3-1-2017

It Depends: Recasting Internet Clickwrap, Browsewrap, "I Agree," and Click-Through Privacy Clauses as Waivers of Adhesion

Charles E. MacLean
Indiana Tech Law School

IT DEPENDS: RECASTING INTERNET CLICKWRAP, BROWSEWRAP, "I AGREE," AND CLICK-THROUGH PRIVACY CLAUSES AS WAIVERS OF ADHESION

CHARLES E. MACLEAN*

ABSTRACT

Digital giants, enabled by America's courts, Congress, and the Federal Trade Commission, devise click-through, clickwrap, browsewrap, "I Agree" waivers, and other legal fictions that purport to evidence user "consent" to consumer privacy erosions. It is no longer enough to justify privacy invasions as technologically inevitable or as essential to the American economy. As forced consent is no consent at all, privacy policies must advance with the technology. This article discusses adhesion waivers, the potential for FTC corrective action, and a comparison to privacy policies of the European Union.

CONTENTS

I. INTRODUCTION

Enter the following query into Google: adult diapers. Then watch the computer screen as pop-up advertisements simultaneously appear for multiple brands of adult diapers, including Tena, Tranquility, Prevail, and, of course, Depends. Google instantaneously sold your consumer data to marketers eager to make a buck.[1] Deep

* Associate Dean of Faculty and Associate Professor of Law, Indiana Tech Law School; J.D. (William Mitchell College of Law); M.B.A. (University of Minnesota). The author extends special thanks to the coordinators of the Cleveland State Law Review Symposium: Regulating Big Data in the Digital Age, April 8, 2016, for which these materials were initially prepared. The author also recognizes the research and conceptual assistance of Youngwoo Ban, Research Librarian and Assistant Professor of Law at Indiana Tech Law School.

[1] Months after entering this query, the author continues to receive regular advertisements for adult diapers; that should come as no surprise because fully 90% of Google's 2015 revenues are derived from advertisements. Google, Inc., Annual Report (Form 10-K), 1, 15

in the bowels of Google's privacy waiver documents, every Google user is deemed to have "consented" to these consumer data privacy erosions.[2] Big data, marketers, resellers, and Internet service providers digitally track consumers, such as those in the diaper example, not only because they can, but also because there is money to be made doing it. The problem becomes compounded when those digital giants, enabled by America's courts, Congress, and the Federal Trade Commission, devise click-through, clickwrap, browsewrap, "I Agree" waivers, and other legal fictions that purport to evidence user "consent" to these consumer privacy erosions.

Imagine a customer, upon entering a brick-and-mortar retail store, is approached by a clerk and told, "I will let you look around our store and even buy an item or two. However, this access only comes if you agree to disclose to us every website you visit for the next several years along with your physical locations in real time, your friends' identities and photographs, and all online purchases you make during that same time period. Further, you must let me sell all that information about you to whomever I wish for any purpose at all." Any reasonable customer would turn around and walk right out of that store. Yet, in the Internet era, virtually all online marketers gather exactly that data and much more from all visitors and customers of their online "stores."[3] We have allowed marketers empowered with the latest computer gadgetry to victimize both our privacy and us. As President Barack Obama's White House noted when it proposed a Consumer Privacy Bill of Rights in 2012, "it is incumbent on us to do what we have done throughout history: apply our timeless privacy values to the new technologies and circumstances of our times."[4]

Nonetheless, all branches of our federal government have enabled this privacy erosion. The government's justification for such large-scale collection and dissemination of private consumer data is largely ex post rationalization. The theory goes that allowing marketers to track all of this private consumer data has the allegedly salutary benefit of allowing those marketers to better target their advertisements to users who are likely to be genuinely interested in the advertised products. This is why once a user engages in online cost comparisons for baby strollers, the user is thereafter inundated with pop-up ads from one vendor after another with advertisements for strollers and other baby-related items. But is the modest shopping convenience really worth the cost of all that privacy erosion? Are

---

(Feb. 11, 2016) https://www.sec.gov/Archives/edgar/data/1288776/000165204416000012/goog10-k2015.htm.

[2] *Privacy & Terms*, GOOGLE, https://static.googleusercontent.com/media/www.google.com/en//intl/en/policies/privacy/google_privacy_policy_en.pdf (last updated Aug. 29, 2016). Google's privacy and terms of service documents exceed 12,000 words, not including Google's Product Privacy Guide that boasts thirty-seven separate constituent documents. *Id.* I venture to say that no one, other than Google's corps of attorneys, has read and understood that entire consumer privacy library.

[3] *Online Tracking More Common Than Most Realize: A Survey of 1 Million Top Websites Finds that 88 Percent Share User Data with Third Parties*, SCIENCEDAILY (Nov. 10, 2015), www.sciencedaily.com/releases/2015/11/151110093923.htm.

[4] Danny Weitzner, *We Can't Wait: Obama Administration Calls for a Consumer Privacy Bill of Rights for the Digital Age*, WHITEHOUSE.GOV (Feb. 23, 2012, 4:00 PM), https://www.whitehouse.gov/blog/2012/02/23/we-can-t-wait-obama-administration-calls-consumer-privacy-bill-rights-digital-age.

American consumers and their elected representatives willing to wade into the Internet and take back their consumer privacy rights? Where does this data reside? In which countries? On which servers? Who has access? Who controls and protects the data?

The digital age has ushered in an age of privacy erosion unparalleled in history. Perhaps the closest analog occurred in the nineteenth century when photography and the growth of newspapers combined to put on the front page what once was hidden in the parlor. Louis Brandeis wrote in 1890 about this last era of privacy erosion.[5] En route to recommending broad adoption of a right to privacy, later-Justice Brandeis and his co-author presaged the digital age:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right "to be left alone." . . . The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others [and each individual] generally retains the power to fix the limits of publicity which shall be given them. . . . The common law has always recognized a man's house as his castle, impregnable, often, even to its own officers engaged in the execution of its commands. Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?[6]

Similarly, in the digital age, when private consumer data—through the wide-open "back door"—is so freely captured, used, resold, reused, aggregated, and more, for profit alone and largely without the knowing and voluntary consent of the consumer subject of the data, our right to privacy has been eroded almost beyond repair.

Consider even a single provider, Verizon Wireless, that provides telephone and wireless Internet access to its users. There is a wide swath of personal information that Verizon users share with the company each day: telephone numbers called, duration of those calls, moment-by-moment geo-location from cell tower triangulation, websites and webpages visited, contact information, email correspondence and all attachments, search queries, usernames, passwords, dates of birth, Social Security numbers, banking records and transactions, the contents of text messages, purchases, browsing details, credit card numbers, addresses, friends, photographs, videos, and so on.[7] Now imagine that the user, probably without any conscious awareness, is magically deemed to have consented to the sharing and release of that data to third parties when the user simply clicked the "I Agree" button months or years before. One cannot deny the ease and convenience of technology, but must we sacrifice so much privacy en route?

It is no longer enough to justify privacy invasions as technologically inevitable or as essential to the American economy. Congress must step in to legislate a path to

---

[5] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195-220 (1890).

[6] *Id.*

[7] *Privacy Policy,* VERIZON, http://www.verizon.com/about/privacy/full-privacy-policy (last updated May 2016).

renewed consumer privacy and enable agencies and courts to enforce the path. It is no longer acceptable to disingenuously claim that click-through, clickwrap, browsewrap, "I Agree" waivers, and other legal fictions amount to real, knowing, voluntary consent. Instead, these legal fictions are waivers of adhesion: the price consumers are forced to pay for access to the Internet. Opaque privacy waivers that consumers merely click through without understanding are no substitute for real and substantive consumer privacy protections in the digital age. Forced consent is not consent at all.

II. THE MISCHIEF WROUGHT BY CONTRACTS OF ADHESION

Contracts of adhesion are form contracts, drafted and controlled in all respects by the party in the vastly superior bargaining position, that leave to the weaker contracting party only two options: (1) adhere to the terms as drafted by the party with superior power, or (2) reject its terms entirely.[8] With contracts of adhesion, there is, by definition, no negotiation option; it is strictly take-it-or-leave-it.[9]

Of course, contracts of adhesion are not automatically unenforceable. Rather, in most jurisdictions, there is a two-part disjunctive test: (1) if the contract of adhesion or its terms fall outside of the reasonable expectations of the weaker party, the contract will not be enforceable as against that weaker party;[10] or (2) even if the contract of adhesion or its terms falls within the reasonable expectations of the weaker party, the contract will not be enforceable if its terms are unconscionable or unduly oppressive.[11] Either is sufficient; the weaker party need not show both.

III. INTERNET CLICKWRAP CLAUSES AS CONTRACTS—AND WAIVERS OF ADHESION

In a contract of adhesion, the weaker party, who is powerless against the stronger party who drafted the contract and is unable to negotiate any modifications to the contract of adhesion, can only escape the contract's terms if the terms are not as expected or are otherwise unconscionable or unduly burdensome.[12] Consumers face this exact situation when in the midst of Internet shopping; the shopper must click the "I Agree" button to complete the purchase. This button is a clickwrap agreement.[13] The seller drafted the terms of the contract and all the implicit and explicit privacy waivers contained therein, and the consumer is powerless to offer or

---

[8] 1 MARTIN DOMKE ET AL., DOMKE ON COMMERCIAL ARBITRATION § 8:26 (2015).

[9] *Id.*; William Alan Nelson, *Take It or Leave It: Unconscionabillity of Mandatory Pre-Dispute Arbitration Agreements in the Securities Industry*, 17 U. PA. J. BUS. L. 573 (2015).

[10] Yasamine Hashemi, *Facebook's Privacy Policy and Its Third-Party Partnerships: Lucrativity and Liability*, 15 B.U. J. SCI. & TECH. L. 140, 157-58 (2009); *see generally* Zev J. Eigen, *The Devil in the Details: The Interrelationship Among Citizenship, Rule of Law and Form-Adhesive Contracts*, 41 CONN. L. REV. 381 (2008).

[11] RAYMOND T. NIMMER & JEFF C. DODD, MODERN LICENSING LAW § 12:13 (2016); RAYMOND T. NIMMER, LAW OF COMPUTER TECHNOLOGY § 6:65 (2015); *see also* U.C.C. § 2-302 (AM. LAW INST. & UNIF. LAW COMM'N 1977).

[12] NIMMER & DODD, *supra* note 11; NIMMER, *supra* note 11.

[13] Specht v. Netscape Comm. Corp., 306 F.3d 17, 21-22 n.4 (2d Cir. 2002); HOWARD O. HUNTER, MODERN LAW OF CONTRACTS § 19:48 (2016).

negotiate any substantive amendments to the waiver, which constitutes a contract. Furthermore, most consumers are completely unaware of the terms they are waiving; thus, those waiver terms fall outside of the reasonable expectations of the average consumer. The terms are uncontrollable, unconscionable, and oppressive when the collected data, metadata, cookies, keylogs, shopping histories, Internet search histories, URLs, emails, mothers' maiden names, credit card numbers, and the like are shared intentionally or inadvertently online with big data aggregators and data resellers that sell those formerly private consumer data to the highest bidders.[14]

The issues related to the forum, choice of law, arbitration, licensing, service, and liability terms of these Internet contracts of adhesion have been widely litigated in courts and discussed in the literature.[15] Typically, courts have upheld clickwrap agreements to those extents, particularly if the user had the easy ability to print its terms, had to affirmatively indicate assent (as by clicking "I Agree"), and had the option of rejecting the agreement in its entirety.[16] The privacy waiver features of these Internet clickwrap "agreements" have been far less frequently addressed. Although clickwrap agreements are clearly "waivers of adhesion," that phrase has never appeared in any appellate opinion or secondary source in American law.[17] As an early commentator noted,

> Click-wrap contracts are regularly formed on websites. When a purchase is made, the user is typically asked to agree to terms and conditions, and sites that allow user postings such as discussion forums and chat rooms usually require member agreements as a condition of registration. By incorporating the privacy policy into a click-wrap user agreement, or turning it into one, the website can potentially limit remedies and damages, exclude consequential damages, provide for notice of and a right to cure any breach, require mandatory dispute-resolution mechanisms such as a negotiation-mediation-arbitration sequence, specify governing law and forum, shorten the statute of limitations, extract representations from the user (e.g., as to nationality or age), provide for contingencies through a force majeure clause, and create clear evidence of binding consents or waivers.

---

[14] Timothy J. Van Hal, *Taming the Golden Goose: Private Companies, Consumer Geolocation Data, and the Need for a Class Action Regime for Privacy Protection*, 15 VAND. J. ENT. TECH. L. 713, 721-22 (2013).

[15] *See* Nathan J. Davis, Note, *Presumed Assent: The Judicial Acceptance of Clickwrap*, 22 BERKELEY TECH. L.J. 577, 589 (2007); *see also* Lucille M. Ponte, *Getting a Bad Rap? Unconscionability in Clickwrap Dispute Resolution Clauses and a Proposal for Improving the Quality of These Online Consumer "Products*," 26 OHIO ST. J. DISP. RESOL. 119, 120 (2011).

[16] *See, e.g.*, Centrifugal Force, Inc. v. Softnet Comm., Inc., No. 08 Civ. 5463(CM)(GWG), 2011 WL 744732, 2011 U.S. Dist. LEXIS 20536, at *7 (S.D.N.Y. Mar. 1, 2011).

[17] With a nod toward Professor Haynes's outstanding 2007 article, in which she noted, "Rather than providing consumers the protection they expect, *privacy policies have become one more online contract of adhesion* for consumers to avoid." Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN ST. L. REV. 587, 624 (2007) (emphasis added).

> Given the minimal money damages likely to result from any given privacy breach and the probability that most consumer complaints can be resolved with a sincere apology and a promise to do better (or to delete the information), it is fair to ask whether a contractual privacy policy is overkill. The two-word answer is: class actions.[18]

As discussed in the following section, inertia and perceived inevitability have brought us to this point.

IV. HOW DID WE GET HERE; WHY DO WE ALLOW THESE PRIVACY WAIVERS OF ADHESION?

Two predominant factors—both related to public perceptions of inevitability—have conspired to bring us to today's situation where online consumer privacy evaporates with a click: (1) inertia associated with the public's subjective belief that digital advancement must sacrifice individual privacy,[19] and (2) an inordinate and largely unsupported fear that even the slightest impediment to free online trade will inevitably, substantially, and adversely impact the U.S. economy.[20] Neither is inevitable.

Think of the police search and seizure analog. In the absence of regulation and oversight through the Fourth Amendment, law enforcement officers would seriatim use every new technological device to pierce suspects' privacy in search of evidence.[21] Similarly, online marketers and data aggregators will use every new technology and privacy-eroding tracking technique or privacy waiver unless Congress or the FTC[22] precludes its use. One can scarcely blame either group. There

---

[18] Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 J. INTELL. PROP. L. 57, 93 (1999).

[19] *See, e.g.*, Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 844 (2002); *see generally* Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 360 (2015); Sarah Elwood, *Privacy, Reconsidered: New Representations, Data Practices, and the Geoweb*, 42 GEOFORUM 6, 6 (2011).

[20] *See* MaryAnne M. Gobble, *Regulating Innovation in the New Economy*, 58 RES. TECH. MGMT. 62, 63 (2015); *see also* Maureen K. Ohlhausen, *The Internet of Things and the FTC: Does Innovation Require Intervention?*, Remarks Before the U.S. Chamber of Commerce 9 (Oct. 18, 2013), http://www.ftc.gov/speeches/ohlhausen/131008internet thingsremarks.pdf; Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598-99 (2014); Mozelle Thompson, *Keynote Address: The Federal Trade Commission and Regulating E-Commerce*, 16 ST. JOHN'S J. LEG. COMMENT. 609, 615 (2002); Isabell Koske et al., *The Internet Economy—Regulatory Challenges and Practices* (OECD Working Paper No. 1171, 2014).

[21] *See* Charles E. MacLean, *Katz on a Hot Tin Roof: The Reasonable Expectation of Privacy Doctrine is Rudderless in the Digital Age, Unless Congress Continually Resets the Privacy Bar*, 24 ALB. L.J. SCI. & TECH. 47, 50 (2014); *see also* Kyllo v. United States, 533 U.S. 27, 34-35 (2001) (holding evidence obtained through the use of a thermal-imaging device inadmissible because it was a type of technology that was not readily available to the public).

[22] *See, e.g.*, Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1, 1 (2009).

are crimes to be solved in the first instance, and there is money to be made in the second.[23] Nonetheless, in past instances of technology eroding privacy beyond our community privacy "threshold," Congress (and sometimes the courts[24]) has stepped in.[25] And of course, although our reasonable expectations of privacy can evaporate to near extinction as technology advances,[26] we can always reset the privacy bar by way of congressional enactment and appellate precedent. It is time we do exactly that in Internet privacy waivers of adhesion.

There is no longer any reason to entertain the flimsy and unsupportable legal fiction that by physically clicking the "I Agree" button, we have knowingly, voluntarily, or intelligently waived a thing. Rather, this is another example where technological advancements proceed as the hare while constitutional privacy jurisprudence and congressional and FTC intervention move at paces more akin to the tortoise.

The concerns here are far more expansive than simply a Luddite wish for a return to "the good old days." On the contrary, with Big Data and the big business of data aggregation and data sharing, consumers—in the henhouse—need to be protected by the FTC, Congress, and the courts; we cannot justify leaving the protection of consumers in their henhouses to the foxes who are collecting and profiting from the aggregation, sale, and resale of all this formerly private consumer data.[27]

Although the digital age seems mature in some senses, it is really in its infancy. Yet, consumer privacy in most aspects has already been compromised almost beyond repair.[28] On the Internet, that data resides in perpetuity only to be mixed and matched and aggregated into a data basket of information for sale to the highest bidder. Our medical records have been digitized and are vulnerable. Our Internet browsing history is vulnerable, too. Additionally, we have consumer ID cards we use at grocery stores, enabling them to track, store, and disseminate our shopping history.

And once a consumer has more-or-less willingly turned over to online marketers the keys to his or her privacy kingdom, along with credit card and bank account

---

[23] *See id.*

[24] *See* Katz v. United States, 389 U.S. 347, 259 (1967) (addressing the legality of an interception of a phone conversation in a public phone booth).

[25] *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511 et seq. (2016); Stored Communications Act of 1986, 18 U.S.C. § 2701 et seq. (2016).

[26] After all, in the digital age, can anyone credibly argue and reasonably believe that anything is truly private? Cell phones can be searched in seconds. The National Security Agency, enabled by FISA, seizes cellphone metadata. GPS tracking allows real-time tracking of anyone, anywhere. Smartphone apps basically require locational services and access to your contacts and photographs. Your Internet searches are tracked. Keyloggers, viruses, malware, cookies, bots, and crawlers mine previously private enclaves for personal data. Your cars have a blackbox that tracks speed and other operational data. The list goes on and will exponentially grow as the digital age plays out.

[27] *Cf.* GEORGE ORWELL, 1984 (Secker & Warburg 1949) (paralleling the current skepticism toward Big Data to "Big Brother").

[28] Richard van Hooijdonk, *In this Digital Age, Your Privacy is Continuously Invaded*, INST. ETHICS & EMERGING TECH. (Sept. 23, 2015), http://ieet.org/index.php/IEET/more/vanhooijdonk20150924.

numbers, social security numbers, and mothers' maiden names, the online marketers are just the first entities to possess these private data, but they are certainly not the last.[29] Many on-line marketers sell their caches of private consumer data to other marketers. Indeed, one can helpfully differentiate between first-party data gatherers, who have a direct relationship with the tracked user, and third-party data gatherers, who purchase consumer data from first-party gatherers and mine the Internet for dozens more data points about those same users. Users' private data, including health records, pregnancy status, HIV status, credit scores, assets, debts, and purchase and browsing history, are all readily available from third-party consumer data vendors. Perhaps more disturbing is that all the heretofore private data on consumers are susceptible to domestic and foreign hackers and other unintended dissemination and sharing of private facts about American consumers.[30]

For the moment, the immediate challenge is that American consumers believe, and act as if they believe, that they are powerless to stem the tide of personal consumer data collection by online marketers. As one 2015 study notes, "Americans believe it is futile to manage what companies can learn about them . . . [the majority] do not want to lose control over their information but also believe this loss of control has already happened."[31] In that study of American consumers:

> 49% incorrectly believed a supermarket must obtain the consumer's permission before selling information about the consumer's purchases to other companies;
>
> 69% inaccurately thought a pharmacy must have your permission before selling to others information about the over-the-counter products you have purchased;
>
> 65% falsely believed that if a company has a "privacy policy," that means the company will not share consumer data with others without consumer permission;
>
> 91% believed it is not fair for business to collect consumer data without their knowledge;
>
> 71% felt it was not fair for businesses that provide free in-store Wi-Fi to collect surfing and use data from consumers using the service;
>
> 64% wrongly believed that clearing cookies on a cell phone prevented marketers from tracking the user;

---

[29] Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES, June 16, 2012.

[30] Christopher Mims, *The Hacked Data Broker? Be Very Afraid*, WALL ST. J., Sept. 8, 2015.

[31] JOSEPH TUROW ET AL., THE TRADEOFF FALLACY: HOW MARKETERS ARE MISREPRESENTING AMERICAN CONSUMERS AND OPENING THEM UP TO EXPLOITATION 3 (Univ. of Pa., Annenberg Sch. for Commc'n 2015).

> 84% want to be empowered to control what data businesses collect from them on-line; but
>
> 65% report that they have come to accept that they have little control over what marketers can learn about on-line consumers; and
>
> only 18% of all Internet users have activated a "do not track" feature to prevent online marketers from tracking and logging their consumer information and activity.[32]

If one examines these results, it appears that those consumers who are more aware of the depth and breadth realities of on-line data collection by marketers are the most resigned to the inevitability of that data collection. The most informed have given up.

As the Wall Street Journal reported in 2010, "One of the fastest-growing businesses on the Internet . . . is the business of spying on Internet users."[33] And why not? It is, after all, big business indeed. Recent studies suggest that buying and selling otherwise private consumer data mined from the Internet will soon top $60 billion in annual revenue in the U.S. alone.[34] We ought not to blame the Internet marketers, first-party data gatherers, third-party data aggregators, and those who purchase consumer data from them. They are just following a free market model; they are simply entering a profitable market. In reality, the regulators and legislators are the ones at fault and, therefore, the ones who hold the keys to the solutions. For example, the Federal Trade Commission ("FTC") is the federal agency most broadly charged with consumer protection, and the agency talks a good game ("In today's world . . . companies are collecting, storing, and sharing more information about consumers than ever before . . . they should not do so at the expense of consumer privacy"[35]) and has some solid policy stances (such as, "[t]he Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security legislation"[36]). Nevertheless, the FTC has largely served as the chief apologist and enabler of data privacy erosion, focusing on industry self-regulation rather than on top-down legislated limits on consumer data privacy erosion.[37]

---

[32] *Id.* at 4, 12-16.

[33] Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 30, 2010.

[34] Nathan Newman, *How Big Data Enables Economic Harm to Consumers, Especially to Low-Income and Other Vulnerable Sectors of the Population,* https://www.ftc.gov/system/files/documents/public_comments/2014/08/00015-92370.pdf (last visited Aug. 29, 2016).

[35] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESS AND POLICYMAKERS i (Mar. 2012).

[36] *Id.*

[37] FED. TRADE COMM'N STAFF REPORT, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (2015).

Even the FTC's data privacy enforcement actions have been largely ineffective.[38] When the FTC compelled Google and Facebook to more clearly disclose to consumers the private consumer data they were capturing and selling to others,[39] the result was not more consumer protection, but merely more dense and indecipherable privacy disclosures that most users simply click through without reading—and

[38] There have been a few notable exceptions, such as the 2012 FTC agreement with Facebook (*In re* Facebook, Inc., No. C-4365, Decision & Order (July 27, 2012)), which was based on these FTC findings:

> • In December 2009, Facebook changed its website so certain information that users may have designated as private—such as their Friends List—was made public. They did not warn users that this change was coming, or get their approval in advance.
>
> • Facebook represented that third-party apps that users' installed would have access only to user information that they needed to operate. In fact, the apps could access nearly all of users' personal data—data the apps didn't need.
>
> • Facebook told users they could restrict sharing of data to limited audiences—for example with "Friends Only." In fact, selecting "Friends Only" did not prevent their information from being shared with third-party applications their friends used.
>
> • Facebook had a "Verified Apps" program & claimed it certified the security of participating apps. It didn't.
>
> • Facebook promised users that it would not share their personal information with advertisers. It did.
>
> • Facebook claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible. But Facebook allowed access to the content, even after users had deactivated or deleted their accounts.
>
> • Facebook claimed that it complied with the U.S.-EU Safe Harbor Framework that governs data transfer between the U.S. and the European Union. It didn't.
>
> The proposed settlement bars Facebook from making any further deceptive privacy claims.

Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers By Failing to Keep Privacy Promises (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

[39] Cameron Scott, *Less than Half of Facebook, Google Users Understand Sites' Privacy Policies*, COMPUTERWORLD (May 4, 2012), http://www.computerworld.com/article/2503822/data-privacy/less-than-half-of-facebook--google-users-understand-sites--privacy-policies.html.

certainly without understanding. Therefore, the consumers do not truly consent to the data privacy erosion.

To compound the problem, all of the consumer data privacy erosion is largely irreparable and likely irreversible. That is to say that consumer data that has already been digitally disclosed, stored, and aggregated is irretrievable, but these past privacy breaches do not free us from the obligation to prevent future data privacy erosions. Once data resides on the Internet, it is very difficult or impossible to erase. Firms routinely take snapshots of the Internet that yield the cached webpages that turn up on your browser searches.[40] Immense amounts of these data can be stored in a very small physical space and thus are easily transported, shared, and stolen.[41] Hackers have successfully targeted data stored in banks, hospitals, stores, and even government computers. According to one source, the Pentagon and the National Security Agency each repelled approximately ten million attempted cyber-intrusions per day in 2014![42] An estimated one million new malware threats were unleashed each day of 2014 alone.[43] In 2014, private data concerning 110 million consumers was stolen from Target, another 83 million from J.P. Morgan Chase, and 56 million from Home Depot.[44] The consumer data stolen from Target earned the cyber-thieves at least $53.7 million on the black market and cost Target at least $148 million.[45] The resultant downstream consequences in cybercrime, identity theft, and even extortion based on stolen consumer data are skyrocketing.[46]

V. THE FEDERAL COMMUNICATIONS COMMISSION IS TAKING A STAND WHERE IT HAS JURISDICTION

The FTC mainly has taken a rather *laissez-faire* approach to consumer data privacy erosions, leaving it to the data gathering and marketing industries to determine the state-of-the-art and best practices in data protections.[47] Thus, in spite

---

[40] *See* Bernard J. Jansen et al., *Real Life, Real Users, and Real Needs: A Study and Analysis of User Queries on the Web,* 36 INFO. PROCESSING & MGMT. 207, 207 (2000) (reporting the results of a research project that analyzed 51,473 web queries that internet users submitted into a popular web search engine)

[41] Martin Hilbert & Priscila López, *The World's Technological Capacity to Store, Communicate, and Compute Information*, SCIENCE (Apr. 1, 2011), http://science.sciencemag.org/content/332/6025/60.full; Sharon Tobias, *The Year in Cyberattacks*, NEWSWEEK, Dec. 31, 2014.

[42] *U.S. Hit with More Than 5,000 Attacks Every Hour,* NETSTANDARD, July 7, 2014; Paul W. Tinker, For the Common Defense of Cyberspace: Implications of a US Cyber Militia on Department of Defense Cyber Operations (Dec. 6, 2015) (unpublished M.M.A.S thesis, US Army Command and General Staff College) (on file with U.S. Army Command and General Staff College).

[43] Virginia Harrison & Jose Pagliery, *Nearly 1 Million New Malware Threats Released Every Day*, CNNMONEY, Apr. 14, 2015.

[44] Tobias, *supra* note 41.

[45] *Id.*

[46] *Id.*

[47] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 586 (2014).

of some more recent improvements in agency interventions,[48] the FTC has been a meek overseer. Another federal watchdog agency, the Federal Communications Commission ("FCC"), which has oversight and enforcement authority far in excess of the FTC in many respects, particularly with respect to telecommunications, appears to be moving in a better direction.[49] One clear FCC privacy protection path involves passage of its proposed Broadband Internet Access Service ("BIAS") provider regulations,[50] which would overhaul regulation of Internet service provider privacy approaches and reset the privacy bar. The notice and comment period continues as this article is in the publication process.

In March 2016, the FCC entered into a Consent Order[51] with Verizon, fined Verizon $1.35 million, and compelled the company to stop using "supercookies" to track users and target advertising without consumer consent unless each consumer had opted in.[52] As the FCC Enforcement Bureau Chief noted, "Consumers care about privacy and should have a say in how their personal information is used, especially when it comes to who knows what they're doing online…privacy and innovation are not incompatible."[53]

In addition to the FCC's isolated pursuit of Verizon, the agency has made additional attempts to reign in phone companies' management of consumer data. In July 2015, the FCC entered into a Consent Decree[54] with two phone companies, TerraCom and YourTel America, exacting a fine of $3.5 million (joint and several) for storing, without any encryption or other robust security systems, consumer data,

---

[48] *Id.* at 673-76 (acknowledging recent acceleration of FTC regulatory attempts in the consumer data privacy sphere while euphemistically labelling the FTC hands-off approach as "nudging . . . bottom up . . . a series of small steps . . . self-regulation").

[49] Press Release, A.G. Schneiderman Urges FCC to Protect Consumer Privacy as Commission Weighs Greater Restrictions on Use of Personal Information by Broadband Internet Access Providers (June 30, 2016), http://www.ag.ny.gov/press-release/ag-schneiderman-urges-fcc-protect-consumer-privacy-commission-weighs-greater.

[50] FCC, *In re Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* Notice of Proposed Rulemaking, No. 16-106 (Apr. 1, 2016), https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1_Rcd.pdf ("[W]ell-functioning commercial marketplaces rest on informed consent. Permission is required before purchasers can be said to agree to buy a product; permission is needed before owners of property transfer their interests in that property.") Thus, it is reasonable to assume, and unreasonable to deny, that our internet-based economy can continue to be well-functioning even if a more robust consent process were interposed, such as opt-in rather than opt-out, and gradations of privacy rather than all-or nothing.

[51] *In re* Cellco Partnership, d/b/a Verizon Wireless, 31 FCC Rcd. 1843 (2016).

[52] Cecilia Kang, *Verizon Settles with F.C.C. Over Hidden Tracking via 'Supercookies,'* N.Y. TIMES, Mar. 7, 2016 ("[T]he F.C.C. said it found that even among customers who had tried to delete regular cookies from their mobile browsers, the supercookies, or hidden code unique to each customer, were undeletable and used as a workaround to continue data collection.").

[53] Press Release, Federal Communications Commission, FCC Settles Verizon "Supercookie" Probe, Requires Consumer Opt-In for Third Parties (Mar. 7, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DOC-338091A1.pdf.

[54] *In re* TerraCom, Inc. & YourTel America, Inc., 30 FCC Rcd. 7075 (2015).

including names, addresses, dates of birth, Social Security numbers, and driver's license numbers of consumers seeking low-income Lifeline telephone services.[55] In April 2015, the FCC fined AT&T $25 million for failure to reasonably secure proprietary consumer information and ordered AT&T to improve its data security organizations and procedures.[56] In September 2014, the FCC exacted a $7.4 million fine from Verizon in a consent decree arising out of Verizon's use of "its customers' personal information when tailoring marketing campaigns without first providing its customers with the required notice or obtaining their consent."[57] These FCC consent orders, among several others,[58] have served as important steps in the right direction to demand that electronic communication be operated in a manner that preserves consumer privacy except to the extent expressly, voluntarily, knowingly, and intelligently waived by the consumer.

VI. EUROPE IS FAR AHEAD ON CONSUMER PRIVACY PROTECTIONS AND THE RIGHT TO BE FORGOTTEN

In France, the Commission Nationale de l'Informatique et des Libertés ("CNIL"), applying France's Data Protection Act,[59] has ordered Microsoft to stop collecting excessive data[60] on Windows 10 users without their express consent to sell the data to marketers.[61] Indeed, Europe has dramatically controlled electronic

---

[55] *See generally* Robert Sprague & Corey Ciochetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91, 97-101 (2009) (providing that as collection, aggregation, and dissemination of data expand, risks related to inadvertent or intentional data breaches and data thefts amplifies risks to consumer privacy online).

[56] *In re* AT&T Services, Inc., 30 FCC Rcd. 2808 (2015).

[57] *In re* Verizon Compliance with the Comm'n's Rules & Regulations Governing Customer Proprietary Network Info., 29 FCC Rcd. 10303 (2014).

[58] *E.g.*, *In re* Cox Commc'ns, Inc., No. EB-IHD-14-0017829 (Fed. Commc'ns Comm'n Nov. 5, 2015); *Cellco Partnership*, 31 FCC Rcd. 1843; *AT&T Services*, 30 FCC Rcd. 2808.

[59] Décret 2005-1309 du 20 octobre 2005 relative à l'informatique, aux fichiers et aux libertés [Decree 20050-1309 of October 20, 2005 on Data Processing, Files and Individual Liberties], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Mar. 25, 2007; Loi 78-17 du 6 janvier 1978 relative à technologie de l'information, aux fichiers et aux libertés [Law 78-17 of January 6, 1978 on Information Technology, Data Files and Individual Liberties], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], March 17, 2014.

[60] Including, without limitation, information on all apps downloaded and time spent on each one, all collected via an advertising identifier activated "by default when Windows 10 is installed, enabling Windows apps and other parties' apps to monitor user browsing and to offer targeted advertising without obtaining users' consent." Commission Nationale de l'Informatique et des Libertés, *Windows 10: CNIL publicly serves formal notice to Microsoft Corporation to comply with the French Data Protection Act within three months* (July 20, 2016), https://www.cnil.fr/en/windows-10-cnil-publicly-serves-formal-notice-microsoft-corporation-comply-french-data-protection.

[61] Isabelle Falque-Pierrotin, Chair, National Data Protection Commission, Decision No. 2016-058 (June 30, 2016) (serving a formal notice on Microsoft Corporation) (France).

communications and Internet service to protect consumer data privacy[62] and has done so without any measurable damage to the European economy.[63] As the European Commission has noted,

> Whenever you open a bank account, join a social networking website or book a flight online, you hand over vital personal information such as your name, address, and credit card number. What happens to this data? Could it fall into the wrong hands? What rights do you have regarding your personal information? Everyone has the right to the protection of personal data. Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose. Furthermore, persons or [organizations] which collect and manage your personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law.[64]

Although Europe has tried to apply those restrictions more globally through international agreements, the European Union's adopted rules and directives only apply to Europe (and presumably to digital data entering or leaving Europe), and many American firms have contested such intrusion of European regulations into American cyberspace.[65]

Throughout Europe, there has been a growing trend to compel Internet service providers to provide a mechanism for users who wish to be "forgotten" on the Internet, that is, who wish their digital information footprint trimmed or excised.[66] Google has begun to migrate that possibility to the United States.[67] Of course,

---

[62] *See, e.g.*, 2010 O.J. (C.83) 7 (defining a right to respect for private and family life); EUR. CONSULT. ASS'N, *Convention for the Protection of Human Rights and Fundamental Freedoms as Amended by Protocols No. 11 and No. 14*, art. 8 (1950) (defining a right to respect for private and family life); EUR. CONSULT. ASS'N, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (1981).

[63] That is a critical fact given that one of the theories underpinning the FTC's laissez faire approach to Internet regulation is that any intrusive regulation would impede the American economy. That appears to be a bogeyman and not a substantive concern based on Europe's experience.

[64] *Protection of Personal Data*, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/ (last visited Sept. 11, 2016).

[65] Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of A Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1053-54 (2000).

[66] Directive 95/46/EC, of the European Parliament and of the Council of Oct. 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such data, 1995 O.J. (L 281) 12 (defining the right to be forgotten); *see also* Case C-131-12, Google Inc. v. Agencia Española de Protección de Datos (AEPD), 2014 EUR - Lex CELEX LEXIS 1 (May 13, 2014).

[67] "If you are worried about your online privacy, it might be of interest to you that Google has quietly brought its Google forget program to the U.S. It has made it quite simple, for the most part. Simply go to myactivity.google.com to see the history of your searches, YouTube viewing and everything else you do on Google platforms, and then be guided through the process of trimming that history." Evan Schuman, *Google Quietly Brings Forgetting to the U.S.*, COMPUTERWORLD (July 13, 2016),

conversely, some view excising information from the Internet as selective censorship.[68]

Given globalization and the international reach of the Internet and Internet service providers, perhaps international treaties are the venue with the proper scope for curtailing privacy erosions worldwide. Even if those global treaties were ratified, each nation must protect its own Internet and telecommunications users because once the data is disseminated and stored, it can be stolen, sold, aggregated, and shared without regard to any treaty-based restrictions.

VII. CONCLUSIONS AND A CALL FOR ACTION

It is past time for the FTC, other agencies, the balance of the executive branch, and Congress to step in and control this torrent of purloined consumer data.[69] Personal privacy causes of action are not enough, and digital data, once shared or stored, are forever vulnerable to dissemination and misuse. If some consumers wish to waive their privacy interests and opt-in to data sharing and storage, then that right and power certainly rests with those consumers. However, for those consumers who value privacy, but wish to avail themselves of modern technologies without sacrificing their privacy unawares or without free consent, opaque privacy waivers that consumers merely click through without understanding are no substitute for real and substantive consumer privacy protections in the digital age. It is time to recast Internet clickwrap, browsewrap, click-through, and "I Agree" privacy waiver fictions as unenforceable waivers of adhesion.

---

http://www.computerworld.com/article/3094833/data-privacy/google-quietly-brings-forgetting-to-the-u-s.html.

[68] Qichen Zhang, *Google Joins Twitter in Move Toward Selective Censorship*, OPENNET INITIATIVE (Feb. 3, 2012), https://opennet.net/blog/2012/02/google-joins-twitter-move-toward-selective-censorship.

[69] In spite of commentators' insistence, private enforcement of a privacy tort, Andrew J. McClurg, *A Thousand Words and Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63 (2003), even within a class action framework, occurs only after the data is shared and breached, and ignores the power and reach of legislative intervention on such a classically interstate concern.