiable information to include information that identifies "[i]nternet or online sites

[273] NEB. REV. STAT. § 87-302(a)(15) (2017).
[274] 18 PA. CONS. STAT. § 4107(a)(10) (2016).
[275] *Id.*
[276] NEV. REV. STAT. ANN. § 205.498(1) (LexisNexis 2016).
[277] MINN. STAT. § 325M.02 (2016).
[278] MINN. STAT. § 325M.04, Subd. 1(1) (2016). Though seemingly broad, this is intended to include only "debt-collection activities, order fulfillment, request processing, or the transfer of ownership." *See* Jordan M. Blanke, *Minnesota Passes the Nation's First Internet Privacy Law,* 29 RUTGERS U. COMPUTER & TECH. L.J. 405, 411 (2003).
[279] MINN. STAT. § 325M.04, Subd. 1(3) (2016).

visited by a consumer, or any of the contents of a consumer's data-storage devices."[280]

Utah law does not restrict the transfer of an individual's personal information but instead requires a commercial entity that either intends to or wants the ability to disclose that nonpublic information to a third party for compensation, to notify the consumer either orally in writing that the entity "[m]ay choose to disclose nonpublic personal information about you, the consumer, to a third party for compensation."[281] Such notice should be sufficiently noticeable so that the consumer would see it before providing any nonpublic information to the entity.[282]

IV. THE TRACKING OF HEALTH-RELATED SEARCHES IS NOT WITHIN THE PROTECTIONS PROVIDED BY HIPAA

Having concluded that existing federal and state authority provides limited to no protection for our user's search of information related to high cholesterol, Part IV considers whether protection can be found instead in the privacy rules contained in HIPAA. While the health records maintained by hospitals, doctors' offices, and insurance companies are clearly within HIPAA's mandates,[283] what is less certain is the status of health-related queries potentially traceable back to and incorporated in the online profile of an identifiable individual. To reach a conclusion on this question, we begin with a look at HIPAA's genesis, the Act's stated requirements, and interpretations of those requirements.

A. The Origins of HIPAA Highlight the Importance of Health Information Privacy

Starting in or around 1929, Baylor University permitted local schoolteachers to pay insurance premiums to cover any medical expenses incurred at its university hospital in Dallas, Texas, thereby giving birth to the modern private health insurance

[280] MINN. STAT. § 325M.01, Subd. 5(3)–(4) (2016).
[281] UTAH CODE ANN. § 13-37-201(1) (LexisNexis 2016).
[282] UTAH CODE ANN. § 13-37-201(3) (LexisNexis 2016).
[283] FTC, *FTC Facts for Business: Complying with the FTC's Health Breach Notification Rule* (2010), https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule.

industry.[284] While other hospitals were quick to adopt similar insurance mechanisms, it was not until the late 1940s that commercial insurance companies entered the health insurance market. The commercial insurance companies' delayed entry into the health insurance market stems from two interrelated reasons: 1) whether medical care was an insurable risk since no clear model could accurately predict losses and 2) how to profitably price premiums when losses are not accurately predictable.[285]

In this early insurance market environment, health insurers were asymmetrically informed about insurance buyers' health status. Buyers' private health information provided different motivations to seek health insurance and impact the functioning of a competitive insurance market. For simplicity, suppose two pools of individuals exist in the health-insurance market: (1) high-risk individuals who have an unhealthy predisposition—either from genetics or lifestyle; and (2) low-risk individuals with no unhealthy predisposition. At one extreme, the market exhibits adverse selection: knowing more about their health status, low-risk individuals will likely choose not to seek health insurance (self-insure) leaving the health-insurance market comprised primarily of high-risk individuals.[286] Lacking individuals' private health information, health insurers set high premiums and historically excluded individuals from obtaining health-insurance coverage resulting in a market failure in the insurance market.[287]

Ideally, commercial health insurers seek to separate the pools of insurance buyers according to health risk in order to charge high-risk individuals high premiums and low-risk individual low premiums. However, at least two factors confound insurers' ability

---

[284] *See, e.g.*, PETER TEMIN, *An Economic History of American Hospitals, in* HEALTH CARE IN AMERICA: THE POLITICAL ECONOMY OF HOSPITALS AND HEALTH INSURANCE 75–102 (H.E. French III ed., 1988).

[285] *See, e.g.*, John K. Iglehart, *The American Health Care System: Private Insurance*, 326 N. ENG. J. MED. 1715 (1992); Harvey M. Sapolsky, *Empire and the Business of Health Insurance*, 16 J. HEALTH POL. & L. 747 (1991).

[286] George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECON. 488, 492–94 (1970).

[287] Michael Rothschild & Joseph Stiglitz, *Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information*, 90 Q.J. ECON. 629 (1976).

to separate insurance buyers: (1) health uncertainty and (2) consumers' private health information. Lacking private health information on the market composition insurees, health insurers likely misprice premiums resulting in sub-optimal profit and potential market failure. While some empirical evidence suggests that adverse selection in insurance markets in general is grossly exaggerated, this possibility cannot be safely ignored.[288]

To mitigate negative health adverse selection risk, insurers attempt to acquire information to screen individuals or groups and set premiums according to the expected medical benefits payout.[289] Screening through the practice of *community rating methods* attempt to set insurance premiums according to insurance plan member risk characteristics.[290] Premiums can vary by individuals under community-based rating methods due to geographic location, cost-of-living, contract type, and plan design. In contrast, *experience rating methods* screen individuals, or groups of individuals, according to personally identifiable risk categories thereby more closely matching insurance premiums to risk and expected medical benefit payouts to insurees.[291] Like community-based rating, premiums based on experience rating methods can be based on geographical location, contract type, and plan design. An individual's historical health data can also help insurers better understand the relationship between risk categories and expected health care costs to insure an individual or groups of individuals.[292]

Health screening and experience rating help insurers mitigate the adverse selection problem in the health insurance market. Therefore, health insurers have incentives to invest in acquiring as much private health information on insurees as possible to guide setting premiums and determining coverage eligibility. Insurers' incentives to mitigate the adverse selection problem leaves high-

---

[288] *See generally* Peter Siegelman, *Adverse Selection in Insurance Markets: An Exaggerated Threat*, 113 YALE L.J. 1223, 1274 (2004).

[289] REXFORD E. SANTERRE & STEPHEN P. NEUN, HEALTH ECONOMICS: THEORY, INSIGHTS AND INDUSTRY STUDIES 337–38 (South Western College., 6th ed. 2013).

[290] *Id*.

[291] *Id.*

[292] *Id.*

risk insurees in vulnerable situations, potentially with no option to acquire health insurance coverage. In 1996, President Bill Clinton signed the HIPAA legislation into law with the goals of ensuring the availability of health coverage and protecting patient privacy.[293]

B. The Privacy Rule of HIPAA

HIPAA was enacted in part to ensure that health insurance would be portable—meaning that individuals would be able to maintain their health insurance between jobs—and that patient health information[294] would be secure and private,[295] especially in the context of the computerization of patients' medical records.

The primary concern for the purposes of this article are the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule")[296] as enacted by the Department of Health and Human Services in accordance with HIPAA's privacy mandate. This Privacy Rule represents the first set of national regulations that protect certain health information.[297] The preamble to these standards illustrates the need for the Privacy Rule:

> According to the American Health Information Management Association (AHIMA), an average of 150 people, "from nursing staff to X-ray technicians, to billing clerks" have access to a patient's medical

---

[293] Willian J. Clinton, *Statement on Signing the Health Insurance Portability and Accountability Act of 1996* (Aug. 21, 1996), http://www.presidency.ucsb.edu/ws/?pid=53211.

[294] As defined in the statute, the term health information means:

> [A]ny information, whether oral or recorded in any form or medium that (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) Pub. L. No. 104-1914 § 1171(4) (1996).

[295] University of Chicago Medical Center Office of Compliance, *HIPAA Background*, (Oct. 23, 2006), http://hipaa.bsd.uchicago.edu/hipaa_background_20070122.pdf.

[296] 45 C.F.R. § 164.502(a) (2016).

[297] U.S. DEPT. OF HEALTH & HUM. SERV., *Summary of the HIPAA Privacy Rule*, https://www.hhs.gov/sites/default/files/privacysummary.pdf.

> records during the course of a typical hospitalization. While many of these individuals have a legitimate need to see all or a part of a patient's records, no laws govern who those people are, what information they are able to see, and what they are and are not allowed to do with that information once they have access to it.[298]

The Privacy Rule applies to health plans and health care providers and "any health care provider that transmits health information in electronic form."[299] It was designed to ensure that entities covered by this rule could only provide non-covered entities access to an individual's protected health information ("PHI")[300] if the individual authorized that disclosure.[301] However, the new rule also built in exceptions that would allow health care professionals to carry out their business functions; for example, PHI could be exchanged with non-covered business associates in connection with treatment, payment, and health care authorization.[302] HIPAA initially defined a business associate as one "who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information."[303] When a covered entity contracts with other businesses to perform some of their functions, the law mandates that the contractual relationship ensures that the business associate maintains the privacy of the

---

[298] Daniel J. Solove, *HIPAA Turns 10: Analyzing the Past, Present, and Future Impact*, AM. HEALTH INFO. MGMT. ASS'N, http://library.ahima.org/doc?oid=106325#.WKGvbH9Rp1g.

[299] Phyllis C. Borzi, *Behind the HIPAA Medical Privacy Regulations: Getting into the HIPAA Box*, 14 BENEFITS L.J. 29, 32 (2001).

[300] PHI includes eighteen items: name, address, significant dates (birth, hospital admission, etc.), telephone number, fax number, e-mail address, social security number, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers, device identifiers, web universal resource locators (URLs), Internet Protocol (IP) addresses, biometric identifiers, full face photographic images, and any other unique identifying number, characteristic, or code. 45 C.F.R. § 164.514(b)(2)(i) (2017).

[301] Borzi, *supra* note 299, at 34.

[302] *Id*. at 35.

[303] Austin Rutherford, *Byrne: Closing the Gap Between HIPAA and Patient Privacy*, 53 SAN DIEGO L. REV. 201, 204–05 (2016).

PHI.[304] In 2009, Congress passed the Health Information Technology for Economic and Clinical Health Act ("HITECH") to expand the scope and reach of HIPAA.[305] HITECH broadened the definition of a business associate to "include any subcontractor, *ad infinitum*, 'that creates, receives, maintains, or transmits protected health information on behalf of the business associate.' This amendment vastly increased the number of entities subject to HIPAA."[306]

Taken together, HIPAA and HITECH require that when unsecured health information is breached, the covered entity or the business associate must notify the individuals affected and the Secretary of Health and Human Services of the breach.[307] Aware that many web-based businesses that collect individual health information may not be covered by the terms of HIPAA, in 2010 the FTC passed the Health Breach Notification Rule to mandate that certain entities not covered by HIPAA notify customers (and sometimes the media) of any breach of their "unsecured, individually identifiable electronic health information."[308] The scope of the rule is broad, applying to businesses that are (1) vendors[309] of personal health records ("PHR"),[310] (2) a PHR-related

[304] Mark G. Simkin & Jeanne H. Yamamura, *What Businesses Should Know About HIPAA*, 73 CPA J. 46, 46–47 (Oct. 2003).

[305] Rutherford, *supra* note 303, at 204. This Act was passed as part of the American Recovery and Reinvestment Act of 2009. *See also HITECH Act Enforcement Interim Final Rule*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html?language=es (last visited Sept. 17, 2017).

[306] Rutherford, *supra* note 303, at 205 (quoting 45 C.F.R. § 164.502(a) (2014)).

[307] *Id*. at 213.

[308] *See FTC Facts for Business*, *supra* note 279; *see also* 16 C.F.R. § 318.5 (2016).

[309] The term vendor refers to a non-HIPAA covered entity that offers or maintains a personal health record. *See* 16 C.F.R. § 318.2(j) (2016).

[310] A personal health record is "an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." 16 C.F.R. § 318.2(d) (2016).

entity, or (3) a third-party service provider for the entities in categories 1 and 2.[311]

Seeking to offer clarity in terms of the types of entities that will be considered a PHR-related entity, the FTC offered the following example:

> For example, if you have an app that helps consumers manage their medications or lets them upload readings from a device like a blood pressure cuff or a pedometer into a personal health record, your business is a PHR-related entity. However, if consumers can simply input their own information on your site in a way that doesn't interact with personal health records offered by a vendor - for example if your site allows consumers to input their weight each week to track their fitness goals-you're not a PHR-related entity.[312]

A violation of the health breach notification rule is treated "as an unfair or deceptive act or practice," and violators may be penalized up to $40,000 per violation.[313]

C. Health-Related Searches as PHI?

A review of the statutory language of HIPAA in combination with the privacy protections implemented by Privacy Rule of the DHS leads to the conclusion that in and of itself Pamela's search of "women and high cholesterol," "cholesterol-lowering drugs," and "coronary artery disease" cannot bring a search engine within the "covered entity" and "business associate" classifications of HIPAA.[314] The question of whether health-related searches might fall within PHI becomes more nuanced when that search is potentially being combined with other information gleaned from

---

[311] 16 C.F.R. § 318.2 (2016).

[312] *FTC Facts for Business*, *supra* note 279.

[313] *Id.*

[314] Recall from the discussion above that HIPAA is intended to cover that information created or maintained by certain parties: health care providers, health plans, public health authorities, life insurers, schools or universities, or clearinghouses. *See supra* Part IV.B. In addition, those performing functions and activities on behalf of one of these providers are also within the scope of the law, but a search engine does not fit within these classifications. *Id.*

the user's online activities which when aggregated yield a profile that can be traced back to a specific individual.[315]

While still not within the letter of the law, there is a question whether the capture and aggregation of health-related searches or other health-related information gathered online violate the spirit of HIPAA. HIPAA was designed, in part, to ensure that patient health information remained confidential. HIPAA acknowledges the importance of patient control over whom this information is shared with. When Pamela searched for women and high cholesterol, she was searching for her diagnosed medical condition, and to the extent that her search became part of an online profile used by website owners for any one of the purposes discussed in Part II, this use and exchange of information without her consent, and possibly to her economic detriment, would violate the spirit of HIPAA's privacy protection. The issue becomes murkier if Pamela searches the internet inputting information that is not hers, but someone else's. For example, suppose she searched "treatment for tumors of the pituitary gland," not because she has that condition, but because her best friend was just diagnosed and she wants to research in order to better support her friend. If a pituitary gland tumor becomes part of the user's online profile, this would appear to be outside the spirit of HIPAA as this information is not personal health information regarding the computer user.

The conclusion that a search engine, such as Google, or a website owner, such as WebMD, is not currently impeded in its tracking, aggregation, and use of a user's online activity highlights the critical need for privacy law reform that will, at a minimum,

---

[315] It has been shown that 87% of Americans can be identified using only three types of information: zip code, birthdate, and gender, and the idea that some information (such as a web browser search) cannot be personal is not accurate since "almost all information can be personal when combined with other relevant bits of data." Nate Anderson, *"Anonymized" Data Really Isn't - and Why Not*, ARS TECHNICA (Sept. 8, 2009), https://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/; *see also* Scott Berinato, *There's No Such Thing as Anonymous Data*, HARV. BUS. REV. (Feb. 9, 2015), https://hbr.org/2015/02/theres-no-such-thing-as-anonymous-data (anonymization is becoming increasingly difficult due to the availability of large metadata datasets).

offer protection for an unsuspecting computer user's health-related actions.

V. LEGISLATION LIMITING THE SCOPE OF THIRD-PARTY TRACKING IS NEEDED

Any legislative or regulatory initiative must recognize, as a starting point, the legitimate interests of businesses to use certain customer information as part of confidential information and trade secret-protected assets. Fundamentally, as described in Part II, information, including customer information, is valuable and integral to the workings and decision-making of businesses. Business interests must be balanced against the individual customer's reasonable expectations of privacy in connection with health-related data online. We propose the following as a sensible scheme designed to protect both these interests.

As explained in Part III, attempts at comprehensive online privacy legislation have repeatedly stalled in Congress. Efforts at industry self-regulation have not fared much better. The now-repealed regulations that the FCC released in October 2016 likely resulted from Congressional inaction in this area coupled with an awareness that some action must be taken at the federal level as technological advances present a greater threat to online privacy.

Recognizing that comprehensive online privacy legislation is not likely to be passed in the short term, we propose instead targeted legislation to address the most egregious of the various uses of individual information described in this paper. Specifically, we advocate controlling the practice of indiscriminate collection, transfer, storage, and aggregation of individual health-related information obtained through internet searching, through visiting health-related content on websites that rely on third-party ad exchanges to generate revenue using third-party tracking, and through other tracking technologies that can identify an individual or household with high probability. Legislation should prohibit such uses unless informed users consent in advance.[316]

[316] Recall that in the pending lawsuit against Google, *see supra* Introduction, complainants cited a lack of transparency in that the terms did not allow users an opportunity to fully understand what they were agreeing to. Requiring informed

This proposal achieves the twin objectives of maintaining business stability and respecting the privacy of an individual's health data. There would be minimal disruption to business. Companies like Google, for example, would not need to change their business model.[317] They could continue to use first-party information based on voluntary provisions of information; transactional data; and first-party tracking that does relate aggregated health-related data to an individual or household with high probability. They also could continue to connect their website users to advertising for all non-health purposes. First-party health-related advertisement could be provided as long as (1) aggregated health data is not related to an individual or household or (2) information could not be transferred to third parties without adequate disclosure and user opt-in.

This type of targeted legislation would be a step in the right direction. It would allow the law to keep pace with technology, which is now able to use individual items of data in ways that computer users have likely never envisioned. As Congress embarks on this path, it follows the lead of the European Union Commission which seeks to ensure that "European legislation is keeping up with the fast space [sic] at which IT-based services are developing and evolving."[318] Indeed, Europe has been recognized as a world leader in efforts to protect individual data.[319] For example, on January 10, 2017 the European Commission released

---

consent would mean that at a minimum, users should be told that "participation is voluntary, refusal to participate will involve no penalty or loss of benefits to which the [user] is otherwise entitled, and the [user] may discontinue participation at any time without penalty or loss of benefits to which the [user] is otherwise entitled." *See* 45 C.F.R. § 46.116(a) (8) (2016).

[317] In fact, as per the terms of Google's stated privacy policy, Google requires opt-in consent for the sharing of sensitive personal information. Google defines sensitive information as including information on religion, race, sexual orientation, or health. *See* GOOGLE, *Privacy Policy*, https://www.google.com/policies/privacy/ (last visited Sept. 17, 2017).

[318] European Commission, *Proposal for an ePrivacy Regulation* (Jan. 10, 2017), https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

[319] STEVE S. MCCARTY-SNEAD & ANNE TITUS HILBY, RESEARCH GUIDE TO EUROPEAN DATA PROTECTION LAW 3 (2013) http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1001&context=leg_res.

a Proposal for a Regulation on Privacy and Electronic Communications, which, among other things, requires that web browsers obtain opt-in consent from end users in order to engage in third party tracking.[320] As per an already existing European Directive,[321] this consent should take the form of "a clear, affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment."[322]

CONCLUSION

The above-recommended privacy protections support the reasonable expectations of privacy held by many consumers and internet users with minimal negative impact on businesses. This alone is sufficient to justify such targeted legislation. In the larger context, the US government has articulated how the benefits of privacy protection extend beyond the individual:

> Strong privacy protections also are critical to sustaining the trust that nurtures Internet commerce and fuels innovation. Trust means the companies and technical systems on which we depend meet our expectations for privacy, security, and reliability. In addition, United States leadership in consumer data privacy can help establish more flexible, innovation-enhancing privacy models among our international partners.[323]

This targeted legislation will protect privacy while strengthening and further developing e-commerce in the twenty-first century.

---

[320] European Commission, *Proposal for an ePrivacy Regulation* (Jan. 10, 2017), https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

[321] Regulation 2016/679 of the European Parliament (Apr., 2016), http://eur-lex.europa.eu/eli/reg/2016/679/oj.

[322] European Commission, *Proposal for an ePrivacy Regulation* (Jan. 10, 2017), https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

[323] *Consumer Data Privacy in a Networked World*, *supra* note 50, at 100.