Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 31
Issue 3 *01/01/2015*

Article 4

January 2015

Limited Consumer Privacy Protections Against the Layers of Big Data

Andrew W. Bagley

Justin S. Brown

LIMITED CONSUMER PRIVACY PROTECTIONS AGAINST THE LAYERS OF BIG DATA

Andrew W. Bagley[†] & Justin S. Brown[††]

Consumers give away their data voluntarily and involuntary through their everyday online interactions. Many of these interactions are governed by "click-wrap" agreements in which consumers agree to data use terms with their Internet service provider (ISP), content provider, or an entire computing ecosystem through various layers of the Internet. This phenomenon effectively means that consumers lose control of their data to an endless web of third party big-data brokers unaccountable to the user. All the while, the increasingly dynamic and valuable nature of datasets makes it difficult to predict how data collected today will be used in the future. To help promote greater privacy protection to consumers, this article proposes that core elements of the Internet ecosystem adopt more robust transparency practices to clarify specific data collection, use, and sharing policies.

TABLE OF CONTENTS

---

† Andrew W. Bagley is privacy counsel at CrowdStrike and serves as the Director of Operations for the Secure Domain Foundation. He is an adjunct professor in the cybersecurity policy program at the University of Maryland University College. Mr. Bagley earned his Juris Doctor from the University of Miami. He holds a Master of Arts in Mass Communication Law, Bachelor of Science in Public Relations, and Bachelor of Arts in Political Science from the University of Florida. The views expressed herein reflect those of the author alone and do not represent the views of any employer or client.

†† Justin S. Brown is an Assistant Professor in the Zimmerman School of Advertising and Mass Communication where he teaches courses in telecommunications and media law. He holds a Doctor of Philosophy in Mass Communications and Masters of Arts in Telecommunications Studies from the Pennsylvania State University, and a Bachelor of Science in Journalism from the University of Oregon.

INTRODUCTION

Today, consumers interact with the Internet through an increasing number of devices that range in size, power, and capabilities. Many computing experiences are especially convenient to consumers because of the ease with which they can access their data quickly anytime, anywhere through wired and wireless broadband connectivity. As part of this trend, network computing is heavily distributed on the backend and data storage is decentralized. Through seamless and sometimes subtle online interactions, consumers transmit data that is replicated on multiple servers, passed along to third parties, and repackaged in the big data[1] marketplace.

Across the layers of the Internet, data is transmitted to and collected by everything, from the mobile operating system and apps on a consumer's phone or tablet[2] to the Internet Service Provider (ISP) that connects a device to the Web and the website destinations to which a user navigates. With each of these parties, consumers form independent relationships defined through "terms of service" or "terms-of-use agreements." Consumer online-behavioral data is highly valuable not

1. *See* Ira S. Rubinstein, *Big Data: Then End of Privacy or a New Beginning?*, 3 INT'L DATA PRIVACY L. 74 (2013) ("Big data refers to novel ways in which organizations, including government and businesses, combine diverse digital datasets and then use statistics and other data mining techniques to extract from them both hidden information and surprising benefits.").

2. Data collection on mobile devices can occur before a user has even used their device to access a webpage. For example, Apple's iPhone automatically collects, stores, and transmits location data. Brian X. Chen, *Why and How Apple Is Collecting Your iPhone Location Data*, WIRED (Apr. 21, 2011), www.wired.com/2011/04/apple-iphone-tracking/; Chris Foresman, *Android Phones Keep Location Cache, Too, But It's Harder To Access*, ARS TECHNICA (Apr. 22, 2011), http://www.arstechnica.com/gadgets/2011/04/android-phones-keep-location-cache-too-but-its-harder-to-access/

only for such primary-service providers[3] but also for secondary-data markets.[4] Free and paid online-service providers alike obtain consent from consumers through opt-in and opt-out regimes to share data with third parties that in turn further share and aggregate data.[5]

This article seeks to answer the following research questions: (1) in terms of data use, what are the legal rights conferred in existing terms of service agreements?; and (2) how are these terms of use agreements interrelated with one another within the layers of the Internet, ostensibly Internet access services (e.g., Verizon), operating systems and/or portals (e.g., Google), and content services (e.g., Facebook)? To explore these questions, this article utilizes legal research and analysis to carefully examine the terms of use agreements of Google, Verizon, and Facebook as well as related data use cases that address the role of consent in terms of service policies. This article suggests that with regard to data use rights and terms of service, consent with one entity in an Internet layer may confer data use rights across other layers. As a result, such broad terms in click-wrap agreements serve as a legal protection mechanism for consumer data to be shared and aggregated, often unknowingly, with third parties.

Part I of this article describes the common ways in which users today transmit data through the layers of the Internet. Part II details the current notice and consent regime and applicable laws governing data use with a specific outline of the data use provisions in different layers of the Internet, specifically those found in the terms of service of Verizon, Google, and Facebook. Part III analyzes the different ways in which current data use, collection, and sharing practices might affect users for years to come in the primary, secondary, and big-data marketplaces. Lastly, the article assesses existing policy proposals, and offers new ideas to improve upon transparency and consumer control in the ever-evolving layers of the Internet ecosystem.

---

3. Stacey Higginbotham, *ISPs Really, Really Want To Be Able To Share Your Data*, FORTUNE (Apr. 28, 2015), http://www.fortune.com/2015/04/28/isps-share-your-data/.

4. Data is collected, sold, traded, and repackaged by data brokers in marketplaces distinct from the consumer-facing content provider. Craig Timberg, *Brokers Use 'Billions' of Data Points to Profile Americans*, WASH. POST (May 27, 2014), http://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19_story.html.

5. Emily Steel, *Acxiom to Create 'Master Profiles' Tying Offline and Online Data*, FIN. TIMES (Sept. 23, 2013), http://www.ft.com/intl/cms/s/0/151d940e-2431-11e3-8905-00144feab7de.html#axzz3VXu4AJYM.

I. THE OMNIPRESENCE OF DATA TRANSMISSION IN EVERYDAY INTERNET INTERACTIONS

Today, Americans interact with the Internet in a variety of ways uncommon a decade ago. Many individuals now access the Internet exclusively through mobile devices[6] rather than traditional computers, and online experiences commonly occur outside of a web browser, through dedicated portals vis-à-vis apps.[7] A vibrant free-to-use ecosystem has flourished based on the ease with which online marketers and advertisers can collect information and target ads.[8] This effectively makes the Internet a layered experience in terms of the transfer of data and the contractual relationships to which a user is bound for everyday online interaction.

A common scenario involves the following: a user unlocks their Android Operating System (OS) powered mobile phone, connected over Wi-Fi to a home Verizon ISP connection, to open the Facebook app. In this situation, the user transmits data directly to three different parties, each within a separate layer of the Internet: Google by the nature of using Android OS; Verizon as the ISP; and Facebook as his destination Internet portal. From there, however, through no further action of their own, a user's data could be shared with third parties for a variety of commercial purposes.[9] While in the case of free services (Facebook and Google) one might argue that users contribute their data in exchange for the service, data is also collected and sold by paid services (the Verizon ISP connection). Yet the degree to which a user's data is collected and shared may change if they elect to use their Verizon Wireless service to connect to the Internet instead of their home FiOS or DSL connection.[10] Furthermore, separate terms of service

---

6. *Mobile Technology Fact Sheet*, PEW RESEARCH CENTER, http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/ (last visited May 15, 2015).

7. *Infographic: 2013 Mobile Growth Statistics*, DIGITAL BUZZ BLOG (Oct. 1, 2013), http://www.digitalbuzzblog.com/infographic-2013-mobile-growth-statistics/; Sarah Perez, *Mobile App Usage Increases in 2014, as Mobile Web Surfing Declines*, TECHCRUNCH (Apr. 1, 2014), http://techcrunch.com/2014/04/01/mobile-app-usage-increases-in-2014-as-mobile-web-surfing-declines.

8. Alexis C. Madrigal, *I'm Being Followed: How Google—and 104 Other Companies—Are Tracking Me on the Web*, ATLANTIC (Feb. 29, 2012), http://www.theatlantic.com/technology/archive/2012/02/im-being-followed-how-google-151-and-104-other-companies-151-are-tracking-me-on-the-web/253758/.

9. This ultimately depends on the data collection and sharing policies that are contained within each provider's terms-of-service agreement.

10. Verizon Wireless has different terms of service and is regulated under different laws than Verizon's wired connections. Because of its use of "radio," wireless services and (mobile)

agreements govern the relationship between a user and Google for use of Android OS services—Verizon for wired and wireless Internet service, and Facebook for social media network access.[11] To complicate matters, similar providers within the same layer of the Internet might offer terms of service and data use policies that vary significantly.[12] This is especially true within the content layer that Facebook represents, as users potentially have an enormous array of social media and smartphone applications from which to choose.[13]

Outside the content layer, even the OS platform, from which users launch apps and visit websites, can access and automatically collect specific device, location, and usage information.[14] This means that a user enjoying the features of the Google Play Store on their Android phone might submit robust information to Google without directly accessing a Google website.[15] This effectively allows Google to collect

broadband Internet access is regulated in part under Title III of the Communications Act. *See* 47 U.S.C. §§ 301, 304, 307, 309 (2013). Traditional wired telephone service falls under Title II regulations. *See id.* § 201. Wired (fixed) and mobile broadband is subject to Section 706 regulation that addresses advanced telecommunications capability. *See id.* § 1302.

11. *See Terms of Service*, GOOGLE, http://www.google.com/intl/en/policies/terms/ (last visited Apr. 17, 2015); *Terms of Service*, VERIZON, http://www.verizon.com/about/terms/ (last visited Apr. 17, 2015); *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms (last visited Apr. 17, 2015).

12. For example, Facebook and Twitter, both social media platforms in the content layer, differ in the way in which they track and store user data. Twitter supports the do-not-track standard, unlike Facebook. *See Twitter Supports Do Not Track*, TWITTER, https://support.twitter.com/groups/33-report-abuse-or-policy-violations/topics/148-policy-information/articles/20169453-twitter-supports-do-not-track# (last visited Apr. 17, 2015); Jim Edwards, *In a Further Humiliation to Microsoft, Facebook Will Not Honor 'Do Not Track' Signals on Internet Explorer*, BUS. INSIDER (June 12, 2014), http://www.businessinsider.com/facebook-will-not-honor-do-not-track-2014-6. For more comparisons of terms-of-service agreements amongst similar services, see *Terms of Service; Didn't Read*, https://tosdr.org/# (last visited Apr. 17, 2015).

13. In addition to Facebook and Twitter, other social media networks include LinkedIn, Pinterest, Tumblr, and Flicker. *See* Shea Bennett, *The 13 Most Popular Social Networks (by Age Group)*, ADWEEK (Oct. 21, 2014, 3:00 PM), http://www.adweek.com/socialtimes/popular-social-networks-age/502497. Furthermore, there are more than 800,000 third-party-app programs available for download from the Apple and Google stores. *See* Harry McCracken, *Who's Winning, iOS or Android, All the Numbers in One Place*, TIME (Apr. 16, 2013), http://techland.time.com/2013/04/16/ios-vs-android/.

14. Both mobile- and desktop-operating systems now collect robust user data. *See* Julia Angwin & Jennifer Valentino-Devries, *Apple, Google Collect User Data*, WALL ST. J. (Apr. 22, 2011), http://www.wsj.com/articles/SB10001424052748703983704576277101723453610; Thomas Halleck, *Apple Automatically Collects Safari Searches, User Location in OS X Yosemite*, INT'L BUS. TIMES (Oct. 20, 2014), http://www.ibtimes.com/apple-automatically-collects-safari-searches-user-location-os-x-yosemite-1708185.

15. *See Google Play Terms of Service*, GOOGLE PLAY (Dec. 10, 2014), http://play.google.com/about/play-terms.html. Because it is a "service" as defined by Google, Google Play Terms of Service also reference Google's terms of service that specify data collection

end-to-end information about a user's online and offline interactions from their Android mobile device in addition to more limited information from non-Android devices used to access Google's websites.[16]

Data is funneled through each layer of the broadband ecosystem as users access the Internet. ISPs typically process the greatest amount of an individual user's data because of their unique role in connecting users to the Internet, but naturally experience blind spots when users connect their device to another ISP to continue their online Facebook or Gmail experience.[17] This is less of an issue for Verizon, which can offer wired- and wireless-Internet access to the same user, thereby processing an overwhelmingly significant portion of a user's virtual transactions.[18] ISPs are also uniquely situated because of the amount of information they possess about a user's existence in the physical world, by virtue of their billing information, as well as any bundled services that are part of a monthly Internet access package.[19]

Users access Facebook with unique user accounts through which they overtly, incidentally, and unintentionally append personal information and behavioral data, including their physical real-world locations.[20] Like many Google services, Facebook may also track users

---

and sharing. *See Terms of Service*, GOOGLE PLAY, http://www.google.com/intl/en/policies/terms/ (last visited Apr. 5, 2015).

16. Moreover, Google has access to even more information in communities in which it serves as an ISP through its Google Fiber Service. *See* GOOGLE FIBER, https://fiber.google.com /about2/ (last visited Mar. 20, 2015). For more information about how Google collects information from its users when they use their services, see SIVA VAIDJYANATHAN, THE GOOGLIZATION OF EVERYTHING: (AND WHY WE SHOULD WORRY) 83–85 (2012).

17. Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1439 (2009) (explaining the breadth and limits of ISP data collection); *see also ISPs Look to Make Money with Mined Data*, NAT'L PUB. RADIO (Dec. 27, 2010), http://www.npr.org/2010/12/27/132 358556/Internet-Providers-Look-To-Make-Money-With-Mined-Data; Peter Whoriskey, *Every Click You Make*, WASH. POST (Apr. 4, 2008), http://www.washingtonpost.com/wp-dyn/content /article/2008/04/03/AR2008040304052.html.

18. An individual could hypothetically subscribe to Verizon's wired home-Internet service and also subscribe to Verizon Wireless for their mobile telephone and Internet services. Verizon in fact offers bundle savings for individuals that subscribe to Verizon FIOS and smartphone services. *See* Marguerite Reardon, *Verizon Offers Discount to Wireless and FIOS Triple-Play Customers*, CNET (Mar. 7, 2014), http://www.cnet.com/news/verizon-offers-discount-to-wireless-and-fios-triple-play-customers/

19. This occurs because customers supply their identity, address, and payment information to pay for such services. *See* Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, SANTA CLARA COMPUTER & HIGH TECH L.J. 14 (2010), *available at* http://www.digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1512&context=chtlj.

20. Heather Kelly, *Facebook Launches Friend-Tracking Feature*, CNN (Apr. 18, 2014), http://www.cnn.com/2014/04/17/tech/mobile/facebook-nearby-friends/.

after they leave the site.[21] Additionally, Facebook's interactive "Like" buttons are embedded on sites across the World Wide Web.[22] This provides the company with data far beyond that relayed through what otherwise appears to be a user's self-contained Facebook session.

The dynamic ways in which information is transmitted, collected, and stored through common online interactions exceeds the norms of traditional peer-to-peer relationships.[23] Data is used to create marketing profiles, sell advertisements, conduct product analysis, and so much more in the big data marketplace.[24] These realities illustrate the difficultly for even a user familiar with the provisions of each terms of service agreement to conceptualize where their data might wind up.

Consequently, Internet users contribute to robust datasets by engaging in seemingly mundane behavior, such as clicking on links or engaging in online text, email, voice, or video conversations. Furthermore, data on a discrete website does not necessarily rest on a single server or even at a specific server site.[25] Instead, Content Delivery Networks (CDNs) increasingly store and replicate data in a decentralized manner.[26] This means that user interaction with the Web is distributed not merely amongst devices but also throughout networks for even simple transactions such as identity verification.

The question of who owns and may trade a user's data generally depends on rights conferred by the terms of use for the service over which the user transmits their data. Once a user consents to the use of their data by their primary-content provider, under the current legal

---

21. Violet Blue, *Facebook Turns User Tracking 'Bug' Into Data Mining 'Feature' For Advertisers*, ZDNET (June 17, 2014), http://www.zdnet.com/facebook-turns-user-tracking-bug-into-data-mining-feature-for-advertisers-7000030603/.

22. Amir Efrati, *'Like' Button Follows Web Users*, WALL ST. J. (May 18, 2011), http://online.wsj.com/news/articles/SB10001424052748704281504576329441432995616.

23. In the physical world, a consumer might reasonably expect a bank, which is heavily regulated, to collect and keep information about them because of the nature of their business. However, the same consumer might not expect a local grocery store to keep track of every item they looked at during a 20-minute visit to the store.

24. Reed Albergotti, *Facebook to Target Ads Based on Web Browsing*, WALL ST. J. (June 12, 2014), http://online.wsj.com/articles/facebook-to-give-advertisers-data-about-users-web-browsing-1402561120.

25. Madrigal, *supra* note 8.

26. Matthias Wählisch et al., *Backscatter from the Data Plane—Threats to Stability and Security in Information-Centric Network Infrastructure*, 57 COMP. NETWORKS 3192 (2013), *available at* http://www.inf.fu-berlin.de/users/waehl/papers/wsv-bdpts-13.pdf.

interpretation,[27] they also effectively give away their data to the derivative-data market. The data collected by these providers and shared with advertising data brokers contributes to the big data ether from which other datasets are spliced and resold for a variety of purposes.[28] This versatility and profitability has led data to be hailed as the oil of the 21st century.[29]

Beyond the value derived from compiling data about individuals from multiple sources, big data analytics applied to larger datasets can draw valuable insights for big business, marketers, political operations, and even local governments.[30] This enables responsiveness and market efficiencies previously unattainable, but also may embolden the manipulation of consumers' virtual and real world behavior. Gathering and use of big data has become ubiquitous in daily Internet experiences[31] despite a mounting number of social, cultural, and ethical concerns.[32]

II. LAYERS OF THE INTERNET AND DATA COLLECTION

User data is collected from active virtual behavior and automated transmissions from devices. Information is collected through log files, cookies, clickstream data, virtual fingerprinting,[33] and user-provided

27. As explained later in this article, the notice-and-consent regime effectively means that a user loses control of their data once they agree to allow their service provider to collect and use it via a terms-of-use agreement.

28. Craig Timberg, *Brokers Use 'Billions' of Data Points to Profile Americans*, WASH. POST (May 27, 2014), http://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19_story.html.

29. Perry Rotella, *Is Data the New Oil?*, FORBES (Apr. 2, 2012), http://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/.

30. Alan Feuer, *The Mayor's Geek Squad*, N.Y. TIMES (Mar. 23, 2013), http://www.nytimes.com/2013/03/24/nyregion/mayor-bloombergs-geek-squad.html.

31. Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. 63 (2012), http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-63_1.pdf.

32. *See, e.g.*, Danah Boyd & Kate Crawford, *Critical Questions for Big Data*, 15 INFO., COMM. & SOC'Y 662 (2012); Julie. E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1919 (2013); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 96 (2014); Neil M. Richards & Jordan H. King, *Three Paradoxes of Big Data*, 66 STAN. L. Rev. 41, 41 (2013).

33. Adam Tannger, *The Web Cookie is Dying. Here's the Creepier Technology That Comes Next*, FORBES (June 17, 2013), http://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/. For more on specific technologies involved in gathering data including deep-packet inspection, web beacons and

content.[34] A complex web of advertisers, data aggregators, and online service providers collect and exchange information about users' online interactions.[35]

In the 1990s, Internet users typically relied upon Netscape Navigator, Microsoft's Internet Explorer, or other desktop-based browsers that were originally sold for a fee to access a much more static World Wide Web 1.0 environment that privileged user consumption.[36] Operating systems, such as Microsoft Windows, which also typically sold for a fee, permitted users to run countless, unrelated, non-integrated applications. During this period, comprehensive information about desktop computer users' online and offline behavior was not generated and transmitted to Microsoft or other operating system owners for use in secondary data markets.[37] Today, however, in the Web 2.0 era, the operating system, browsers, and other applications are part in parcel to the online user experience and the big data economy, readily collecting, sharing, and aggregating data[38] as users participate and share information within social media and smartphone applications.

The increasing number of software applications collecting data in Web 2.0 and social media is now augmented by physical devices as part of the budding "Internet of Things."[39] The layers of the broadband ecosystem are expanding as users interact with the Internet in more ways than accessing static websites and communicating over instant

scraping, see LORI ANDREWS, I KNOW WHO YOU ARE AND SAW WHAT YOU DID: SOCIAL NETWORKS AND THE DEATH OF PRIVACY 22–31 (2011).

34. Madigral, supra note 8.

35. *Id.*

36. For good comparisons of Web 1.0 versus Web 2.0, see Graham Cormode & Blachander Krishnamurthy, *Key Differences Between Web 1.0 and Web 2.0*, 13 FIRST MONDAY (2008), http://journals.uic.edu/ojs/index.php/fm/article/view/2125/1972; Tim O'Reilly, *What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, 65 COMM. & STRATEGIES 1, 17 (2007), *available at* http://mpra.ub.uni-muenchen.de/4578/1/MPRA_paper_4578.pdf.

37. There were, however, privacy concerns about much more limited hardware-ID collections. For a prophetic piece on the privacy concerns of the time, see A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1469 (2000), *available at* http://osaka.law.miami.edu/~froomkin/articles/privacy-deathof.pdf

38. *See* Christian Bizer, Tom Heath & Tim Berners-Lee, *Linked Data—The Story So Far*, 5 INT'L J. ON SEMANTIC WEB AND INFO. SYS. 1 (2009); Cormode & Krishnamurthy, *supra* note 36.

39. For an illustration of the budding Internet of Things, see Bill Wasik, *In the Programmable World, All Our Objects Will Act as One*, WIRED (May 14, 2013), http://www.wired.com/2013/05/internet-of-things-2/all/.

messaging. For example, retailers now use Wi-Fi beacons to track shoppers in the physical world,[40] and consumers use their mobile devices to pay for real world goods.[41] Information from such interactions can be combined with other data from Web usage to create all-encompassing marketing profiles of specific consumers to facilitate behavioral advertising,[42] also known as behavioral targeting.[43]

The online data market has long been dominated by Web destinations reliant upon advertising profits rather than telecommunications infrastructure providers. However, ISPs such as Verizon today compete in the data economy with Google, Facebook, and other web giants to sell information about their users to third parties.[44] This means that data collection in terms of use for paid services (ISPs) does not necessarily afford consumers more privacy rights than those of free services (Google).[45] Nonetheless, different laws regulate the various layers of the Internet. In particular, ISPs, which primarily deal with data in transit, are subject to more restrictions under the Electronic Communications Privacy Act and related Wiretap Act.[46]

Many users' online experience now takes place through what could be characterized as an Internet of Hubs by which users enjoy

---

40. Natalie Gagliordi, *Apple iBeacon Challengers Multiply: A Look at Five Rivals*, ZDNET (June 24, 2014), http://www.zdnet.com/article/apple-ibeacon-challengers-multiply-a-look-at-five-rivals/.

41. BD. OF GOVERNORS OF THE FED. RESERVE SYS., CONSUMERS AND MOBILE FINANCIAL SERVICES 2015, at 5–6, 14–18 (2015), http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf.

42. *See, e.g.*, ANDREWS, *supra* note 33, at 17–19.

43. Lauren Drell, *Four Ways Behavioral Targeting is Changing the Web*, MASHABLE (Apr. 26, 2011), http://mashable.com/2011/04/26/behavioral-targeting/.

44. Declan McCullah, *Verizon Draws Fire For Monitoring App Usage, Browsing Habits*, CNET (Oct. 16, 2012, 5:00 AM PDT), www.cnet.com/news/verizon-draws-fire-for-monitoring-app-usage-browsing-habits/; Robert McMillan, *Verizon's 'Perma-Cookie' is a Privacy-Killing Machine*, WIRED (Oct. 27, 2014, 6:30 AM), www.wired.com/2014/10/verizons-perma-cookie/; Kashmir Hill, *How to Opt Out of AT&T's Plan to Sell Everything It Knows About You and Your Smartphone Use*, FORBES (July 3, 2013, 3:20 PM), http://www.forbes.com/sites/kashmirhill/2013/07/03/how-to-opt-out-of-atts-plan-to-sell-everything-it-knows-about-you-and-your-smartphone-use/.

45. AT&T recently offered its ISP customers in Austin, Texas a higher-priced plan that will help protect some of their data from being collected by AT&T and shared to other parties. *See, e.g.*, Quineten Plummer, *At What Price? For Extra $29/Month, AT&T Will Not Slurp Privacy Data From GigaPower Users*, TECH TIMES, (Feb. 19, 2015), http://www.techtimes.com/articles/33949/20150219/at-what-price-for-extra-29-month-at-t-will-not-slurp-privacy-data-from-gigapower-users.htm/.

46. Ohm, *The Rise and Fall of Invasive ISP Surveillance*, *supra* note 17, at 1478.

Internet access via contained operating systems, apps, and cloud-based services. Google, for example, offers some users a completely integrated online experience through which a consumer may use their Chromebook laptop computer[47] to connect to the Internet via Google Fiber, open the Chrome web browser and visit their Google+ social networking profile to make a post, and comment about a YouTube video.[48] Moreover, Google's share of the online search market means that many consumers who rely on different ISPs or opt to use other web browsers still interact with Google at some point in their Internet experience.[49] The company's Android operating system dominates the mobile device arena.[50] Hence, the success of a free, fully integrated operating system and advertising conduit offers a drastic departure from the traditional role of an operating system as a standalone platform.

It should be noted that users may still transmit enough data to paint a comprehensive picture of their lives regardless of whether they are part of a singular company's digital ecosystem or opt to use hardware, software, and connectivity platforms from wholly different entities. For example, a user engaged in private browsing, off the record mode in Google Chat, or another form of privacy still might contribute the content of their Web interactions to Verizon ISP's data trove.[51] Similarly, many users enjoy the convenience of using their Facebook credentials to log into other websites or use the Facebook "like" buttons found elsewhere online to express and align themselves with product

47. Edward C. Baig, *Google's New Chromebook Pixel is Power Users' Pleasure*, USA TODAY (Mar. 12, 2015, 7:10 AM EDT), http://www.usatoday.com/story/tech/columnist/baig/2015/03/11/google-chromebook-pixel-poweruser-pleasure/24744023/.

48. For an explanation of how Google is vertically integrating its offerings, see Brian Fung, *Google is Serious About Taking on Telecom. Here's Why It'll Win*, WASH. POST (Feb. 6, 2015), http://www.washingtonpost.com/blogs/the-switch/wp/2015/02/06/google-is-serious-about-taking-on-telecom-heres-why-itll-win/.

49. As of February 2014, Google commanded 67.5% of PC-based search-engine queries in the United States, and 87.1% of those from mobile devices. Greg Sterling, *Google Search Share Stable, Bing Growth Continues at Yahoo's Expense*, SEARCH ENGINE LAND (Mar. 20, 2014, 10:16 AM), http://searchengineland.com/google-search-share-stable-bing-continues-cannibalize-yahoo-187124.

50. Android is on over 80% of smartphones worldwide and just under 50% of smartphones in the United States. *See* Fred O'Connor, *Android Gains Share, iOS Falls in 2014 Smartphone OS Market*, PC WORLD (Feb. 24, 2015), http://www.pcworld.com/article/2888532/idc-android-ios-again-dominate-smartphone-os-market.html; *Apple iOS Leads US OS Share for the First Time Since Q4 2012*, KANTAR WORLD PANEL (Apr. 2, 2015), http://www.kantarworldpanel.com/global/News/Apple-iOS-leads-US-OS-share-for-the-first-time-since-Q4-2012.

51. ISPs potentially have the ability to see everything flowing through their networks. Ohm, *The Rise and Fall of Invasive ISP Surveillance*, *supra* note 17, at 1440–41.

and service brands, star personas, media content, leisure activities, organizations, and institutions.[52]

The reality of this "Internet of Hubs" is especially apparent in the mobile device landscape in which a few major providers dominate mobile broadband access, limited mobile OS options exist, and users interact with the Web through dedicated apps.[53] Approximately 63% of Americans access the Internet using their mobile devices, with 34% using their mobile device to access the Internet most of the time.[54] Device information and usage data is collected and transmitted by mobile apps, sometimes without a user's consent.[55] Moreover, data on many mobile devices also is transmitted through malware by the form of "data leakage" unbeknownst to users.[56]

A user plugged into one brand's ecosystem for their online experience might consent to the lowest common denominator for privacy protections and therefore find themselves subject to an array of unanticipated information disclosure, sharing, and aggregating among third parties.[57] This is perhaps even more prevalent with smartphones, which can transmit location information all the time while also providing specific physical world purchasing and browsing information via data collection beacons.[58] In fact, user communication practices are now all-encompassing throughout the layers of the Internet, from confidential messaging to consumption of video, social

52. Amir Efrati, *'Like' Button Follows Web Users*, WALL ST. J. (May 18, 2011), http://online.wsj.com/news/articles/SB10001424052748704281504576329441432995616; Michael Olson, *Social Login Trends Across the Web for Q1 2013*, JANRAIN (Apr. 8, 2013), http://www.janrain.com/blog/social-login-trends-across-the-web-for-q1-2013/.

53. OPEN INTERNET ADVISORY COMMITTEE, FED. COMMC'N COMM'N, OPENNESS IN THE MOBILE BROADBAND ECOSYSTEM, 2013 ANNUAL REPORT 47–65 (2013), http://transition.fcc.gov/cgb/oiac/oiac-2013-annual-report.pdf.

54. *Mobile Technology Fact Sheet*, *supra* note 6.

55. James Vincent, *Free Android Flashlight App Stole Location Data to Send to Advertisers*, INDEPENDENT (Dec. 6, 2013), http://www.independent.co.uk/life-style/gadgets-and-tech/free-android-flashlight-app-stole-location-data-to-send-to-advertisers-8988668.html.

56. Radoniaina Andriatsimandefitra et. al, *User Data on Androïd Smartphone Must Be Protected*, 90 ERCIM NEWS 18 (2012), *available at* http://ercim-news.ercim.eu/en90/special/user-data-on-android-smartphone-must-be-protected.

57. Higinio Maycotte, *How Top Data Brokers Collect and Use Your Data Read*, WIRED (Oct. 14, 2014, 2:00 PM), http://insights.wired.com/profiles/blogs/how-top-data-brokers-collect-and-use-your-data#axzz3W72HhuMF; Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES (June 16, 2012), http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?ref=natashasinger&_r=0.

58. Stephen Lawson, *Ten Ways Your Smartphone Knows Where You Are*, PC WORLD (Apr. 6, 2012), http://www.pcworld.com/article/253354/ten_ways_your_smartphone_knows_where_you_are.html.

media, and information retrieval. Arguably most of these users are not readily aware of all of these data collection techniques and privacy issues existent within the cumulative effects of terms of service agreements that serve as permission paths and enablers for the creation of their own big data footprint.[59]

III. THE TERMS, CLICKS, AND LAWS PERMITTING NEVER-ENDING DATA USE

U.S. private-industry privacy law is regulated through sector-specific federal laws and state laws.[60] Absent a specific law in place, the relationship between a user and service provider is largely defined by company terms of service or privacy policies rooted in contract law and, more often than not, the FTC's enforcement against deceptive practices.[61] Consequently, a consent-based regime links users to primary parties but does little to fully illustrate the derivative use of their data and what that consent truly entails.

Today, users click or tap "I agree" to terms of service, terms of use, end user-license agreements, and other contracts to utilize free- or paid-online services.[62] However, unlike many typical contracts, the terms are not negotiated between a service provider and a user.[63] Instead, the terms are presented as a "take it or leave it" set of conditions.[64] The terms outline everything from forum selection in the event of litigation to specific privacy and information sharing provisions.[65] Such contractual agreements are branded with the moniker "click-wrap agreements" in reference to several court decisions from the 1990s and early 2000s.[66] These cases upheld contractual agreements packed in shrink-wrapped software that could

59. Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 260–63 (2013), http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1.

60. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM L. REV. 583, 587 (2014), http://columbialawreview.org/wp-content/uploads/2014/04/Solove-Hartzog.pdf.

61. *Id.*

62. Mark A. Lemley, *Terms of Use*, 91 MINN. L REV. 459, 465–66 (2006).

63. *Id.*

64. *Id.*

65. *Id.*

66. Ryan J. Casamiquela, *Contractual Assent and Enforceability: Cyberspace*, 17 BERKELEY TECH. L.J. 475, 475–76 (2002), *available at* http://scholarship.law.berkeley.edu/btlj/vol17/iss1/28.

not be read until the purchase was complete.[67] Today, in a digital online world, contracts which require a user's active click for acceptance are commonly referred to as "click-through" agreements, whereas those which passively list the terms on their website are called "browse-wrap" agreements.[68]

At their core, click-through agreements are contracts between a service provider and a user.[69] Traditional contract law requires an offer for a service or good, acceptance of that offer, and some form of consideration or reliance on the offer in exchange for its procurement.[70] Acceptance traditionally presumes that parties reasonably understand the terms and conditions to which they are bound.[71] However, many online-service users today do not even read, much less understand, the terms to which they are assenting and simply click through to access the particular service, app, or website they wish to utilize. Nonetheless, such click-through agreements are generally enforceable contracts.[72]

Digital consumers rarely review terms of service agreements with detailed scrutiny and those who do may not have the legal knowledge to understand them fully and thus self-manage their privacy.[73] If they read the agreements carefully, perhaps there would be a chilling effect on their behavior because of the agreements' broad and ambiguous terms.[74] Furthermore, sometimes service providers change terms

67. *See generally id.*

68. Ian Rambarran & Robert Hunt, *Are Browse-Wrap Agreements All They Are Wrapped Up To Be?*, 9 TUL. J. TECH. & INTELL. PROP. 173 (2007).

69. Nathan J. Davis, *Presumed Assent: The Judicial Acceptance of Clickwrap*, 22 BERKELEY TECH. L.J. 577, 580–82 (2007), *available at* http://scholarship.law.berkeley.edu/btlj/vol22/iss1/29.

70. RESTATEMENT (SECOND) OF CONTRACTS §§ 1, 24, 50, 71 (1981).

71. *Id.* §§ 20, 201.

72. Ty Tasker & Daryn Pakcyk, *Cyber-Surfing on the High Seas of Legalese: Law and Technology of Internet Agreements*, 18 ALB. L.J. SCI. & TECH. 80, 110–11 (2008), http://www.albanylawjournal.org/Documents/Articles/18.1.79-Tasker.pdf; Nathan J. Davis, *Presumed Assent: The Judicial Acceptance of Clickwrap*, 22 BERKELEY TECH. L.J. 577, 579 (2007), *available at* http://scholarship.law.berkeley.edu/btlj/vol22/iss1/29; *see also* ProCD v. Zeidenberg, 86 F.3d 1447 (7th. Cir. 1996).

73. *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1883 (2013). Solove summarizes the cognitive problems as follows: "(1) people do not read privacy policies; (2) if people read them, they do not understand them; (3) if people read and understand them, they often lack enough background to make an informed choice; and (4) if people read them, understand them, and can make an informed choice, their choice might be skewed by various decision-making difficulties." *Id.* at 1888.

74. *Id.*

without acquiring new informed consent from the users.[75] To make matters worse, terms of service agreements are generally not visually inviting to their intended audience.[76] The features of a website might even provide a user with apparent rights and privileges to affect data.[77] Commentators have suggested that such features should be considered in the interpretation and enforcement of online contracts,[78] but instead the plain language of the terms of service is given legal weight.[79] Despite all of these misgivings, a consenting user seems to be making a long-term commitment to the control of their data by other parties for uses that are unimaginable at the time of consent.[80] In effect, consent garnered quickly at one layer through a click-through agreement is being employed as a marketing and data collection tool for third parties to use throughout the layers of the Internet.

A. Actual Versus Implied Consent

When it comes to providing the first and last mile of Internet access, consumers often do not have many choices for their hardwire ISP.[81] Wireless providers are not very abundant either.[82] This draws into question whether or not there is true consent because each broadband Internet-access provider has already crafted rules-of-the-road for its terms and conditions of service. If a fixed-broadband consumer may

75. Declan McCullagh, *Yahoo: Your House is My House*, WIRED (June 29, 1999), http://archive.wired.com/science/discoveries/news/1999/06/20472.

76. *Id.*

77. *Id.*

78. *See* Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635 (2011).

79. *Id.*

80. Higinio Maycotte, *How Top Data Brokers Collect and Use Your Data Read*, WIRED (Oct. 14, 2014, 2:00 PM), http://insights.wired.com/profiles/blogs/how-top-data-brokers-collect-and-use-your-data#axzz3W72HhuMF ("For users, the collection of data without consent is generally understood to be a breach of privacy. Companies considered to be data brokers circumvent this issue via terms and conditions, the likes of which most people do not thoroughly read.").

81. David Carr, *Telecom's Big Players Hold Back the Future*, N.Y. TIMES (May 19, 2013), http://www.nytimes.com/2013/05/20/business/media/telecoms-big-players-hold-back-the-future.html?pagewanted=all&_r=1; Jon Brodkin, *Most of the US Has No Broadband Competition at 25Mbps, FCC Chair Says*, ARS TECHNICA (Sept. 4, 2014), http://www.arstechnica.com/business/2014/09/most-of-the-us-has-no-broadband-competition-at-25mbps-fcc-chair-says/; Steve Lohr, *The Push for Net Neutrality Arose From Lack of Choice*, N.Y. TIMES (Feb. 25, 2015), http://www.nytimes.com/2015/02/26/technology/limited-high-speed-internet-choices-underlie-net-neutrality-rules.html.

82. Nilay Patel, *The Internet is Fucked (But We Can Fix It)*, VERGE (Feb. 25, 2014, 12:30 PM), http://www.theverge.com/2014/2/25/5431382/the-internet-is-fucked.

only choose between DSL and cable for high-speed Internet service,[83] then they remain left with the lesser of two evils. Without pressure from competition or regulation, there is little but hope that either broadband provider will be entrusted not only with necessary quality of service features and open network neutrality principles, but also terms of service provisions that may enable security and other protective measures to curb the gathering, sharing and aggregation of personal data.[84]

A user may expect the primary party (e.g. Google) with which they engage to collect information and tailor advertisements.[85] However, this does not mean that they expect their data will be sold at-will to other parties, combined with other sources of their data, and form a wholly sophisticated compilation of their online life.[86] Likewise, social media companies and Web portals gradually change their privacy policies, adjusting the privacy rights of their users.[87] This means that a company might employ self-restraint with how it uses data as it builds up its user base only to significantly modify terms of service once a loyal fan base is dependent upon its product for everyday communication.[88]

---

83. Brian Fung, *FCC Chairman: 'A Duopoly' Dominates Basic Internet Service in America*, WASH. POST (Sept. 4, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/04/fcc-chairman-a-duopoly-dominates-basic-internet-service-in-america/.

84. Duopolies in general do not produce desirable outcomes when it comes to the first and last mile of Internet access for a variety of reasons. *See* Nicholas Economides, *Broadband Openness Rules Are Fully Justified by Economic Research*, 84 COMMS. & STRATEGIES 1, 1–5 (2011). "The academic literature, as well as DOJ, strongly supports the position that a duopoly market confers greater market power and ability to charge higher prices and to engage in other anticompetitive practices than markets with more competitors. In the broadband context, market power possessed by residential broadband access network providers allows them to impose fees on content and applications providers to the detriment of social welfare." *Id*. at 2.

85. For more information about how Google collects information to build profiles and tailor advertisements, see SIVA VAIDJYANATHAN, THE GOOGLIZATION OF EVERYTHING: (AND WHY WE SHOULD WORRY) 83–85 (2012).

86. *Protecting Consumer Privacy in an Era of Rapid Chang*e, FTC REPORT 60, 68 (Mar. 2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

87. *See generally* Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907 (2013); Richard P. Console, Jr., *Examining Your Rights and Facebook's Privacy Policies*, ADWEEK SOCIAL TIMES (July 2, 2013, 2:17 PM), http://www.adweek.com/socialtimes/guest-post-rights-facebook-privacy-policies/294671.

88. One example lies in Facebook, which began in 2004 and continues to modify its terms of service and privacy policy as it grows. *See* Matt McKeon, *The Evolution of Privacy on Facebook*, BUS. INSIDER (May 7, 2010, 3:55 PM), http://www.businessinsider.com/the-evolution-of-privacy-on-facebook-2010-5; Kate Knibbs, *Don't Be Fooled by that Nice Blog Post,*

B. Recent Legal Challenges to Data Use Terms

It is well-established that consumers do not read terms of service agreements, understand their ramifications, or expect that their data will be collected and used in such dynamic ways.[89] Nonetheless, courts generally uphold terms of service agreements in the digital world, thereby keeping the consent regime alive and well.[90]

Federal statutes, such as the Electronic Communication Privacy Act (ECPA),[91] Computer Fraud and Abuse Act,[92] Video Protection Privacy Act,[93] and state laws,[94] are often invoked, albeit generally unsuccessfully, to sue online-service providers for alleged privacy violations. All were relied upon in a class action suit against Facebook that ultimately settled due in part to Facebook's release of users' private details without their affirmative consent through its Beacon program, which automatically shared users' web behavior with their friends.[95] This case highlights the need for user consent for the sharing of personal information because, while there are some boundaries to how a user consents, courts have broadly interpreted what a service provider may do once they obtain valid consent.

The federal Wiretap Act, as amended by the ECPA, prohibits the unlawful interception of wire, oral, or electronic communications.[96]

Facebook's Latest Privacy Change is a Big Deal, DIGITAL TRENDS (Oct. 12, 2013), http://www.digitaltrends.com/social-media/facebooks-privacy-changes-are-a-big-deal/; Brian Fung, *Your Facebook Privacy Settings are about to change. Again*, WASH. POST (Apr. 8, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/04/08/your-facebook-privacy-settings-are-about-to-change-again/.

89. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y 540 (2008).

90. Juliet M. Moringiello & William L. Reynolds, *From Lord Coke to Internet Privacy: The Past, Present, and Future of the Law of Electronic Contracting*, 72 MD. L. REV. 452, 478–79 (2013) (discussing that the length of agreements and whether a consumer has read them does not necessarily alter their enforceability even if other legal issues do).

91. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510–32, 2701–12, 3121–27 (2013)).

92. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified at 18 U.S.C. § 1030 (2013)).

93. Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (1988) (codified at 18 U.S.C. § 2710 (2002)).

94. For example, the California Consumer Legal Remedies Act, CAL. CIV. CODE §§ 1750–56 (West 2013), and the California Comprehensive Computer Data Access and Fraud Act, CAL. PENAL CODE § 502 (West 2013).

95. Lane v. Facebook, Inc., 696 F.3d 811 (9th Cir. 2012), *cert. denied*, 134 S. Ct. 8 (2013); David Kravets, *Facebook's $9.5 Million 'Beacon' Settlement Approved*, WIRED (Sept. 21, 2012), http://www.wired.com/2012/09/beacon-settlement-approved/.

96. 18 U.S.C. §§ 2510–2522 (2013).

Consequently, plaintiffs have attempted to use this law and the related Stored Communications Act[97] to sue companies engaged in online data collection and sharing on unlawful interception grounds.[98] A seminal and oft-cited case involving online ad data broker DoubleClick distinguished early on the behavior of cookies from activities prohibited by the ECPA.[99] Due to this consent regime, users today are subjected to a variety of online tracking mechanisms more dynamic than cookies because users consent to the terms of the sites they are browsing and those sites consent to tracking relationships with advertising companies.[100]

Beyond web browser tracking technologies, plaintiffs have also attempted to use the ECPA to restrict ISP's commercial use of their data. In *Kirch v. Embarq*, the 10th Circuit of the U.S. Court of Appeals held that an ISP did not violate the ECPA when it permitted an advertising company, NebuAd, to access the network traffic data of the ISP's customers to conduct market research about their online behavior.[101] The court reasoned that Embarq accessed the information in the same way it had in the normal course of business and therefore did not "intercept" customer data.[102] Moreover, the court noted that NebuAd could not be held liable for any violation of the ECPA merely for receiving the data that was passed along to it by Embarq, which collected the data.[103]

A user must know that they are assenting to terms by clicking a button or engaging in some other form of acceptance in order for the terms to be enforceable.[104] However, this does not mean that the user actually needs to know what the terms are even if they are required to

97. *Id.* §§ 2702–2711.

98. *See* Johnathan D. Frieden, Charity M. Price & Leigh M. Murray, *Putting the Genie Back in the Bottle: Leveraging Private Enforcement to Improve Internet Privacy*, 37 WM. MITCHELL L. REV. 1671, 1706–1712 (2011) (describing several cases involving federal privacy law and online data privacy).

99. *In re* DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

100. Omer Tene & Jules Polonetsky, *To Track or 'Do Not Track': Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 281, 291, 313 (2012), *available at* http://cyberlaw.stanford.edu/files/publication/files/totrack-or-dono track.pdf.

101. Kirch v. Embarq Mgmt. Co., 702 F.3d 1245, 1248–49 (10th Cir. 2012), *cert. denied*, 133 S. Ct. 2743 (2013).

102. *Id.* at 1248–50.

103. *Id.*

104. Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 28–30 (2d Cir. 2002) (finding that Netscape did not inform users that they were agreeing to terms of service merely by clicking "download" to install software.).

be aware of their existence and understand how to navigate to them.[105] Several recent cases out of Silicon Valley have showcased the struggles plaintiffs face in challenging terms of service and accompanying privacy policies. In one such case, the U.S. District Court for the Northern District of California held that a terms-of-use contract remained enforceable even when a user was not presented with the terms directly but instead with a link to the information through the mobile app interface of a Zynga videogame.[106]

The U.S. District Court for the Northern District of California has also analyzed the applicability of the ECPA to online service providers' use of consumer data.[107] In a case involving Gmail, the court denied with leave to amend part of Google's motion to dismiss and analyzed plaintiffs' claims of unlawful interception under the Wiretap Act.[108] The court explained that consent must be explicit and not merely based on the notion that a user knows the service provider is capable of intercepting communications for a certain purpose.[109] Instead, the court reasoned that terms of service must clearly explain how such collected data will be used.[110] In this instance, the court found that Google's terms of service and privacy policy during the relevant time period only elicited consent for email data to be intercepted for purposes unrelated to creating advertising profiles.[111] Therefore, the court concluded, users did not explicitly consent to the use of their Gmail correspondence for such use even if they were arguably on notice that Google had such a capability.[112]

In the same district, an analysis of LinkedIn's policy and plaintiffs' online behavior persuaded the court that explicit consent meant that LinkedIn's collection of data from users' Gmail accounts did not violate the ECPA.[113] Instead, the court reasoned that the user provided consent under the SCA and authorization under the Wiretap Act when they clicked through the LinkedIn account creation

105. *Id.*

106. Swift v. Zynga Game Network, Inc., 805 F. Supp. 2d 904, 910–12 (N.D. Cal. 2011).

107. *In re* Google Inc., 13-MD-02430-LHK, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013), *motion to certify appeal denied*, 5:13-MD-2430-LHK, 2014 WL 294441 (N.D. Cal. Jan. 27, 2014).

108. *Id.*

109. *Id.*

110. *Id.*

111. *Id.*

112. *Id.*

113. Perkins v. LinkedIn Corp., 13-CV-04303-LHK, 2014 WL 2751053, at 13, 14 (N.D. Cal. June 12, 2014).

questions.[114] Notably, the plaintiffs unsuccessfully argued that they did not know how LinkedIn defined "Google Contacts" and were unaware that they were consenting to LinkedIn's import of every email address they had communicated with from their Gmail account.[115] Here, the court distinguished a notice "presented immediately prior to the moment" of acceptance from "a disclosure buried in a Terms of Service or Privacy Policy that may never be viewed."[116]

In a case against Google, the Northern District of California also made clear that proving injury in fact is a hurdle for plaintiffs who claim nothing more than the mere monetization of their information as their alleged harm.[117] This case highlighted that the ECPA is also problematic for plaintiffs because the ordinary course of business exception to the ECPA's restrictions has been interpreted to include those furthering legitimate business purposes.[118]

In another case heard by the U.S. District Court for the Northern District of California, the court rejected the notion that a mobile phone was a "facility" under the SCA's definition of an electronic communication service.[119] Moreover, the court explained that location data stored on the device was not "electronic storage" for purposes of the statute.[120] A similar argument was rejected by the U.S. District Court for the Western District of Washington in litigation involving Microsoft, when that court also determined that a user's mobile device was not a "facility" for purposes of the SCA.[121] The court reasoned that the mere fact that a smartphone can send and receive data does not make it a facility, which by definition provides services to other users.[122] Ultimately, the court concluded that the SCA was intended to protect computers used in a server-like manner, providing electronic storage.[123]

---

114. *Id.*

115. *Id.*

116. *Id.*

117. *In re* Google, Inc. Privacy Policy Litig., C-12-01382-PSG, 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013).

118. *Id.* at 11.

119. *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1057–58 (N.D. Cal. June 12, 2012).

120. *Id.* at 1059.

121. Cousineau v. Microsoft Corp., 6 F. Supp. 3d 1167, 1174–75 (W.D. Wash. Mar. 25, 2014).

122. *Id.* at 1175.

123. *Id.*

The U.S. District Court for the Northern District of California dismissed a case with leave to amend from plaintiffs who alleged that iPhone apps' collection of device information, including contacts, violated a myriad of legal rights, including those under the ECPA.[124] In this case, the court distinguished "the use of data by different memory components of the same device" from an unlawful interception barred by the ECPA.[125] Taken together, the judicial guidance from the heart of Silicon Valley seems to suggest that terms of service and privacy policies must, at least in a general way, inform consumers as to what type of data will be used and for which categorical purposes. However, consumers have little recourse against the creative ways in which their data will be used within those broad categories once they have provided consent.

Despite significant court hurdles for plaintiffs who challenge terms after consenting to them, the Federal Trade Commission (FTC) offers another approach to shaping privacy policies through its enforcement role against companies that engage in false and misleading practices.[126] In 2009, the FTC filed a complaint against Sears after it "collected consumers' personal information" through software installed on their computers, including data "such as the contents of shopping carts, online bank statements, drug prescription records, video rental records, library borrowing histories, and the sender, recipient, subject, and size for Web-based e-mails."[127] The FTC's complaint resulted in a settlement by which Sears agreed to destroy the collected data and properly disclose what its software would "monitor, record, or transmit" if it chose to provide similar tracking software to consumers in the future.[128]

The FTC also reached a settlement with Google after the company launched its now-defunct Buzz social media service by automatically

124. Opperman v. Path, Inc., 13-CV-00453-JST, 2014 WL 1973378 (N.D. Cal. May 14, 2014).

125. *Id.* at 11.

126. Jeffrey T. Cox & Kelly M. Cline, *Parsing the Demographic: The Challenge of Balancing Online Behavioral Advertising and Consumer Privacy Considerations*, 15 J. INTERNET L. 1, 3 (2012).

127. Press Release, Fed. Trade Comm'n, FTC Approves Final Consent Order Requiring Sears to Disclose the Installation of Tracking Software Placed on Consumers Computers (Sept. 9, 2009), http://www.ftc.gov/news-events/press-releases/2009/09/ftc-approves-final-consent-order-requiring-sears-disclose.

128. *Id.*

enrolling Gmail users.[129] As a result, the FTC required the company to divulge how "information will be disclosed to one or more third parties, (2) the identity or specific categories of such third parties, and (3) the purpose(s) for respondent's sharing" and obtain express affirmative user consent for data sharing.[130] A year later, the FTC fined Google $22.5 million when it violated the agreement by surreptitiously tracking users of Apple's Safari web browser who had opted out of such monitoring.[131]

Collectively, the aforementioned cases imply that companies may use and share consumer data in robust ways so long as their privacy policies suggest, at least in broad terms, what type of data will be collected and shared. Given this scenario, it may be advantageous for companies to be somewhat vague in their terms of service and data use policies to help shield full disclosure or not divulge trade secrets while still protecting them from potential liability.

C. Data Use Rights & Terms of Service: Verizon, Google & Facebook

For the sake of efficiency, terms of service involved in the layers of the Internet tend to be "take it or leave it" propositions, yet contain important language regarding data use policies. Therefore, the terms of use for three companies that serve as primary Internet portals for many—Verizon, Google and Facebook—are important to analyze as they each serve as an example of a layer of the Internet. The following section examines these portals' terms of service, focusing primarily on what rights are conferred with regard to their data use policies. More specifically, the following questions are discussed. What does each company collect and do with the data? Is there any reference to third party use of the data? If so, how are these parties defined? What distinguishes a "third party" from an "affiliate" or "partner" for purposes of terms of use agreements? Aren't they all third parties to the consumers agreeing to the terms? Are these companies telling us everything they're doing with user data?

---

129. Google Inc., Docket No. C-4336, FTC File No. 102-3136 (Mar. 30, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf.

130. *Id.* at 4

131. Press Release, Fed. Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser, (Aug. 9, 2012), http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

1. Verizon

Verizon Communications Inc. (Verizon) offers broadband Internet service to consumers through both fixed (wired) and mobile (wireless) services. Wired services include Direct Subscriber Line (DSL) and Fiber Optic Service (FiOS) that generally connect consumers in residential and business locations.[132] Verizon Wireless offers cellular Internet connections such as 4G LTE to consumers using wireless devices or specialized antennas and routers.[133] Verizon users agree to different terms depending on which method they use to connect to the Internet.[134]

Verizon Wireless' customer agreement,[135] for mobile users, and the Verizon Online Terms of Service,[136] which applies to wired broadband, binds customers to Verizon's common Privacy Policy.[137] The policy discloses information about what Verizon collects from its subscribers but is not as detailed regarding how the information is used, how long it is retained, or with which specific parties the information is shared.[138] Among other things, Verizon collects data about "websites visited, wireless location, application and feature usage, network traffic data, [and] product and device-specific information."[139] This information can be used by Verizon in a variety of ways, including marketing, network security, as well as for the research and development of new products.[140] Moreover, Verizon states that customer data "may be aggregated or anonymized for business and

132. *Services*, VERIZON, http://www.verizon.com/home/services/ (last visited Apr. 17, 2015).

133. *Home & Office Solutions*, VERIZON WIRELESS, http://www.verizonwireless.com/home-office-solutions/ (last visited Apr. 17, 2015).

134. Verizon's global privacy policies specifies different terms depending on the service, including a section called "Additional Information for Wireless Customers." *See Privacy Policy*, VERIZON, http://www.verizon.com/about/privacy/policy/ (last visited Apr. 17, 2015).

135. *Customer Agreement*, VERIZON WIRELESS, http://www.verizonwireless.com/b2c/support/customer-agreement (last updated Feb. 5, 2015).

136. *Verizon Online Terms of Service*, VERIZON, http://www.verizon.com/idc/groups/public/documents/adacct/verizon_internet_tos_121614.pdf (last visited Aug. 15, 2014).

137. *Privacy Policy*, VERIZON, http://www.verizon.com/about/privacy/policy/ (last updated Aug. 2014).

138. *Id.*

139. *See id.* (explaining the information collected when using Verizon products and services).

140. *Id.*

marketing uses" by the company or third parties.[141] Notably, the amount of data included in an *aggregated* collection is not defined.[142]

Verizon also passively collects data about its users. For example, Verizon can receive Facebook friend list data and information about a Facebook user's "likes" when a Verizon customer uses a Facebook account to log into Verizon services.[143] Verizon also collects demographic data about subscribers from third parties.[144] The privacy policy highlights examples of such information as "gender, age range, sports enthusiast, frequent diner, or pet owner."[145] This data is combined with data Verizon collects from other companies to build customer profiles for direct advertising purposes.[146] However, Verizon states that they require affirmative consent from customers prior to using data based on their visits "over time" to non-Verizon websites for direct customized advertising.[147]

Verizon also uses cookies to collect information about users as they visit Verizon websites and navigate through any websites on which Verizon is advertising.[148] When this occurs, Verizon collects "IP address, mobile telephone or device number, account information, web addresses of the sites you come from and go to next and information about your connection, including your device's browser, operating system, platform type and Internet connection speed."[149] In doing so, Verizon abides by the self-regulating principles of the Digital Advertising Alliance that permits people to opt out of such behavioral advertising programs.[150]

Verizon takes additional liberties with data collection for wireless customers.[151] The company collects mobile usage and location

141. *Id.*

142. *Verizon Privacy Policy*, *supra* note 137.

143. *Id.* (under heading "Information Provided to Us by Third Parties").

144. *Id.*

145. *Id.* (under heading "Information Provided to or Used by Third-Party Advertising Entities or Social Networks").

146. *Verizon Privacy Policy*, *supra* note 137 (under heading "Additional Information for Wireless Customers").

147. *Id.* (under heading "Information Collected When You Use Verizon Products and Services").

148. *Id.*

149. *Id.*

150. *Id.*; *see also* DIGITAL ADVERTISING ALLIANCE (DAA) SELF-REGULATORY PROGRAM, http://www.aboutads.info/ (last visited Apr. 17, 2015).

151. *Verizon Privacy Policy*, *supra* note 137 (under heading "Additional Information for Wireless Customers").

information from its subscribers and reserves the right to use it in "marketing reports."[152] Information such as websites visited and even search terms are collected and combined with other information Verizon receives to create the marketing reports.[153] Verizon claims the right to share these reports with other companies but in a non-personally identifiable way.[154] However, Verizon allows customers to opt out of their information being shared in these reports by contacting the company.[155]

Verizon shares information inside its "family of companies" and with third parties.[156] The Privacy Policy contains a dedicated section specifically addressing third party advertisers.[157] Verizon reserves the right to share data about its users' web browsing history, geographic information, and demographic information in an anonymous way.[158] However, Verizon's policy permits wired and wireless Internet customers to opt out of relevant advertising.[159] The policy confers other opt-out rights to users. For example, Verizon permits users to choose whether or not to share their Customer Proprietary Network Information[160] with other Verizon entities for marketing unrelated to the subscribers' current services.[161] This occurs in part because VoIP receives protection under federal laws related to telecommunication privacy.[162] Verizon does not publicize specific data retention policies and instead notes that it retains the information it collects about its

152. *Id.*

153. Verizon notes that collected data includes: "Mobile usage information includes the addresses of websites you visit when you use our wireless services. These data strings (or URLs) may include search terms you have used." *Id.*

154. *Id.*

155. *Id.*

156. *Verizon Privacy Policy*, *supra* note 137 (under heading "Information We Share").

157. *Id.* (under heading "Information Provided to or Used by Third-Party Advertising Entities or Social Networks").

158. *Id.*

159. *Id.* (under heading "Relevant Advertising").

160. Verizon defines this as "type, technical arrangement, quantity, destination, location, and amount of use of telecommunications and interconnected Voice over Internet Protocol (VoIP) services and related billing information." *Privacy Policy*, *Customer Proprietary Network Information or CPNI*, VERIZON, http://www.verizon.com/about/privacy/cpni/ (last visited May 27, 2015); *see also* 47 U.S.C. § 222 (2013).

161. *Verizon Privacy Policy*, *supra* note 137 (under heading "Information We Share").

162. Implementation of the Telecom Act of 1996, CPNI, Docket 96-115, IP Enabled Services Proceeding, Docket 04-36.

customers "only as long as reasonably necessary for business accounting, tax or legal purposes."[163]

Verizon's terms contain a seemingly standard disclaimer outlining the specific circumstances under which the company will share individualized information about a customer or their device, such as when legally required to, or when a user consents.[164] "Verizon does not sell, license or share information that individually identifies our customers, people using our networks, or website visitors with others outside the Verizon family of companies for non-Verizon purposes without the consent of the person whose information will be shared."[165] Verizon acknowledges in its software-development kit's terms of service that an advertiser might obtain personally identifiable information of a user via user interaction with the ad.[166] In addition, "[i]f Verizon enters into a merger, acquisition or sale of all or a portion of its assets or business, customer information will also be transferred as part of or in connection with the transaction."[167]

Verizon may pair wired desktop web browsing information with wireless browsing data.[168] Verizon may use "information such as call records, websites visited, wireless location, application and feature usage, network traffic data, service options you choose, mobile and device number, and other similar information" to determine users' "eligibility" for new products or services in addition to marketing to customers.[169] In addition to Verizon's specific use of the information, the policy makes clear that, "[t]his type of information may be aggregated or anonymized for business and marketing uses by us or by third parties."[170]

---

163. *Verizon Privacy Policy*, *supra* note 137 (under heading "Information Security and Data Retention").

164. *Verizon Privacy Policy*, *supra* note 137 (under heading "Information Shared Outside the Verizon Family of Companies").

165. *Id.*

166. *Terms of Use,* Navbuilder Inside Software Development Kit and Service Agreement, VERIZON DEVELOPER COMMUNITY, http://developer.verizon.com/content/vdc/en/verizon-tools-apis/verizon_apis/navbuilder-inside-sdk/verizon-toolsandapis-nbi-downloads/verizon-toolsandapis-nbi-downloads/nbi_sup_terms.html (last updated June 19, 2012).

167. *Verizon Privacy Policy*, *supra* note 137 (under heading "Information Shared Outside the Verizon Family of Companies").

168. *Id.* (under heading "Information We Collect and How We Use It").

169. *Important Information About Verizon Wireless Broadband Internet Access Services*, VERIZON WIRELESS, http://www.verizonwireless.com/support/information/broadband.html (last visited Aug. 15, 2014).

170. *Id.*

Verizon reserves the right to change their policy at any time and therefore encourages users to check back often.[171] Also, Verizon warns users that "[i]f Verizon elects to use or disclose information that identifies you as an individual in a manner that is materially different from that stated in our policy at the time we collected that information from you, we will give you a choice regarding such use or disclosure by appropriate means, which may include use of an opt-out mechanism."[172] This effectively means that Verizon could opt-in users for new uses of collected data only to offer an opportunity to opt-out after the fact.

2. Google

Google offers an entire device and service ecosystem through which consumers can enjoy instant synchronized access to entertainment and productivity suites.[173] This seamless integration stems in part from collecting and sharing data between the company's many free services.[174]

Traditional desktop giant Microsoft historically did not collect robust consumer-use data from its Windows desktop-operating system.[175] Google, however, collects device and usage information via its Android OS and services,[176] and defines devices broadly to include any "desktop, tablet or smartphone" that is used to access Google's

171. *Verizon Privacy Policy*, *supra* note 137 (under heading "Changes to This Policy").

172. *Id.*

173. Dylan Love, *The Era of the Tech 'Ecosystem'—Who to Go With and Why*, INT'L BUS. TIMES (Nov. 3, 2014), http://www.ibtimes.com/era-tech-ecosystem-who-go-why-1717170. For a list of Google's offerings, see *About Google–Products*, GOOGLE, http://www.google.com/about/products/

174. *Id.*; Michael deAgonia, Preston Gralla & JR Raphael, *Battle of the Media Ecosystems: Amazon, Apple, Google and Microsoft*, COMPUTER WORLD (Aug. 2, 2013), http://www.computerworld.com/article/2483616/personal-technology/battle-of-the-media-ecosystems--amazon--apple--google-and-microsoft.html.

175. Today's user behavior is interconnected with Internet queries instead of solely relying upon local computer resources. *See* Tim O'Reilly, *The State of the Internet Operating System*, RADAR (Mar. 29, 2010), http://www.radar.oreilly.com/2010/03/state-of-internet-operating-system.html. Whereas, Windows 95 was the first version of Windows to even have built-in Internet connectivity. *See A History of Windows*, MICROSOFT, http://windows.microsoft.com/en-us/windows/history#T1=era4 (last visited May 18, 2015). Even as Windows' own data collection became more robust, such data was still stored locally in the operating system's registry. *See* Vivienne Mee, Theodore Tryfonas & Iain Sutherland, *The Windows Registry As A Forensic Artefact: Illustrating Evidence Collection For Internet Usage*, 3 DIGITAL INVESTIGATION 166 (2006).

176. *Privacy Policy*, Information We Collect, GOOGLE PRIVACY & TERMS, http://www.google.com/intl/en/policies/privacy/ (last modified Feb. 25, 2015).

services.[177] As Google explains, this allows the company to tailor ads based on information about a user's computer or device, including their device model, browser type, or sensors in their device such as the accelerometer.[178]

Naturally, users contribute data to Google when they consume content such as YouTube videos or communicate through Google services by sending their search queries to the company and, along with them, user behavior patterns such as video choices, viewing habits, and preferences. More surreptitiously, however, extensive data is collected from Google and non-Google Web users alike as they encounter Google's HTTP Referrers, cookies, and pixel tags throughout the Web.[179] Google can use its trove of collected data in a variety of ways, even to conduct market research for its own product development.[180] However, Google bars some uses and "prohibit[s] advertisers from remarketing based on sensitive information, such as health information and religious beliefs."[181]

Google analyzes the content of communications on its services, such as Gmail, to tailor ad content.[182] Google's privacy policy states that the company collects log information, location data, unique application numbers, local storage, cookies, and anonymous identifiers.[183] Google also notes that it may correlate a user's phone number and unique device identifier with their account.[184] Moreover, Google combines user information collected amongst its various services.[185] However, the company asserts that it does not combine information from the cookies of its DoubleClick subsidiary with

177. *Key Terms*, Device, GOOGLE PRIVACY & TERMS, http://www.google.com/intl/en/policies/privacy/key-terms/#toc-terms-device (last visited Aug. 15, 2014).

178. *Advertising*, Other Technologies Used in Advertising, GOOGLE PRIVACY & TERMS, https://www.google.com/intl/en/policies/technologies/ads/ (last visited Aug. 15, 2014).

179. *Privacy Policy*, How We Use Information We Collect, GOOGLE PRIVACY & TERMS, http://www.google.com/intl/en/policies/privacy/#infouse (last modified Feb. 25, 2015).

180. Greg Satell, *How Google is Quietly Taking Over*, FORBES (July 30, 2013), http://www.forbes.com/sites/gregsatell/2013/07/30/how-google-is-quietly-taking-over/.

181. *Advertising*, Why Am I Seeing Ads By Google For Products I've Viewed?, GOOGLE PRIVACY & TERMS, https://www.google.com/intl/en/policies/technologies/ads/ (last visited Aug. 15, 2014). This self-imposed restriction might be difficult to implement in practice.

182. *Ads You'll Find Most Useful*, GOOGLE PRIVACY & TERMS, http://www.google.com/intl/en/policies/privacy/example/ads-youll-find-most-useful.html (last visited Aug. 15, 2014).

183. *Privacy Policy*, Information We Collect, GOOGLE PRIVACY & TERMS, http://www.google.com/intl/en/policies/privacy/#infocollect (last modified on Feb. 25, 2015).

184. *Id.*

185. *Id.*

personally identifiable information.[186] Google's policy states that it shares *personally identifiable information* with third parties only if a user consents but may share *aggregated*, non-personally identifiable information with third parties without further consent.[187]

Google collects a lot of information about users' real world interactions with electronics. For example, Google collects a vast amount of telephone data, which includes a user's "phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls."[188] Google collects information about the "use of apps and domains (but not full URLs)" from Chromecast.[189] Consequently, Chromecast allows Google to know which online movies people decide to stream when using the device.[190]

Google states that it does not *sell* its users' "personal information."[191] However, such information is defined rather narrowly to include only "information which you provide to us which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google."[192] This statement does not appear to disavow Google from *sharing* personal information or selling user information that does not explicitly identify them. For example, Google may send information to "trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other

186. *Id.*

187. *Privacy Policy,* Information We Share, GOOGLE PRIVACY & TERMS, http://www.google.com/intl/en/policies/privacy/#nosharing (last modified Feb. 25, 2015).

188. *Privacy Policy*, Information We Collect, Log Information, GOOGLE PRIVACY & TERMS, http://www.google.com/intl/en/policies/privacy/ (last modified Feb. 25, 2015).

189. *Chrome Privacy Notice*, Information Google Receives When You Use Chrome, GOOGLE CHROME, https://www.google.com/intl/en/chrome/browser/privacy/ (last modified Nov. 12, 2014).

190. This occurs by virtue of the fact that a user must sign into Chromecast with a Google account in order to use it and is then subject to the data use policies of Google services. Like other Google products, Chromecast enables the company to collect data. *See* Steve Baldwin, *Chromecast—5 Things To Know*, DIDIT (Aug. 13, 2013), http://www.didit.com/chromecast-5-things-to-know/

191. *Technologies and Principles*, Give Users Meaningful Choices to Protect Their Privacy, GOOGLE PRIVACY & TERMS, http://www.google.com/intl/en/policies/technologies/ (last visited Aug. 15, 2014).

192. *Key Terms*, GOOGLE PRIVACY & TERMS, https://www.google.com/policies/privacy/key-terms/#toc-terms-personal-info (last visited Aug. 15, 2014).

appropriate confidentiality and security measures."[193] However, the company does not define what a trusted business or person is.

Google notes that the privacy policy applies to all of its services, with some exceptions, but the company does not provide an exhaustive list of exempt services.[194] Elsewhere in the privacy policy, four discrete policies are identified for Google Chrome,[195] Wallet,[196] Fiber,[197] and Books.[198]

Google's Chrome Privacy Notice applies to Chrome OS in addition to the Chrome Web browser.[199] Use of Chrome to browse the Web ostensibly gives Google more insight into a user's Web browsing habits than a user who used Google's services but opted for another browser such as Internet Explorer, Firefox, or Safari.[200] However, Google's policy explains to users "the fact that you are using Chrome does not cause Google to receive any special or additional personally identifying information about you."[201] Despite this, users still transmit Web search and URL information to Google via Chrome, and Google combines information from its multitude of services, including personally identifiable information.[202] Nonetheless, Google explains to Chrome users: "Google will notify you of any material changes to this

193. *Privacy Policy*, Information We Share, GOOGLE PRIVACY & TERMS, http://www.google.com/intl/en/policies/privacy/#nosharing (last modified Feb. 25, 2015).

194. *Privacy Policy*, When This Privacy Policy Applies, GOOGLE PRIVACY & TERMS, http://www.google.com/intl/en/policies/privacy/#application (last modified Feb. 25, 2015).

195. *Google Chrome Privacy Notice*, Information Google Receives When You Use Chrome, GOOGLE CHROME, https://www.google.com/intl/en/chrome/browser/privacy/ (last visited Aug. 15, 2014).

196. *Google Wallet Privacy Notice*, Affiliate Sharing, GOOGLE, https://wallet.google.com /legaldocument?family=0.privacynotice (last modified May 7, 2014).

197. *Google Fiber Privacy Notice*, GOOGLE FIBER, https://fiber.google.com/legal /privacy.html (last visited Aug. 15, 2014).

198. *Google Play—Privacy Policy for Books*, GOOGLE (Oct. 13, 2011), http://www.google.com/googlebooks/privacy.html.

199. *Information Google Receives When You Use Chrome*, GOOGLE PRIVACY & TERMS, https://www.google.com/intl/en/chrome/browser/privacy/ (last visited Aug. 15, 2014).

200. For example, Google collects user-typed URLs that do not resolve to active websites when users do so through Chrome but not through other browsers. *Google Chrome Privacy Notice*, Information Google Receives When You Use Chrome, GOOGLE CHROME, https:// www.google.com/intl/en/chrome/browser/privacy/ (last visited Aug. 15, 2014).

201. *Id.*

202. *Privacy Policy*, How We Use Information We Collect, GOOGLE PRIVACY & TERMS, http://www.google.com/intl/en/policies/privacy/#infouse (last modified Feb. 25, 2015); *Privacy Policy*, Combine Personal Information From One Service With Information, Including Personal Information, From Other Google Services, GOOGLE PRIVACY & TERMS, http://www.google.com /policies/privacy/example/combine-personal-information.html (last visited May 18, 2015).

policy, and you will always have the option to use Chrome in a way that does not send any personally identifiable information to Google, or to remove your information and discontinue using it."[203]

The policy for Google's fiber optic-based ISP, Google Fiber, notes that Google's primary policy is applicable to Fiber customers. Although a Google account is used to connect to Fiber, "[o]ther information from the use of Google Fiber Internet (such as URLs of websites visited or content of communications) will not be associated with the Google Account" used for Google Fiber unless a user consents.[204] However, Google notes that it "may share non-personally identifiable information publicly and with" its partners, which it describes as "content providers, publishers, advertisers or connected sites."[205]

The policy for Google's digital payment service, Google Wallet, notes that the information it collects regarding a user's financial transactions is shared with the company's subsidiaries.[206] However, Google permits users to opt-out of the sharing of information about their creditworthiness and to opt-out out of targeted marketing from other Google entities based on Google Wallet information.[207]

Google Books' policy advises that book purchase information collected through the Google Play store is retained indefinitely and cannot be deleted by the user.[208] Like other Google services, information about a user's device and web browser is collected when a user browses books online.[209] Moreover, a user's unique device identifier and the last five pages a user has viewed for each book viewed in Google Books is saved to enforce copyright policy and viewing limits.[210]

---

203. *Google Chrome Privacy Notice*, *supra* note 200.

204. *Google Fiber Privacy Notice*, GOOGLE FIBER, https://fiber.google.com/legal/privacy.html (last modified Nov. 12, 2014).

205. *Google Fiber Privacy Notice*, Information We Share, GOOGLE FIBER, https://fiber.google.com/legal/privacy.html (last visited Aug. 15, 2014).

206. *Google Wallet Privacy Notice*, Affiliate Sharing, GOOGLE WALLET, https://wallet.google.com/legaldocument?family=0.privacynotice (last modified May 7, 2014).

207. *Id.*

208. *Google Play—Privacy Policy for Books*, GOOGLE BOOKS (Oct. 13, 2011), http://www.google.com/googlebooks/privacy.html.

209. *Id.*

210. *Id.*

3. Facebook

From its infancy as a mere social media network, Facebook has evolved into an all-inclusive web portal from which users post intimate details about their lives, share information from outside sites, message each other, and even search the Web.[211] The company has one comprehensive Data Use Policy to govern privacy for its Web and mobile app portals.[212]

By its very nature, the company logs virtually all user activity within Facebook, including details about which content a user browses and the frequency of use.[213] Along with this, Facebook collects users' IP addresses, mobile phone numbers, browser types, ISP names, operating system versions, locations, and other device data.[214] Facebook then correlates such data to associate it with all of a user's devices.[215] Moreover, Facebook collects data on a user's "activities on and off Facebook from third-party partners" but does not specify the exact type or define the scope of information it receives.[216]

Facebook places social network plugins such as "Like" buttons on other, non-Facebook controlled websites. When a user visits one of these websites while logged into their Facebook account, Facebook collects information including their user ID and the URL of the website visited along with "the date and time and other browser-related info."[217] Even users not logged-in to Facebook can transmit data back to Facebook by visiting pages with embedded "Like" buttons.[218]

211. Tom Simonite, *What Facebook Knows*, MIT TECH. REV. (June 13, 2012), *available at* http://www.technologyreview.com/featuredstory/428150/what-facebook-knows/.

212. *Data Policy*, FACEBOOK, https://www.facebook.com/full_data_use_policy (last updated Jan. 30, 2015).

213. *Id.*; Mary C. Long, *Using the Facebook Activity Log Like a Boss*, ADWEEK (Nov. 20, 2014, 7:52 AM), http://www.adweek.com/socialtimes/facebook-activity-log/301717.

214. *Data Policy*, Other Information We Receive About You, FACEBOOK, https://www.facebook.com/full_data_use_policy#infoaboutyou (last updated Jan. 30, 2015).

215. *Id.*

216. *Id.*

217. *About Social Plugins*, FACEBOOK HELP CENTER, https://www.facebook.com/help/443483272359009 (last visited Apr. 8, 2015).

218. *Desktop Help: Apps, Games & Payments*, What Information Does Facebook Get When I Visit A Site With The Like Button?, FACEBOOK HELP CENTER, https://www.facebook.com/help/443483272359009 (last visited Apr. 8, 201) ("Like other sites on the Internet, we receive info about the web page you're visiting, the date and time and other browser-related info.").

Facebook's Data Policy notes that information, regardless of its source, is stored "as long as it is necessary to provide products and services."[219]

Facebook shares robust information with sites and apps that are integrated with its own services.[220] Facebook permits "third-party apps, websites and or other services that use or are integrated with" its services to receive information about what content users post or share and provide access to a user's ID, friend list, and other information in the user's public profile.[221] However, Facebook allows users to opt-out of this feature via a user's "Apps" page in their Facebook account privacy settings.[222]

Facebook states that it shares information only with its advertising partners after it has removed a user's name or email address or aggregated the user's data.[223] A user may adjust their advertising preferences to better control the types of ads they see.[224] In addition, a user may request to opt out of information collection or use for the purpose of showing ads on Facebook through the Digital Advertising Alliance.[225]

---

219. *Data Policy*, How Can I Manage Or Delete Information About Me?, FACEBOOK, https://www.facebook.com/full_data_use_policy#infoaboutyou (last updated Jan. 30, 2015).

220. *Data Policy*, How is the Information Shared?, FACEBOOK, https://www.facebook.com/full_data_use_policy (last updated Jan. 30, 2015). This encompasses "a wide variety of products and services," including Facebook mobile app, Messenger, Paper, Slingshot, Room, Page Manager or Audience insights. *See Desktop Help*, What Are Facebook Services, FACEBOOK HELP CENTER, https://www.facebook.com/help/1561485474074139 (last visited May 13, 2015). Facebook may also share information with companies that it owns and operates, including Instagram LLC. *See Desktop Help*, The Facebook Companies, FACEBOOK HELP CENTER, https://www.facebook.com/help/111814505650678 (last visited Apr. 18, 2015).

221. *Data Policy*, How is the Information Shared?, FACEBOOK, https://www.facebook.com/full_data_use_policy (last updated Jan. 30, 2015).

222. *Desktop Help: Apps, Games & Payments*, Privacy for Apps & Websites, Games & Apps, FACEBOOK HELP CENTER, https://www.facebook.com/help/403786193017893/ (last visited May 13, 2015).

223. *Data Policy*, Advertising, Measurement, and Analytics Services, FACEBOOK, https://www.facebook.com/full_data_use_policy#inforeceived (last updated Jan. 30, 2015). Facebook does not share a user's personally identifying information with advertisers unless it receives permission to do so. Instead, Facebook's policy claims that it shares information with advertisers only after removing a user's name and other personally identifiable information. However, the terms imply that Facebook defines *personally identifiable information* as a name or email address but would nonetheless openly share such specific details as "25 year old female, in Madrid, who likes software engineering." This might mean that a third-party advertiser could infer a user's identity based on the complete set of characteristics that Facebook provides. *Id.*

224. *About Advertising on Facebook*, FACEBOOK, https://www.facebook.com/about/ads/.

225. *About Facebook Ads*, How Can I Adjust How Ads Are Targeted To Me Based On My Activity Off Of Facebook?, FACEBOOK HELP CENTER, https://www.facebook.com/help/56813749

Facebook lays out specific rules for its advertisers, including a provision informing them, "In no event may you use Facebook advertising data, including the targeting criteria for a Facebook ad, to build or augment user profiles, including profiles associated with any mobile device identifier or other unique identifier that identifies any particular user, browser, computer or device."[226] Moreover, Facebook forbids its advertisers from transferring data to a third party that thereafter transfers it to another ad network. Instead, Facebook permits data transfers only to parties involved in Facebook advertising.[227] While this restriction perhaps limits the scope of data sharing, it might do more to ensure that valuable data stays within Facebook's robust advertising ecosystem than it does to protect user privacy.

Despite the aforementioned data-sharing restrictions, Facebook provides information to companies beyond advertisers. The data use policy states:

> We transfer information to vendors, service providers, and other partners who globally support our business, such as providing technical infrastructure services, analyzing how our Services are used, measuring the effectiveness of ads and services, providing customer service, facilitating payments, or conducting academic research and surveys.[228]

Facebook requires companies with which it shares data to abide by "strict confidentiality obligations" and its data use policy.[229]

IV. ONE CONSENT MAY APPLY TO ALL: DATA USE PRACTICES & THE LAYERS OF THE INTERNET

The policies governing data use for Verizon, Google, and Facebook potentially mean that a user begins transmitting location, device, network traffic, and specific web browsing information to their Verizon wired or wireless ISP as soon as they connect their device online. Per Verizon's terms, such information is then likely retained for indefinite periods of time, anonymized, and compiled with data from

---

3302217#How-can-I-adjust-how-ads-are-targeted-to-me-based-on-my-activity-off-of-Facebook? (last visited May 13, 2015).

226. *Facebook Advertising Policies*, FACEBOOK, https://www.facebook.com/ad_guidelines.php (last updated Apr. 15, 2015).

227. *Id.*

228. *Data Policy*, FACEBOOK, https://www.facebook.com/full_data_use_policy (last updated Jan. 30, 2015).

229. *Id.*

other users in marketing reports. The same user will be assigned an anonymous unique identifier and be subject to targeted-mobile advertising through Verizon's Precision Insights products.[230]

Just as a user connects to the Internet with Verizon, their location and device information are simultaneously sent to Google from his Android OS device. Google's terms make clear that data about the personal use of mobile apps, Web browsing, and Google's services will be recorded by the company and shared with third party partners. Google may then combine this information with personally identifiable information and even data about a user's phone calls, although the personally identifiable part of the information is not *sold* to other parties, making it unclear as to whether it will be *shared* with them. Without any further notice to the user beyond the initial terms, Google will have in-depth online behavioral information that will be retained for an undefined period.

Next, according to Facebook's terms, the company may collect the user's device, IP address, location, and even web browsing information, especially if the user visits a website with embedded Facebook "like" buttons. This means that the user's behavior within Facebook is combined with their external Web behavior and physical location before being shared with Facebook advertisers.

Assuming a user thoroughly read the terms and understood how to opt-out of data collection and sharing as much as possible, ad hoc changes to privacy policies nevertheless could opt consumers into new data use and sharing provisions. Moreover, the data use policies in terms of service agreements for each provider do not readily cover what happens to data once it has been shared with a third party. That third party, for example, may also combine data from multiple sources and further share the information with other entities, meaning in effect that a singular consent may lead to the sharing of a user's data with multiple third parties. These third parties do not have to seek consent from individual users but will nevertheless benefit from big-data aggregation.

Corporate self-restraint by primary data collectors might control the types of data that exist elsewhere. For example, Verizon is now a major player in the behavioral marketing information marketplace and

230. *What We Do*, PRECISION MKT. INSIGHTS, http://precisionmarketinsights.com/?page_id=2309 (last visited Aug. 15, 2014); Robert L. Mitchell, *Why Verizon Wireless Wants to Share Your Data—And Why I Said No*, COMPUTERWORLD (Feb. 10, 2014), http://blogs.computerworld.com/privacy/23503/verizon-wireless-wants-share-your-data.

actively touts its unique ability to collect valuable data from its own mobile network to analyze virtual and real world customer activities.[231] The company has made it a point to assert that it does not sell raw data about its mobile phone users to third parties and instead merely shares broader trend data.[232] However, online data is so valuable to companies that there still exists a temptation to collect data even when privacy policies permit users to opt-out through industry-wide protocols.[233] For example, Google overrode privacy settings in Apple's Safari Web browser to track users without their knowledge by embedding special code within online advertisements.[234] As a result, Google agreed to a $17 million settlement with 36 states.[235] This highlights the lack of transparency in ensuring compliance with self-regulation by primary data collectors much less those operating on the more opaque derivative data market.

The aforementioned examples showcase the breadth with which consent gives each company the ability to collect and store information. More profound, each highlights the lack of clarity about with which entities such information might be shared or for how long a user's primary or derivative data might exist. In this paradigm, the amount of data transmitted by users is increasing along with the ability of companies to monetize data collection for purposes extending far beyond the service provided. Transmitted data is not only valuable for

231. Kashmir Hill, *Verizon Very Excited That It Can Track Everything Phone Users Do and Sell That to Whoever Is Interested*, FORBES (Oct. 17, 2012, 1:46 PM), http://www.forbes.com/sites/kashmirhill/2012/10/17/verizon-very-excited-that-it-can-track-everything-phone-users-do-and-sell-that-to-whoever-is-interested/.

232. *How Our Privacy Policy Affects You*, VERIZON WIRELESS (Oct. 19, 2012), http://www.verizonwireless.com/news/2012/10/verizon-wireless-privacy-policy.html.

233. Verizon was recently fined by the FCC for its failure to provide its wired-telephone customers with information about their ability to opt-out of Verizon's use of their personal information to market Verizon products to them. *See* Brian Fung, *Verizon Failed to Tell 2 Million People It Was Using Their Personal Info for Marketing. Now the FCC Is Making It Pay*, WASH. POST (Sept. 3, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/03/Verizon-failed-to-tell-2-million-people-it-was-using-their-personal-info-for-marketing-now-the-fcc-is-making-it-pay/?tid=HP_business.

234. Julia Angwin & Jennifer Valentino-Devries, *Google's iPhone Tracking, Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*, WALL ST. J. (Feb. 17, 2012), http://www.wsj.com/articles/SB10001424052970204880404577225380456599176; Matthew Sparkes, *High Court: 'Google Privacy Case Can Be Heard In UK'*, TELEGRAPH (Jan. 16, 2014), http://www.telegraph.co.uk/technology/google/10576284/High-Court-Google-privacy-case-can-be-heard-in-UK.html.

235. Gitte Laasby, *Wisconsin to Share in $17 Million Settlement With Google Over Privacy*, JOURNAL SENTINEL (Nov. 18, 2013), http://www.jsonline.com/watchdog/pi/google-to-pay-17-million-for-circumventing-safari-privacy-settings-b99144911z1-232370171.html.

purchasing habits and preference insights, but such data may also reveal a user's thoughts, ideas, and innovations. Applying big data analytics to the right type of information may effectively allow for the crowdsourcing of intellectual property creation and ideation by those who acquire the data.

But is there true consumer awareness over the combination of data from different sources? Is the sum of the parts, for instance, a robust marketing profile, greater than the whole, a common Internet browsing experience? Likewise, to what extent are the future uses of data being anticipated and should there be an expiration date on data retention? Most terms of service agreements do little in addressing potential data use problems. Perhaps more importantly, the development of sophisticated algorithms able to manipulate an increasingly vast amount of data points means that data once anonymized could be personally identifiable again.[236] In other words, data that is not identifiable today might be combined with data in the future that will erase the utility of current privacy safeguards.

The same software and hardware that enrich users' lives might limit them. One externality of the adaptive nature of the current data-enlightened, algorithmic Internet involves the scope and quality of user experiences. Consumers contribute information as they seek content, which in turn provides the data with which companies such as Facebook craft and shape their content.[237] At a certain point, users are narrowing their own online experience because of this paradoxical big data loop by which algorithmic behaviors change as a result of past user input (e.g. Facebook's newsfeed).[238]

As noted in its policies, Google, and similar web giants, uses web beacons (also known, among other things as "web bugs") on affiliate websites to track users.[239] Consequently, a website running an ad from

236. For a thorough exploration of this topic, see Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010), http://uclalawreview.org/pdf/57-6-3.pdf; *see also* EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 8 (2014), http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

237. Anthony Wing Kosner, *Facebook Is Recycling Your Likes To Promote Stories You've Never Seen To All Your Friends*, FORBES (Jan. 1, 2013, 7:19 PM), http://www.forbes.com/sites/kashmirhill/2013/01/22/how-to-keep-facebook-from-promoting-2-girls-1-cup-to-your-family-and-friends-under-your-name/.

238. David Auerbach, *The Big Data Paradox*, SLATE (Aug. 7, 2014, 12:00 PM), http://www.slate.com/articles/technology/bitwise/2014/08/what_is_big_data_good_for_incremental_change_not_big_paradigm_shifts.html?utm_medium=referral&utm_source=pulsenews.

239. JOSHUA GOMEZ ET AL., UC BERKELEY SCHOOL OF INFORMATION, KNOWPRIVACY REPORT 8 (2009), http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf.

Google's affiliate network transmits data back to Google about site visitors, many of whom could likely also directly use Google products. This provides quality insight into advertising-investment returns for Google but would potentially unnerve a web user who did not expect their use of non-Google services to be correlated with their Gmail use.

Users have little control over what type of data eventually ends up in ever-growing datasets. For the most part, users traditionally do not possess statutory rights under which to sue providers for selling their data unless the information is covered by a sector-specific federal regulation or state law. Instead, a user must depend upon a breach of contract suit to argue that the terms to which they consented were violated or that no consent was given in the first place. Legal rights conferred by popular terms of service agreements are narrow and non-negotiable for consumers, thereby providing an extraordinary amount of power to the provider to collect and share data.

V. DISCUSSION AND POLICY PROPOSALS

User *consent* to terms of use might not match user *intent* to further share information. While the new European right-to-be-forgotten concept is debated and interpreted,[240] the U.S. data marketplace continues to thrive without heavy oversight. Many aspects of American consumers' interactions with the Internet lack statutory control or administrative regulation. Instead, online practices are governed by numerous terms of service agreements based on the notion of click-through consent. After initial consent, the sharing of collected data with third parties often leaves data beyond the control of the very consumer who supplied it. This makes it difficult for an Internet user to future-proof and ultimately protect the use of their data from unwanted purposes down the road.[241] Such a paradigm differs from the European

240. This debate is now sometimes called "the right to be delisted" to reflect the central dispute regarding an EU citizen's effort to remove certain webpages bearing his name from Google's results. The real life event central to this man's plight is perhaps a prescient warning of debates to come over the right to remove contextualized metadata and evidence of digital activities. Perhaps the right to remove one's own name from search engine result lists is less significant than the right to remove one's data from unknown data brokers. Julia Powles & Enrique Chaparro, *How Google Determined Our Right to Be Forgotten*, GUARDIAN (Feb. 18, 2015), http://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search.

241. This can be particularly troublesome in a variety of existing data uses and those unfathomable today. For example, online data can be factored into determining a consumer's creditworthiness, an area that greatly affects lives but one in which consumers are disincentivized from accessing information too often for fear of flagging their own credit reports. In some cases

approach to data privacy in which data controllers are required to provide "subjects with unambiguous notice of what information is being collected, why it is gathered, and who will be able to access it".[242]

Data aggregation and anonymization are frequently touted as solutions to ease the friction created by the desire to utilize data for monetary gain and the often-competing value of protecting user privacy.[243] However, the more that data is anonymized, the less useful it becomes to marketers, which renders it far less valuable overall.[244] Data tells the stories of individuals and groups as well as the relationships they form with each other.[245] The parties that ultimately control much of the data generated through the layers of the Internet, data brokers, have been accused of "operating under a veil of secrecy" because of their lack of direct interaction with consumers.[246] A user might not remember a movie they liked five years ago, but Acxiom by virtue of data collected from a publicly-facing website such as Facebook potentially could. Accordingly, there are calls to prevent the indefinite retention of user data,[247] and the FTC has called on Congress to regulate data brokers.[248]

The FTC remains engaged in the topic of digital privacy, focusing on emerging consumer trends. Specific to mobile technology, the FTC

---

users might be incentivized to share under one content presentation regime but would have been less forthcoming if they knew how accessible, prominent, or correlated the same data would be years later. *See* Meghan Kelly, *Do This Now, Before Facebook's Graph Search Embarrasses You*, VENTUREBEAT (Jan. 16, 2013, 3:41 PM), http://venturebeat.com/2013/01/16/facebook-graph-search-privacy/.

242. Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433, 465 (2014).

243. Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, *supra* note 236, at 1708–10 (2010).

244. *Id.*

245. Seth Grimes, *Metadata, Connection and the Big Data Story*, HUFFINGTON POST (Apr. 28, 2014, 5:59 AM EDT), http://www.huffingtonpost.com/seth-grimes/metadata-connection-and-t_b_5225861.html?.

246. OFFICE OF OVERSIGHT AND INVESTIGATIONS MAJORITY STAFF, U.S. SENATE COMM. ON COMMERCE, SCIENCE & TRANSP., A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES 3 (Dec. 18, 2013), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577.

247. Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433, 434–35 (2014).

248. FED. TRADE COMM'N, DATA BROKERS: CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

proposed privacy principles by which companies should disclose more thorough information as to what is being collected and shared.[249] In its Mobile Privacy Disclosures, the FTC suggested that all players in the mobile ecosystem play a role in increasing privacy protections.[250] For example, the report recommended that mobile operating system providers offer built-in privacy warnings and safeguards, including "just-in-time disclosures to consumers" that would require their express consent before data is transferred.[251] This idea, if implemented, could perhaps enrich rather than disrupt the current notice and consent paradigm by increasing transparency.

Recently, the White House commissioned a study on the privacy implications of big data.[252] The resulting report proposed preset digital privacy profiles as one possible successor to the current notice and consent regime.[253] The proposal conceptualized an option through which consumers could choose from a fixed menu of privacy options for their online consumption that would be adhered to by companies within the digital ecosystem.[254] For example, one profile might offer the best consumer value but share more data whereas an alternative profile could promise much more privacy.[255] Such a solution would require voluntary or legally mandated coordination between online providers, advertisers, and data brokers. Ultimately, this idea acknowledges today's reality that online privacy is often treated as a commercial luxury rather than an absolute right.[256]

---

249. FED. TRADE COMM'N STAFF, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

250. *Id.* at 6.

251. *Id.* at ii.

252. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., EXEC. OFFICE OF THE PRESIDENT, REPORT ON BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 40 (2014), http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [hereinafter BIG DATA AND PRIVACY RPT.] (Section 4.5.1, "A Successor to Notice and Consent, Big Data and Privacy: A Technological Perspective").

253. *Id.* at 40–41.

254. *Id.*

255. *Id.*

256. For example, AT&T has proposed charging their high-speed ISP customers extra money to not analyze their Internet traffic via deep-packet inspection. *See* Jon Brodkin, *AT&T's Plan To Watch Your Web Browsing—And What You Can Do About It*, ARS TECHNICA (Mar. 27, 2015), http://arstechnica.com/information-technology/2015/03/atts-plan-to-watch-your-web-browsing-and-what-you-can-do-about-it/.

Another way forward might be to couple upfront transparency requirements with routine reporting regarding data sharing and data use. Although in the context of the network neutrality debate that addresses to what degree ISPs may control traffic on their network,[257] transparency rules already require wireless and fixed broadband Internet access providers like Verizon to disclose network management practices and quality of service measures to consumers[258] and may be expanded to address consumer privacy concerns.[259] Beyond ISPs and network neutrality, transparency efforts could conceivably include the layers of the Internet represented by the likes of Google and Facebook. Whether performed as a holistic analysis of provider-data use or, when technically feasible, as an analysis tailored toward individual user accounts, providers may better inform users as to the different ways in which data has been collected and used in practice and with which specific entities it has been shared for a given time period. This disclosure, linked to term-based, renewable notice and consent agreements could allow users to give truly informed consent on an

257. There is a great deal of scholarship addressing network neutrality. *See*, *e.g.*, Jan Krämer et al., *Net Neutrality: A Progress Report*, 37 TELECOMM. POL'Y 794 (2013); Tim Wu, Network Neutrality, *Broadband Discrimination*, 2 J. ON TELECOMM. & HIGH TECH. L. 141 (2003); Christopher S. Yoo, *Beyond Network Neutrality*, 19 HARV. J.L. & TECH. 2 (2005); Tim Wu & Christopher Yoo, *Keeping the Internet Neutral?: Tim Wu and Christopher Yoo Debate*, 59 FED. COMM. L.J. 575 (2007); Rob Frieden, *Network Neutrality or Bias-Handicapping the Odds for a Tiered and Branded Internet*, 29 HASTINGS COMM. & ENT. L.J. 171 (2006).

258. *See* Preserving the Open Internet: Broadband Industry Practices, GN Docket No. 14-28, 25 FCC Rcd. 17,905 (2010) (Report & Order). All broadband providers "shall publicly disclose accurate information regarding network management practices, performance and commercial terms of [their] broadband Internet access services sufficient for consumers to make informed choices regarding the use of such service and for content, application, service and device providers to develop, market and maintain their Internet offerings." *Id.* The FCC recently enhanced its transparency requirements. *See* Protecting and Promoting the Open Internet, GN Docket No. 14-28, FCC No. 15-24, at ¶24 (Report and Order on Remand, Declaratory Ruling and Order, released March 12, 2015) [hereinafter *2015 Open Internet Order*].

259. The FCC classified broadband Internet access service as a telecommunications service, thus falling under Title II common carrier regulations. *See 2015 Open Internet Order*, *supra* note 258, at ¶¶ 47–49; The FCC refrained from applying its current customer proprietary network information (CPNI) rules that address telephone call privacy to broadband Internet-access providers. *Id.* at ¶¶ 462–68. However the FCC did acknowledge the importance of privacy concerns recognizing broadband ISPs are "necessary conduit for information passing between an Internet user and Internet sites or other Internet users, and are in a position to obtain vast amounts or personal and proprietary information about their customers." *Id.* at ¶ 463. The FCC plans to hold a workshop to explore issues concerning broadband consumer privacy as a result of its 2015 Open Internet Order. *See* Press Release, Fed. Commc'n Comm'n, The Wireline Competition and Consumer & Governmental Affairs Bureaus Schedule Public Workshop on Broadband Consumer Privacy (rel. Mar. 30, 2015), http://www.fcc.gov/document/wcb-and-cgb-public-workshop-broadband-consumer-privacy.

annual, biannual, or other regularly occurring basis and require reaffirmation when terms of service change.[260] Nevertheless, issues still arise with consumer challenges in reading and understanding terms of service agreements.[261] Ideally any broadband-transparency effort should disclose all the information necessary for consumers to make an informed decision, which should be easy to access, written with clarity and simplicity, and verifiable.[262]

Without specific regulatory or legislative mandates, implementing any of these ideas to better contain, control, and inform the use of consumer data depends upon increased corporate responsibility. Self-regulatory schemes such as the "Do Not Track" standards subscribed to by Internet content providers have achieved only limited success in improving consumer control over the collection and use of collected data.[263] This stems in part from the lack of comprehensive voluntary standards that consistently follow data use throughout the Internet ecosystem and from a lack of knowledge on the part of consumers.[264] These problems will only exacerbate as other concerns such as those related to cybersecurity increase with regard to safeguarding primary and derivative data. Consequently, corporate responsibility is vital to guaranteeing that data is treated as agreed upon not only by the primary entity that gathers and shares the data but also by all who receive and process the data thereafter.

For the longer term, the White House has recommended, amongst other things, that school children should be taught digital literacy to better understand the realities of their digital presence as they go through life.[265] This could foster a more nuanced understanding of the risks posed by online interactions and empower decision making if

260. Increased transparency and opportunities for a user to be reminded of how their data is being shared might increase competition in layers of the Internet. This could incentivize providers to showcase the ways that they protect, control, and use the data of their users responsibly while giving users access to a new factor to consider when choosing an online-service provider.

261. See Solove, *supra* note 73.

262. *See* Gerald R. Faulhaber, *Transparency and Broadband Internet Service Providers*, 4 INT'L J. OF COMM. 742 (2010).

263. Jamie Campbell, *Microsoft Turns Off 'Do Not Track' As Default Internet Explorer Setting*, INDEPENDENT (Apr. 6, 2015), http://www.independent.co.uk/life-style/gadgets-and-tech/microsoft-turns-removes-do-not-track-as-default-internet-explorer-setting-10157749.html.

264. Elise Ackerman, *Google And Facebook Ignore "Do Not Track" Requests, Claim They Confuse Consumers*, FORBES (Feb. 27, 2013, 7:58 PM), http://www.forbes.com/sites/eliseackerman/2013/02/27/big-internet-companies-struggle-over-proper-response-to-consumers-do-not-track-requests/.

265. BIG DATA AND PRIVACY RPT., *supra* note 252, at 59.

future consumers have access to more information about their data. The degree to which data use is made transparent will likely depend on whether such mandates are legislative, such as President Obama's proposed Consumer Privacy Bill of Rights,[266] regulatory, from a more aggressive FTC or possibly FCC (in the context of ISPs),[267] or voluntary, influenced by market pressure from consumers concerned about the mysterious ways in which they lose control of increasingly personalized and dynamic data.

CONCLUSION

Just one click agreeing to terms of service can lead to a slippery slope of consent. There is a funnel of rights by which service providers must confer certain degrees of choice onto users. At present, users do not have many rights beyond those afforded to them by their online service providers in the data use or privacy policies. Recent cases show that users must know that they are consenting to terms, cannot be misled about the use of their data, and are protected from the sharing of their data outside the normal course of business. Nonetheless, a data use or privacy policy that does not mislead consumers generally will be enforceable even if it lacks transparency regarding the specific ways in which consumer data will be used, shared or the duration for which it will exist.

The Internet will continue to be a multi-layered experience, growing more dynamic and increasingly invisible to users with the budding Internet of Things. Moreover, the context derived from troves of interwoven metadata will remain powerful whether or not paired with relevant user-generated content. However, data flows need not

266. Grant Gross, *Obama Calls for Data Breach Notification Law, Privacy Bill of Rights*, COMPUTERWORLD (Jan. 12, 2015, 11:08 AM PT), http://www.computerworld.com/article/2867839/obama-calls-for-data-breach-notification-law-privacy-bill-of-rights.html. For a discussion draft of the Consumer Privacy Bill of Rights, see *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015*, THE WHITE HOUSE, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (last visited Apr. 18, 2015). Section 101 of the draft legislation suggests greater transparency where by individuals are given "concise and easily understandable language, accurate, clear, timely and conspicuous notice." *Id.* at 6. The notice must contain, among other provisions, what data is processed, methods and purposes of collection, disclosure of collected data, retaining of data, methods of user access to data as well as security measures to protect data. *Id.* at 6–7.

267. As a result of the FCC's network-neutrality regulations and use of common-carrier classification, the FCC is claiming jurisdiction over ISPs to ensure they protect their customer's privacy even though the FTC typically addresses consumer protection and online privacy. *See* Brendan Sasso, *Net Neutrality Has Sparked an Interagency Squabble Over Internet Privacy*, NAT'L JOURNAL (Mar. 9, 2015), http://www.nationaljournal.com/tech/the-future-of-broadband/net-neutrality-has-sparked-an-interagency-squabble-over-internet-privacy-20150309.

remain opaque. So long as the notice and consent regime remains the backbone of lucrative data markets, steps should be taken to increase transparency and therefore ensure that consumers are genuinely on notice and provide truly informed consent to each party's use of their data.

Online privacy is a shared responsibility that can be better achieved through technical controls and warnings that go hand-in-hand with transparent policy disclosures that provide more thorough and accurate information. This will help nurture digital literacy at a time when digital footprints are everywhere and can last in virtual perpetuity. Moreover, transparency requirements imposed on providers can enhance consumer awareness of how their data will be used and specify exactly which other parties will utilize and further share potentially personal and valuable information.