ONLINE PRIVACY AND THE INVISIBLE MARKET FOR OUR DATA

Rebecca Lipman[*]

Consumers constantly enter into blind bargains online. We trade our personal information for free websites and apps, without knowing exactly what will be done with our data. There is nominally a notice and choice regime in place via lengthy privacy policies. However, virtually no one reads them. In this ill-informed environment, companies can gather and exploit as much data as technologically possible, with very few legal boundaries. The consequences for consumers are often far-removed from their actions, or entirely invisible to them. Americans deserve a rigorous notice and choice regime. Such a regime would allow consumers to make informed decisions and regain some measure of control over their personal information. This article explores the problems with the current marketplace for our digital data, and it explains how we could make a robust notice and choice regime work for consumers.

INTRODUCTION

When you go online or use an app on your phone, you are sharing your information with multiple companies at once.[1] If you tell the dating website OKCupid you occasionally drink or do illegal drugs, OKCupid will save that information to your profile, but marketers can also buy that information in real time.[2] If you look up something on the Center for Disease Control's website, say, "herpes symptoms," the CDC will tell Google what you looked up.[3] The CDC is not trying to profit from you, but they use Google Analytics to measure their website traffic. The

[*] Law Clerk to the Honorable Anne E. Thompson, United States District Judge, District of New Jersey. J.D. *cum laude*, Harvard Law School, 2015. Many thanks to Professors Phil Heymann, Jonathan Zittrain, Lorrie Faith Cranor, and Richard Parker for their notes and support. Thank you to Ryland Li, Jodie Liu, Michelle Sohn, Melinda Brown, Jana Schwartz, and Stephen Van Meter for their helpful comments.

[1] Robert L. Mitchell, *Ad Tracking: Is Anything Being Done?*, COMPUTERWORLD (Apr. 2, 2014), http://www.computerworld.com/article/2489106/data-privacy/ad-tracking--is-anything-being-done-.html.

[2] Daniel Zwerdling, *Your Digital Trail: Private Company Access,* NPR (Oct. 1, 2013), http://www.npr.org/blogs/alltechconsidered/2013/10/01/227776072/your-digital-trail-private-company-access.

[3] Brian Merchant, *Looking Up Symptoms Online? These Companies Are Tracking You*, MOTHERBOARD (Feb. 23, 2015), http://motherboard.vice.com/read/looking-up-symptoms-online-these-companies-are-collecting-your-data.

CDC uses Google Analytics because it is a free, useful tool.[4] It is a "free" tool because it is quietly paid for with your data.[5]

There are programs that can show you which third parties are watching you on a given website.[6] They can even block many of these third parties,[7] though blocking them may disrupt the appearance or usability of some sites.[8] But these programs cannot tell you what those third parties will do with your information.[9] They also cannot tell you what inferences these companies might make about you.[10] For example, Target famously created an algorithm to determine which female customers might be pregnant, in order to send them relevant coupons.[11] The women did not need to buy baby clothes for Target to know they were pregnant – it was subtler cues like buying zinc, lotion, and a purse large enough to double as a diaper bag.[12] Target was aware it could make women "queasy" by suddenly sending them ads for maternity clothes, so it started to put the baby-related ads in between ads for unrelated products, to make the placement look random.[13] "As long as we don't spook her," a Target executive said, "it works."[14]

---

[4] *Id.*
[5] *Id.*
[6] *See, e.g., Features,* GHOSTERY, https://www.ghostery.com/en/features.
[7] *See id.* But Ghostery itself may actually track you too, if you let it. Tom Simonite, *A Popular Ad Blocker Also Helps the Ad Industry*, MIT TECHNOLOGY REVIEW (June 17, 2013), http://www.technologyreview.com/news/516156/a-popular-ad-blocker-also-helps-the-ad-industry/. Ghostery and similar program can also be thwarted. *See, e.g.*, *Chrome Extensions – AKA Total Absence of Privacy*, DETECTIFY LABS (Nov. 19, 2015), http://labs.detectify.com/post/133528218381/chrome-extensions-aka-total-absence-of-privacy.
[8] *See* Andrew Couts, *Privacy Plug-in Showdown: Do Not Track Plus vs. Ghostery*, DIGITAL TRENDS (Aug. 15, 2012), http://www.digitaltrends.com/web/do-not-track-plus-vs-ghostery/.
[9] *See* Andy Kahl, *Ghostery 5.3 – Getting to Know the Companies Who Are Getting to Know You*, GHOSTERY (June 2, 2014), https://purplebox.ghostery.com/post/1016024123.
[10] *See id.*
[11] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp.
[12] *Id.*
[13] *Id.*
[14] *Id.*

Many Americans feel spooked.[15] Our data seems to be more widely disseminated, and more vulnerable than ever. Hackers gained access to millions of Americans' accounts at JP Morgan and Anthem Health Insurance.[16] The NSA collected millions of Americans' phone records for years.[17] Commercial data brokers buy and sell our data to such an extent that one broker has 3,000 data points for nearly every single U.S. consumer.[18]

At least 30% of Americans have taken one or more steps to avoid surveillance since the Edward Snowden revelations.[19] The remaining 70% have not taken steps perhaps because they are not concerned, or because they do not know where to begin. The above scenarios – cyber attacks, government surveillance, and commercial data aggregation – are fundamentally different problems, with different solutions. But it is easy for the disparate threads to merge together to become one amorphous fear, with no hint of how to secure our personal information.

This article seeks to take on just one of those threads – commercial use of individuals' data. Consumers enter into essentially blind bargains online, where they trade their personal

---

[15] Annie Flaherty, *Americans Growing More Concerned Over Their Online Privacy: Study*, ASSOCIATED PRESS (Sept. 5, 2013), http://www.huffingtonpost.com/2013/09/05/online-privacy-study_n_3870670.html. 50 percent of Internet users saying they are worried about the information available about them online, up from 33 percent in 2009.

[16] Supriya Kurane, *JPMorgan Data Breach Entry Point Identified: NYT*, REUTERS (Dec. 22, 2014), http://www.reuters.com/article/2014/12/23/us-jpmorgan-cybersecurity-idUSKBN0K105R20141223; Elizabeth Weise, *Millions of Anthem Customers Alerted to Hack*, USA TODAY (Feb. 5, 2015), http://www.usatoday.com/story/tech/2015/02/05/anthem-health-care-computer-security-breach/22917635/.

[17] The USA FREEDOM Act mandated that the NSA's bulk collection end on November 29, 2015. Ellen Nakashima, *With Court Approval, NSA Resume Bulk Collection of Phone Data*, WASH. POST (June 30, 2015), https://www.washingtonpost.com/world/national-security/with-court-approval-nsa-resumes-bulk-collection-of-phone-data/2015/06/30/a40c5a64-1f3f-11e5-bf41-c23f5d3face1_story.html. The NSA is not the only agency that had been in the habit of collecting Americans' telephone records in bulk. The DEA kept records of virtually all Americans' international calls to as many as 116 countries from 1992 to 2013 with no court supervision whatsoever. The program stopped after the public backlash to the NSA's similar program. John Ribeiro, *US Drug Enforcement Amassed Bulk Phone Records for Decades*, PCWORLD (Apr. 7, 2015), http://www.pcworld.com/article/2907332/us-drug-enforcement-amassed-bulk-phone-records-for-decades.html.

[18] FEDERAL TRADE COMMISSION, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 65 (2014), *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[19] Jason Hahn, *Pew: 22% of Americans Have Changed Email, Social Media, Cell Phone Use Post-Snowden*, DIGITAL TRENDS (Mar. 21, 2015), http://www.digitaltrends.com/web/pew-22-of-americans-have-changed-email-social-media-cell-phone-use-post-snowden-nsa/. Other studies have previously shown the number of Americans who have tried at least one method of hiding their online activity is as high as 86%. Flaherty, *supra* note 16.

information for free websites and apps. There is nominally a notice and choice regime in place via lengthy privacy policies, but virtually no one reads them.[20] Some consumers think just having a privacy policy means a website will keep their information private.[21] In this ill-informed environment, companies can gather and exploit as much data as technologically possible, with very few legal boundaries. The consequences for consumers are often far-removed from their actions, or entirely invisible to them. Consumers deserve a more rigorous form of notice and choice that allows them to make informed decisions and regain some measure of control over their personal information online.

Part I of this article will explore why the current system of buying and selling individuals' digital data is problematic. Part II will describe the various laws and agencies that are active in this area of privacy law. Lastly, Part III will propose a new, mandatory notice and choice regime to empower individuals and pressure companies to take greater responsibility for what they do with their customers' data. Part IV will briefly conclude.

I. WHAT'S WRONG WITH "CREEPY?"

Third party advertisers – "third" parties because they are present in addition to #1, you, and #2, the website you are visiting – can often foster "creepy" outcomes. Just three years ago it was considered newsworthy to report that if you searched for an item on Google, Facebook would show you ads for that same item the next day.[22] One young journalist described this

[20] James Temple, *Why Privacy Policies Don't Work – And What Might*, SF Gate (Jan. 29, 2012), http://www.sfgate.com/business/article/Why-privacy-policies-don-t-work-and-what-might-2786252.php.
[21] *Id.*
[22] Walter Hickey, *I Just Realized How Zealously Facebook Tracks Me And Sells That Info To Advertisers*, BUSINESS INSIDER (Apr. 18, 2013), http://www.businessinsider.com/i-didnt-know-facebook-tracked-me-2013-4.

experience as "creepy." Today, the experience is commonplace.[23] Many users may still be creeped out, but others are pleased to receive ads that are relevant to them.[24]

These relevant ads are made possible by the extensive profiles built by data brokers. Data brokers collect vast amounts of information about consumers, such as their race, sex, education level, politics, buying habits, and social security numbers.[25] Consumers are then classified according to their age, socioeconomic status, political leanings, or even religious affiliations.[26] These classifications are useful to advertisers trying to reach specific consumers, but they can also shade into discrimination. A data broker-created category containing high numbers of low-income minorities might be targeted with high-interest payday loans.[27] The Federal Trade Commission ("FTC") posits that a category like "Biker Enthusiasts" could be useful for advertisers wanting to sell motorcycles, but could also be used by an insurance company looking for signs of risky behavior.[28]

Additionally, the data brokers' profiles usually contain mistakes, with one of the largest brokers admitting up to 30% of a person's profile may be wrong at any given time.[29] These mistakes, which consumers are almost inevitably unaware of, can have real consequences. One

---

[23] *See How Online Advertisers Read Your Mind*, THE ECONOMIST (Sept. 21, 2014), http://www.economist.com/blogs/economist-explains/2014/09/economist-explains-12.

[24] A 2012 Pew Poll found that 28% of Americans, particularly younger Americans, did not mind targeted advertising because it provided them with more relevant ads. *Internet Users Don't Like Targeted Ads*, Pew Research Center (Mar. 13, 2012), http://www.pewresearch.org/daily-number/internet-users-dont-like-targeted-ads/.

[25] *See* 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.

[26] *Companies Tracking Our Online Footsteps Should Be More Transparent, Says FTC*, PBS NEWSHOUR (June 13, 2014), http://www.pbs.org/newshour/bb/companies-tracking-online-footsteps-transparent-says-ftc/.

[27] Press Release, Federal Trade Commission, FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information (May 27, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more, Julie Brill, U.S. Federal Trade Commissioner, Big Data and Consumer Trust: Progress and Continuing Challenges (Oct. 15, 2014) *available at* 2014 WL 5319633, at *3.

[28] Press Release, Federal Trade Commission, FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information, *supra* note 26.

[29] Melanie Hicken, *Find Out What Big Data Knows About You (It May Be Very Wrong)*, CNN MONEY (Sept. 5, 2013), http://money.cnn.com/2013/09/05/pf/acxiom-consumer-data/.

broker named Spokeo paid $800,000 to settle FTC charges that it marketed its profiles as an employment screening tool, while failing to ensure its information was accurate.[30] It is not hard to imagine a job applicant being passed over because a broker incorrectly reported his education level, or managed to paint an unflattering picture through various other inaccurate pieces of personal information.[31]

There are laws against employment discrimination, and other types of discrimination that data brokers' profiles could facilitate.[32] However, the brokers themselves are essentially unregulated, operating with what the FTC calls "a fundamental lack of transparency."[33] So while a job applicant who believes she encountered a racist interviewer can sue under anti-discrimination laws, that same applicant will have no inkling that she was discriminated against because of her (possibly incorrect) Spokeo profile.[34] The data brokers enable employers and others to discriminate, or at the very least, get uncomfortably close to ethical gray areas by offering vast amounts of personal information that were not previously readily available.

We are hardly the first generation to have struggled with the effects of new, privacy-reducing technologies. Justice Louis Brandeis was disturbed by the proliferation of gossip

---

[30] Press Release, Federal Trade Commission, Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FRCA (June 12, 2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed.

[31] One plaintiff alleged that Spokeo hurt his employment prospects by incorrectly listing his employment status, marital status, age, educational background, number of children, "economic health," and "wealth level." Brief of Plaintiff-Appellant at 11, Robins v. Spokeo, Inc., No. 11-56843 (9th Cir. June 1, 2012), *available at* 2012 WL 2132528. The Ninth Circuit did not decide if the prospective harm to Robins' employment status was enough to support standing, because the court found that he had standing under the Fair Credit Reporting Act. Robins v. Spokeo, 742 F.3d 409, 413-14 (9th Cir. 2014). The Supreme Court granted cert and heard argument this past November. The question presented was if Congress may confer Article III standing on a plaintiff "who suffers no concrete harm." *Spokeo v. Robins*, SCOTUSBLOG, http://www.scotusblog.com/case-files/cases/spokeo-inc-v-robins/.

[32] *See, e.g.,* Title VII of the Civil Rights Act of 1964, Pub. L. No. 88-352.

[33] DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, *supra* note 19, at vii.

[34] Even if she were aware of her profile, she may not have standing or the ability to show a harm to her employment prospects. *See Robins*, 742 F.3d at 414 n.3.

columns, and particularly the advances in "instantaneous photograph[y]" in 1890.[35] He wrote an article called "The Right to Privacy" which provided the background principles for modern privacy law.[36] His worries feel outdated now, but at the time, the "unauthorized circulation of portraits of private persons" was a real concern because of the new technology that enabled that wide circulation.[37] One generation's technological crisis is another generation's status quo. When Caller ID was first introduced, some felt it created serious privacy problems.[38] Some states even sought to regulate it.[39] Today, Caller ID is ubiquitous, and an essential part of any cell phone's functionality.[40]

One difference between photographs, Caller ID, and our current situation is that photographs and Caller ID are visible to the consumer. Many of the technologies that invade our privacy today do so invisibly. Besides the data brokers and smaller third party trackers described in the introduction, various apps and items we purchase directly can collect a surprising amount of personal information. You might not mind your Groupon app knowing your location, so it can offer you deals for local businesses, but you might mind it checking your location every twenty minutes, and selling your location to advertisers.[41] You might be happy to buy a TV that can be voice-activated, but you might not realize that means your TV will record all your conversations

[35] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).
[36] *See generally, id.*
[37] *See id.*
[38] Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J. L. & TECH. 59, 72-73 (2014).
[39] *Id.*
[40] Many people may not answer their phone if they do not recognize the number calling them. Moreover, try to imagine looking up a recent call, or finding an old voice mail, without each item helpfully labeled with the correct name or number.
[41] Dozens of popular apps collect your location every three minutes, sharing your location information with advertisers 73% of the time. Mary Beth Quirk, *Study: Some Popular Android Apps Tracking User Location Once Every Three Minutes*, CONSUMERIST (Mar. 24, 2015), http://consumerist.com/2015/03/24/study-some-popular-android-apps-tracking-user-location-once-every-three-minutes/.

and send them to third parties (albeit for apparently benign purposes.)[42] There is a wealth of new data being recorded from users, including sensitive (but unprotected) health data,[43] but the economy growing up around individuals' data is largely invisible to us.

That is not to say that we are not active participants in this economy. Our data is purchased (for very small amounts, at the individual level),[44] and we are compensated for it. Services like Gmail, Google Calendar, and Facebook are only free because users' data empowers Google and Facebook to generate a lot of revenue from selling ads.[45] If they were barred from aggregating our data, they could no longer offer targeted ads, potentially seriously hurting their bottom lines, and their ability to offer services for free.[46] We have, in a sense, simply bargained our data away for free services.[47] But it is a bargain we went into without any firm sense of what exactly we were giving up.

I do not wish to underplay the multifaceted value of many online services. Ben Wittes and Jodie Liu wrote an excellent article that argues there are actually many privacy gains we

---

[42] Samsung apparently uses a third party company to help comprehend your voice commands, but it does not say who that third party is, or if your voice data is encrypted or otherwise protected when it is transferred. Parmy Olson, *Samsung's Smart TVs Share Living Room Conversations With Third Parties*, FORBES (Feb. 9, 2015), http://www.forbes.com/sites/parmyolson/2015/02/09/samsungs-smart-tv-data-sharing-nuance/.

[43] Health apps have greatly increased in popularity, but the information collected in them is not covered by HIPAA because the health information is generated by the user, not by a HIPAA-covered entity such as a hospital. Andrea Peterson, *Privacy Advocates Warn of 'Nightmare' Scenario as Tech Giants Consider Fitness Tracking*, WASH. POST (May 19, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/19/privacy-advocates-warn-of-nightmare-scenario-as-tech-giants-consider-fitness-tracking/.

[44] Your location is only worth about $.0005, though information about your health information can go for $.26. Emily Steel, Callum Locke, Emily Cadman, and Ben Freese, *How Much is Your Personal Data Worth?*, FINANCIAL TIMES (June 12, 2013), http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html#axzz3XPy8lowp.

[45] *See* Heather Kelly, *Why Gmail and Other E-mail Services Aren't Really Free*, CNN (Apr. 1, 2014), http://www.cnn.com/2014/03/31/tech/web/gmail-privacy-problems/, Rolfe Winkler & Jack Marshall, *Google May Offer New Way to Target Ads*, WALL STREET JOURNAL (Apr. 14, 2015), http://www.wsj.com/articles/google-may-offer-new-way-to-target-ads-1429044389.

[46] *See After Success, More Spending on Mobile Local Ads*, EMARKETER (Apr. 17, 2014), http://www.emarketer.com/Article/After-Success-More-Spending-on-Mobile-Local-Ads/1010763, Steven Perlberg, *Targeted Ads? TV Can Do That Now Too*, WALL STREET JOURNAL (Nov. 20, 2014), http://www.wsj.com/articles/targeted-ads-tv-can-do-that-now-too-1416506504.

[47] For an alternative perspective on the value of individuals' data, *see* JARON LANIER, WHO OWNS THE FUTURE? (2013). Lanier advocates for individuals being compensated for their data and other digital contributions via an attribution and micro-payments system. *Id.* at 19-21.

receive from modern technologies, which are often unfairly dismissed as merely gains in convenience or efficiency.[48] Most people are grateful they can ask Google about their embarrassing medical symptoms instead of asking a friend or making a doctor's appointment. It is definitely a privacy gain to keep your medical concerns or pornography preferences away from people you know, even if the tradeoff is sharing that information with Google. However, by using examples like health information and pornography, Wittes and Liu primarily envision privacy as secrecy. But when Americans are aware of any type of surveillance, they often react negatively, whether it concerns their darkest secrets or their everyday behavior. For example, Google Glass was a flop in large part because people disliked the idea that they could be unknowingly filmed by anyone wearing Google Glass.[49] Even if the filming was in a public place, such as a bar or restaurant, people were upset by it.[50] People do not want their everyday interactions recorded. Therefore, the privacy gain of Google keeping our embarrassing secrets for us must be measured against the privacy loss of Google learning things that might not be secret per se, but that we do not want recorded on a daily basis.

We are fairly adept at protecting our privacy in the physical world. We know to lower our voices when having a private conversation in a public place. We often change our behavior when someone points a recording device at us, whether or not we were engaged in a "secret" activity at the time. But when we go online, these physical cues are absent. There is consequently an

[48] Benjamin Wittes & Jodie C. Liu, *The Privacy Paradox: The Privacy Benefits of Privacy Threats*, BROOKINGS INSTITUTE (May 2015), http://www.brookings.edu/~/media/research/files/papers/2015/05/21-privacy-paradox-wittes-liu/wittes-and-liu_privacy-paradox_v10.pdf.
[49] Alyssa Newcomb, *From 'Glassholes' to Privacy Issues: The Troubled Run of the First Edition of Google Glass*, ABC NEWS (Jan. 16, 2015), http://abcnews.go.com/Technology/glassholes-privacy-issues-troubled-run-edition-google-glass/story?id=28269049.
[50] *See, e.g.,* Hillary Crosley Coker, *Entitled Creep Secretly Films People With Google Glass*, JEZEBEL (Feb. 28, 2014), http://jezebel.com/entitled-creep-secretly-films-people-with-google-glass-1532859496.

intuition gap between how private our online browsing feels, and how public it actually is.[51] We may know intellectually that our activities are being recorded, but there is no physical trigger that warns us to watch what we do or say. At the same time, the consequences are arguably much greater. A stranger might eavesdrop on you in a restaurant, but the stranger does not know who you are, and likely will not remember your conversation a day later. When a data broker or Google tracks your behavior online, that information is identified with you personally, and it will be saved for an unknown (and possibly indefinite) period of time.[52] If users could intuitively understand how they were being monitored, they might take a much stronger approach to protecting their data.

Currently, it is not clear how we strongly we should protect Americans' privacy online. There are privacy policies that alert users, albeit in opaque terms, that their data will be collected and shared. However, virtually no one reads these policies.[53] Americans provide inconsistent opinions about privacy in survey results.[54] One survey suggests we tend to accept whatever data sharing is the current status quo, but resist additional sharing, without any firm idea of what the status quo is.[55] On a more academic level, the federal Privacy and Civil Liberties Oversight

---

[51] *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027, 1040 (2012) (discussing how "visceral" notice could be a boon to online privacy).

[52] *See* Cecilia Kang, *Google Tracks Consumers' Online Activities Across Products, and Users Can't Opt Out*, WASH. POST (Jan. 24, 2012), http://www.washingtonpost.com/business/technology/google-tracks-consumers-across-products-users-cant-opt-out/2012/01/24/gIQArgJHOQ_story.html.

[53] If someone wanted to read all the privacy policies for the websites they visit in a year, it would take them about one month. Shankar Vedantam, *To Read All Those Web Privacy Policies, Just Take A Month Off Work*, NPR (Apr. 19, 2012), http://www.npr.org/blogs/alltechconsidered/2012/04/19/150905465/to-read-all-those-web-privacy-policies-just-take-a-month-off-work.

[54] *See, e.g.,* Tene & Polonetsky, *supra* note 37, at 59, 64 (discussing a study where approximately half of the respondents did not want companies being able to hear them complaining about the companies, unless the companies' goal was to improve their products, in which case listening in was fine).

[55] A survey by Carnegie Mellon Professor Lorrie Faith Cranor and Stanford Professor Aleecia McDonald showed that only 11% of Americans would pay $1/month to withhold their data from their favorite news site. But 69% of Americans would not accept a $1 discount on their monthly internet bills in exchange for allowing their data to be tracked. Alexis C. Madrigal, *How Much Is Your Data Worth? Mmm, Somewhere Between Half a Cent and $1,200*, THE ATLANTIC (Mar. 19, 2012), http://www.theatlantic.com/technology/archive/2012/03/how-much-is-your-data-worth-mmm-somewhere-between-half-a-cent-and-1-200/254730/.

Board held a day-long public meeting in 2014 called "Defining Privacy."[56] Over a dozen panelists highlighted the many different ways people think about privacy.[57] If privacy experts cannot agree on a single definition of privacy, and if average Americans have inconsistent opinions about what they are comfortable sharing, how can we craft a coherent policy approach to address Americans' concerns about online privacy?

One important first step we can take is to better inform individuals about the invisible personal data marketplace. If users had access to clear, concise information about what data was being collected about them, and what was being done with that data, the intuition gap between the physical world and the online could be greatly reduced. Americans might then speak with a more uniform voice about what practices they are comfortable with. Dr. Lorrie Faith Cranor, a computer science professor and privacy expert at Carnegie Mellon University, ran a study where consumers used a custom-built search engine to find products to buy online. Next to the links to websites selling the products, the search engine displayed a simple "privacy meter" that indicated how strong the privacy policy was for each website. A significant number of consumers chose to pay more for the products when they could buy them from more privacy-protective websites.[58] This suggests that effective privacy notices could make a real difference in changing consumers' behavior, and consequently, the privacy practices of individual companies.

Different privacy notice regimes have been tried previously, with mixed, mostly poor results. Part III will explore these previous attempts before suggesting how a new regime could

[56] *See November 12: Public Meeting on "Defining Privacy"*, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD (Nov. 7, 2014), https://www.pclob.gov/newsroom/20141020.html.
[57] *See generally Defining Privacy Forum*, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD (Nov. 12, 2014), https://www.pclob.gov/library/20141112-Transcript.pdf.
[58] Lorrie Faith Cranor, *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. TELECOMM. & HIGH TECH. L. 273, 292-93 (2012).

actually benefit consumers. However, it is helpful to first examine what laws we currently have in place that can protect Americans' privacy online.

II. THE CURRENT STATE OF PRIVACY LAW

A. Federal Statutes and the Fourth Amendment

The Fourth Amendment protects citizens against unreasonable searches and seizures,[59] including warrantless searches of our digital data.[60] While the Fourth Amendment has significant implications for the interplay between government and the private companies that hold our data,[61] the Fourth Amendment does not protect us from our voluntary interactions with private companies.

Congress has passed a number of sectoral statutes that protect discrete types of data that may be held by corporations. The Fair Credit Reporting Act (FCRA) protects our credit information.[62] The Family Educational Rights and Privacy Act (FERPA) protects students' educational records.[63] The Health Information Portability and Accountability Act (HIPAA) protects our medical information.[64] These statutes cover limited types of information, in limited situations. The medical information your FitBit or Apple Watch collects is not covered by HIPAA, because HIPAA only covers certain entities like hospitals or health insurance companies, not user-generated health information.[65] New educational apps record how long students spend watching tutorials, how they do on quizzes, and how long it takes them to do their

[59] U.S. CONST. amend. IV.
[60] *See* Riley v. California, 134 S. Ct. 2473 (2014).
[61] *See* Rebecca Lipman, *The Third Party Exception: Reshaping an Imperfect Doctrine for the Digital Age*, 8 HARV. L. & POL'Y REV. 471 (2014).
[62] 15 U.S.C. §§1681-1681x (2006 & Supp. V 2011).
[63] 20 U.S.C. §1232g.
[64] Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).
[65] *See* 45 C.F.R. § 160.103(4)(iv). *See also* Peterson, *supra* note 42.

homework online.[66] But none of this information, or the consequential inferences educational companies can make about a child's intelligence or interests, is protected by FERPA because the apps' data does not constitute a protected "education record."[67] Congress will hopefully close some of these holes, but statutory reform is painfully slow compared to how quickly technology moves forward.

Our system is significantly different from Europe's approach. The European Union ("EU") has pursued an omnibus approach, where data is protected regardless of what type of entity is holding the data, or the exact type of data at issue.[68] This more comprehensive view of a "right to privacy" affects how companies view their obligations to their customers. For its UK website, the giant data broker Acxiom has a privacy policy page that begins with "Acxiom Ltd respects the right of individuals to privacy."[69] The equivalent U.S. webpage begins with "Acxiom respects the privacy of every individual about whom we either process information or maintain information within Acxiom's information products."[70] Besides being much more legalistic and difficult to read, the U.S. version does not contemplate any individual "right" to privacy, and it mirrors the U.S.' sectoral approach by carefully defining whose privacy it will respect. These differences in approach can result in real impacts on consumers.[71] However, the

[66] Stephanie Simon, *Big Tech Pledges Student Privacy; Critics Scoff*, Politico (Oct. 7, 2014), http://www.politico.com/story/2014/10/student-privacy-tech-companies-111645.html.
[67] *See* 20 U.S.C. §1232g(a)(4).
[68] Paul M. Schwartz, *The Eu-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1975 (2013).
[69] *UK Privacy Policy,* ACXIOM, http://www.acxiom.com/about-acxiom/privacy/uk-privacy-policy/.
[70] *US Products Privacy Policy,* ACXIOM, http://www.acxiom.com/About-Acxiom/Privacy/US-Products-Full-Privacy-Policy/.
[71] For example, a European court held that individuals have a broad "right to be forgotten" that they can utilize to force Google to take down certain negative (though truthful) search results. No comparable right exists for Americans who are unhappy about their Google results. *See* Alistair Barr & Sam Schechner, *Google Advisory Group Recommends Limiting 'Right to Be Forgotten' to EU*, WALL STREET JOURNAL (Feb. 6, 2015), http://www.wsj.com/articles/google-advisory-group-says-limit-right-to-be-forgotten-to-eu-1423206470.

EU has struggled to meaningfully engage consumers about online privacy.[72] The EU's recent attempt at creating a notice and choice regime will be discussed below in Part III.

B. Agency Actions in Privacy Law

Despite our lack of omnibus privacy laws, the FTC and Federal Communications Commission ("FCC") have taken steps to regulate data privacy more broadly. The FTC has shown a significant interest in privacy, writing reports on facial recognition technology, privacy disclosures in apps, and privacy issues in apps aimed at children.[73] They have also studied health apps, specifically looking at what data those apps are sharing with other companies.[74] In 2014, they released a long report on data brokers, focusing on nine brokers in an attempt to shed some light on the industry as a whole.[75] The name of the report is telling: "Data Brokers: A Call for Transparency and Accountability." The FTC can only *call for* transparency and accountability, they cannot mandate it without supporting legislation. The press release for the report highlights this fact, providing a long list of policies the FTC "encourages" Congress to consider enacting.[76]

However, the FTC has been making the most of the statutory authority it does have to protect consumers' privacy. The FTC has authority from Section 5 of the Federal Trade Commission Act to prohibit "unfair or deceptive acts or practices."[77] This allows them to pursue companies that are blatantly trying to scam people, and companies with practices that fall into

---

[72] *See* Nicole Kobie, *Why the Cookies Law Wasn't Fully Baked – and How to Avoid Being Tracked Online*, THE GUARDIAN (Mar. 19, 2015), www.theguardian.com/technology/2015/mar/19/cookies-how-to-avoid-being-tracked-online.
[73] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 626 (2014).
[74] Kate Kaye, *FTC: Fitness Apps Can Help You Shed Calories – and Privacy*, ADVERTISING AGE (May 7, 2014), http://adage.com/article/privacy-and-regulation/ftc-signals-focus-health-fitness-data-privacy/293080/.
[75] Press Release, Federal Trade Commission, FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information, *supra* note 26.
[76] Press Release, Federal Trade Commission, FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information, *supra* note 26.
[77] 15 U.S.C. § 45.

more of a gray area.[78] For example, the FTC entered into a consent decree with the app Snapchat, which promised users they could send messages that would disappear instantly after reading. It turned out there were relatively simple workarounds that allowed people to secretly save messages, and the FTC got Snapchat to agree to 20 years of monitoring Snapchat's practices to make sure they do not deceive customers with false promises in the future.[79] The FTC was able to get a similar consent decree from Facebook, when Facebook broke numerous promises it had made to users in its privacy policies.[80]

While Section 5's "unfair or deceptive" language is powerful, these situations require the FTC to catch companies in a lie. A company could simply be vague about its commitment to privacy, or have a very broad privacy policy and count on nobody reading it, and Section 5 would not apply. For example, the company Groupon was relatively open about the fact that it was going to widely share its users' data, including their location, so the FTC could not come after them for doing so.[81] Conversely, the FTC was able to go after a popular flashlight app that sold location data, but that app actively deceived users by giving them a fake option that made it look like users could opt out of tracking.[82] If users do not do their homework on what information their apps are collecting about them, and the app makers are not foolish enough to outright lie about what they are doing, the FTC's ability to control how companies share our data is limited.

---

[78] *See* FEDERAL TRADE COMMISSION, 2014 PRIVACY AND DATA SECURITY UPDATE (2014), *available at* https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

[79] Brett Molina, *Snapchat Settles Privacy Complaint with FTC*, USA TODAY (May 8, 2014), http://www.usatoday.com/story/tech/2014/05/08/snapchat-ftc/8853239/.

[80] Press Release, Federal Trade Commission, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises (Nov. 29, 2011), *available at* https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

[81] David Magee, *Groupon's New Privacy Policy Goes Too Far: Selling Out Users*, International Business Times (July 11, 2011), http://www.ibtimes.com/groupons-new-privacy-policy-goes-too-far-selling-out-users-297525.

[82] Cecilia Kang, *Flashlight App Kept Users in the Dark About Sharing Location Data: FTC*, WASH. POST (Dec. 5, 2013), http://www.washingtonpost.com/business/technology/flashlight-app-kept-users-in-the-dark-about-sharing-location-data-ftc/2013/12/05/1be26fa6-5dc7-11e3-be07-006c776266ed_story.html.

In addition to using Section 5 to protect consumer privacy, the FTC has also used its Section 5 authority to address data security. It has forced multiple companies into settlements where the companies "put consumers' personal data at unreasonable risk."[83] This is a relatively novel use of Section 5, and the FTC has been challenged on their ability to mandate how companies protect user data from hackers. When Wyndham Hotels and Resorts suffered a data breach, the FTC brought an action against them, and Wyndham moved to dismiss it.[84] Wyndham asserted that the FTC lacks the authority to pursue unfairness claims in the context of data security, and that even if they do have that authority, FTC's current actions violate fair notice principles, as they had not promulgated regulations saying what data security measures companies must take.[85] A district court held in favor of the FTC,[86] Wyndham appealed, and the Third Circuit affirmed, providing a major win to the FTC.[87]

The FCC has not been as active on the privacy front, though they also have taken steps to regulate data security. Recently, they entered a $25 million settlement with AT&T, after hundreds of thousands of customers had their accounts breached.[88] The FCC's statutory authority is limited to telecommunication carriers under Section 222 of the Communications Act of 1934,[89] giving them far fewer companies to regulate than the FTC. Like the FTC, their authority in this area has also been questioned – by two of the FCC's own commissioners. Commissioner Pai has said that the FCC has never interpreted the Act to create an enforceable duty for

[83] *See* 2014 PRIVACY AND DATA SECURITY UPDATE, *supra* note 73.
[84] *See* F.T.C. v. Wyndham Worldwide Corp., 10 F.Supp.3d 602, 607 (D.N.J. 2014).
[85] *Id.*
[86] *Id.*
[87] F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (2015). *See also* Paul Rosenweig, *The FTC Takes Charge – FTC v. Wyndham*, LAWFARE (Aug. 26, 2015), https://www.lawfareblog.com/ftc-takes-charge-ftc-v-wyndham.
[88] Press Release, Federal Trade Commission, AT&T To Pay $25M To Settle Investigation Into Three Data Breaches (Apr. 8, 2015), *available at* http://www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches-0.
[89] 47 U.S.C. § 222.

companies to reasonably protect their users' personally identifiable information.[90] Commissioner O'Reilly has said that that he is "not convinced" the FCC has the authority to act in this area, even if companies generally have a responsibility to safeguard their customers' data.[91] Both commissioners also raised fair notice concerns similar to those Wyndham raised against the FTC.[92] Given the questions surrounding the FTC's and FCC's authority to force companies to implement reasonable data security measures, it is unsurprising that there have been strong calls on Capitol Hill for data breach legislation.[93]

In addition to Section 5 of the FTC Act, the FTC has authority to police privacy under two other statutes that bear mentioning. The Fair Credit Reporting Act ("FCRA") gives the FTC enforcement authority over companies that provide consumer reports.[94] The FTC has used this authority to force settlements with companies like Spokeo and Instant Checkmate,[95] who do not advertise themselves as credit reporting agencies,[96] but do provide information that can amount to a credit "consumer report."[97] The FTC can bring charges when these companies fail to comply with the FCRA by not properly verifying their information, fail to ensure that their information will only be used for legally permissible purposes, or fail to notify consumers about the

[90] *See* Statement of Commissioner Michael O'Reilly, Notice of Apparent Liability for Forfeiture, In re TerraCom, Inc. and YourTel America, Inc. at 25, File No.: EB-TCD-13-00009175, *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-173A1.pdf.
[91] *Id.* at 27.
[92] *Id.* at 25, 27.
[93] *See* Cory Bennett, *Lawmakers See Momentum for Data Breach Legislation*, THE HILL (Jan. 27, 2015), http://thehill.com/policy/cybersecurity/230867-data-breach-bill-is-achievable-goal.
[94] *See* 15 U.S.C. § 1681s.
[95] *See* Press Release, Federal Trade Commission, Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FRCA, *supra* note 29; 2014 PRIVACY AND DATA SECURITY UPDATE, *supra* note 73.
[96] *See About Instant Checkmate*, http://www.instantcheckmate.com/about/; *About Spokeo* http://www.spokeo.com/about.
[97] *See* 2014 PRIVACY AND DATA SECURITY UPDATE, *supra* note 73.

information they are selling about them.[98] And under the Children's Online Privacy Protection Act, the FTC can bring charges when companies collect children's personal information without their parents' consent.[99]

Lastly, the FTC has power beyond enforcement actions. The FTC can issue guidelines, press releases, and the above-mentioned reports. These documents create a kind of "soft law," as the FTC does not clearly indicate what parts of its recommendations might be mandatory, and what parts could just be considered "best practices."[100] Particularly larger, more responsible companies will tend to obey even soft signals from the FTC to avoid the chance of facing an enforcement action.[101]

The FTC has taken the lead on privacy through these different methods, but its ability to fully address digital privacy concerns is limited. The FTC is responsible for policing anticompetitive behavior, as well as unfair and deceptive practices in every industry in the U.S.[102] The agency may not have the bandwidth to also figure out how to extend their existing authorities to cover the abundance of new privacy problems. Moreover, the FTC's basic approach makes the most sense when the agency is policing the relationship between consumers and the companies they interact with. When a third party aggregator collects information about an individual from various sources, there is no direct interaction where they could have "deceived" the consumer. It also is difficult to argue that data brokers acted "unfairly" when their business model is the established driver of online advertising. The FTC cannot even mandate privacy policies – that was done by state law, by the innovative state of California.

---

[98] Press Release, Federal Trade Commission, Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FRCA, *supra* note 29; 2014 PRIVACY AND DATA SECURITY UPDATE, *supra* note 73.
[99] 2014 PRIVACY AND DATA SECURITY UPDATE, *supra* note 73.
[100] Solove & Hartzog, *supra* note 68, at 626.
[101] *See id.*
[102] *About the FTC*, http://www.ftc.gov/about-ftc.

C. California's Privacy Laws

California has long been a leader in online privacy laws. Most websites have privacy policies thanks to California's Business and Professions Code Section 22575, which requires that any website collecting personally identifiable information must "conspicuously post" a privacy policy on its website.[103] The law applies to any website that people in California might use, and therefore effectively requires privacy policies nationwide.[104] The law went into effect in 2004, and has since been amended to require websites disclose how they respond to "Do Not Track" signals, as well as if third party trackers may be present on the company's website.[105] A bill was proposed in 2013 to mandate that privacy policies must be much simpler and shorter, but the bill died a year later.[106]

California further forces disclosure through its "Shine the Light" law. Section 1798.83 of California's Civil Code requires companies to disclose if it sold a consumer's personal information for direct marketing, or alternatively, let a consumer opt out of the information sharing.[107] If the company chooses the disclosure route, it must disclose both what companies it shared the individual's information with, and what information was shared.[108] The law is limited, however, in how it defines "direct marketing purposes." Direct marketing only covers solicitations made to consumers via phone, mail, or e-mail.[109] It does not cover ads on websites

---

[103] Cal. Bus. & Prof. Code § 22575(a) (2014).
[104] *See id.*
[105] *See* 2013 Cal. Legis. Serv. (A.B. 370) (Consumers: internet privacy), *searchable at* http://leginfo.legislature.ca.gov/faces/billSearchClient.xhtml?.
[106] 2013 Cal. Legis. Serv. (A.B. 242) (Privacy: Internet), *searchable at* http://leginfo.legislature.ca.gov/faces/billSearchClient.xhtml?.
[107] *See* Cal. Civ. Code § 1798.83(a) (2006), Cal. Civ. Code § 1798.83(e)(6)(A) (2006), *California' S.B. 27, "Shine the Light" Law*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/profiling/sb27.html.
[108] *Id.*
[109] Cal. Civ. Code § 1798.83(e)(2).

and phones, or collection by data brokers.[110] The disclosures are also only available to consumers upon request,[111] and studies have shown that compliance with the law is spotty.[112] A "Right to Know" Act proposed in 2013 sought to expand Section 1798.83, but it died in January 2014.[113] It would have removed the "direct marketing" limitation, allowing consumers to find out all the different companies their information was being sold to.[114] The proposed act still would have required consumers to file a request in order to find out exactly who the company was sharing their personal information with.[115]

California has been the most aggressive in protecting children online. Section 22581 of their Business and Professions Code requires that websites and apps allow minors to take down content they previously posted.[116] If a teenager posts an inappropriate photo on Facebook, and later realizes that was a bad idea, the photo can be permanently deleted – but the law does not force third parties to remove content that has already been re-posted by someone else.[117] In another area of children's privacy, California passed a Student Online Personal Information Protection Act last year.[118] When the Act goes into effect in 2016, it will go a long way towards regulating educational apps that track students' development.[119] It prohibits targeted advertising, using data about students to build a profile about them for non-educational purposes, and selling or disclosing students' information.[120] Similar bills have been discussed at the federal level, but

---

[110] *See id.*
[111] Cal. Civ. Code § 1798.83(a).
[112] *Illuminating Calif.'s 'Shine the Light' Law*, LAW360, http://www.law360.com/articles/299095/illuminating-calif-s-shine-the-light-law.
[113] 2013 Cal. Legis. Serv. (A.B. 1291) (Privacy: Right to Know Act of 2013: disclosure of a customer's personal information), *searchable at* http://leginfo.legislature.ca.gov/faces/billSearchClient.xhtml?.
[114] *Id.*
[115] *Id.*
[116] Cal. Bus. & Prof. Code § 22581(a)(1).
[117] Cal. Bus. & Prof. Code § 22581(b)(2).
[118] 2014 Cal. Legis. Serv. (S.B. 1177) (Privacy: students), *searchable at* http://leginfo.legislature.ca.gov/faces/billSearchClient.xhtml?.
[119] *See id.*
[120] *Id.*

Congress has yet to follow California's lead.[121] California is also ahead on data security, with strong data breach notification laws already in place, while Congress mulls over potentially weaker alternatives.[122]

III. NOTICE AND CHOICE AS A SOLUTION

While all the above laws and agency actions are helpful in addressing certain privacy concerns, they do relatively little to address the larger problem of individuals entering into blind bargains for their data, and feeling insecure about their privacy as a result. Consumers can be empowered by giving them effective, immediate notice of what a given company will do with their information. However, before exploring a new notice and choice regime, it is important to review the regimes that have previously been attempted, and analyze why they failed.

A. Previous Attempts at Notice and Choice Solutions

Europe has been concerned about data privacy for a long time. The EU adopted the Data Protection Directive in 1995, which established many rules for information privacy.[123] However, a directive is not a law directly applicable to the various EU members. It is a mandate for the

[121] The federal Student Digital Privacy and Parental Rights Act was introduced in Congress at the end of April 2015. Natasha Singer, *Legislators Introduce Student Digital Privacy Bill*, N.Y. Times (Apr. 29, 2015), http://bits.blogs.nytimes.com/2015/04/29/legislators-introduce-student-digital-privacy-bill/.

[122] David Lazarus, *Federal Data-Breach Bill Would Replace Dozens of Stronger State Laws*, L.A. Times (Apr. 21, 2015), http://www.latimes.com/business/la-fi-lazarus-20150421-column.html. California also recently passed its own Electronic Communications Privacy Act, to protect all of its citizens' digital data (be it text messages, emails, or documents stored in the cloud) from being searched without a warrant by law enforcement. Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, WIRED (Oct. 8, 2015), http://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/. The bill is in part an updated and stronger version of the federal Electronic Communications Privacy Act, which has not been updated since it was passed in 1986. *See id.*; *H.R. 4952 – Electronic Communications Privacy Act of 1986*, https://www.congress.gov/bill/99th-congress/house-bill/4952/all-actions.

[123] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 25, 1995 O.J. (L 281).

different countries to pass their own laws consistent with the directive.[124] This results in a patchwork of protections that can lead to the original directive being watered down in practice. This is apparent in the EU's attempt to notify users when websites collect their data via cookies. The EU passed additional privacy directives in 2002 and 2009 to specifically regulate the use of cookies.[125] The 2002 directive created an opt-out system for users to avoid cookies, and the 2009 directive ostensibly strengthened privacy protections by requiring users to opt-in before cookies could be placed on their computers.[126] This has resulted in many websites simply adding a small banner on the top of their homepage that says something like: "We use cookies to give you the best possible experience on our site. By continuing to use the site you agree to our use of cookies."[127] This may be followed by a link that says "find out more," which leads to an extensive privacy policy.[128] There is little reason to think this type of notice is much more effective than American websites that include links to their privacy policies at the top or bottom of their webpages.[129] Moreover, different European countries have different requirements for providing users with cookie notices,[130] leading to a complex web of regulation for companies to

[124] Paul M. Schwartz, *The Eu-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1971-72 (2013).
[125] Eoin Carolan & M. Rosario Castillo-Mayen, *Why More User Control Does Not Mean More User Privacy: An Empirical (and Counter-Intuitive) Assessment of European E-Privacy Laws*, 19 VA. J.L. & TECH. 324, 336-38 (2015).
[126] *Id.*
[127] www.tesco.com, website for a leading British grocery and general merchandise retailer, last visited December 30, 2015.
[128] *Id.*
[129] One commenter notes that the cookie banners do not cause users to think about what cookies are or why they are used, making them ineffective for enhancing users' knowledge or privacy. Nicole Kobie, *Why the Cookies Law Wasn't Fully Baked – and How to Avoid Being Tracked Online*, THE GUARDIAN (Mar. 19, 2015), www.theguardian.com/technology/2015/mar/19/cookies-how-to-avoid-being-tracked-online (quoting Greg Rouchotas, technical director at Civic UK). A British web software development firm created a humorous infographic explaining the ineffectiveness of the UK's cookie laws, and celebrated their "death" in 2013. Oliver Emberton, *The Stupid Cookie Law is Dead at Last*, January 31, 2013, https://silktide.com/the-stupid-cookie-law-is-dead-at-last/.
[130] *Status of Implementation of the Amendment to Article 5.3 of Directive 2002/58/EC (the "EU Cookie Law")*, Bristows, June 5, 2015, http://www.debrauw.com/wp-content/uploads/NEWS%20-%20NEWSLETTERS/IP%20ICT/2015/European-Cookie-Law-Implementation-Survey-June-2015.pdf (explaining

navigate. At the same time, there has been little enforcement against non-complying websites,[131] leading to a much weaker notice and choice regime than the privacy directives envisioned.

The most prominent previous attempt at a notice and choice regime in the United States was P3P, the Platform for Privacy Preferences. P3P was a standard created by the World Wide Web Consortium, the organization that sets many of the standards for the internet.[132] In the mid-1990s, people had already noticed the unintelligibility of many websites' privacy policies, and there was a movement to simplify and standardize the policies.[133] If the policies were standardized, they could be easily read by both humans and machines. This would ideally lead to a person being able to set their privacy preferences just once in their browser, and then whenever the user visited a website that did not conform to their preferences, their browser would either block the site, or the user would be notified and she could choose to visit the site anyway.[134]

P3P ran into many problems. The primary issue was that creating a binding machine-readable P3P privacy policy was not mandatory.[135] When Microsoft incorporated P3P into Internet Explorer, companies had to provide a P3P policy in order for their cookies to get through. However, there was no enforcement mechanism forcing companies to obey their own P3P policies (the FTC declining to get involved in enforcement here), and even more egregiously, it turned out the policy could literally just say "Bogus Policy" and Internet Explorer

---

how companies can comply with each country's cookie laws. The report notes that many countries have provided no official guidance on how to comply with the laws.)

[131] Saira Nayak, *EU Regulatory Update: Dutch Cookie Rules Enforced*, TRUSTe Blog (Aug. 5, 2014), http://www.truste.com/blog/2014/08/05/eu-regulation-update-dutch-cookie-rules-enforced/ (noting that Spain took the lead on cookie law enforcement by fining two companies in 2013, and the Dutch had pursued two cases since then); Jennifer Baker, *French Privacy Cops Snarl at Websites Over Crap EU Cookie Warnings*, THE REGISTER (July 2, 2015), http://www.theregister.co.uk/2015/07/02/cnil_tells_20_french_websites_stop_tracking_users/ (reporting that France warned but did not fine twenty non-complying websites).

[132] CENTER FOR DEMOCRACY AND TECHNOLOGY, LOOKING BACK AT P3P: LESSONS FOR THE FUTURE 1 (2009), *available at* https://cdt.org/files/pdfs/P3P_Retro_Final_0.pdf.

[133] *Id.* at 2.

[134] ELECTRONIC PRIVACY INFORMATION CENTER, PRETTY POOR PRIVACY: AN ASSESSMENT OF P3P AND INTERNET PRIVACY (2000), *available at* https://epic.org/reports/prettypoorprivacy.html.

[135] *See id.*

would let the cookies through, since "Bogus Policy" was not on the browser's list of policies to block.[136] P3P's ineffectiveness led many to criticize it as a false attempt at self-regulation that merely served to put off actual regulation by Congress.[137] P3P was also criticized for being overly complex,[138] and it never gained a large amount of support from the public.

"Do Not Track" is a more recent effort at protecting users' privacy online, and it also has a notice element to it. All major browsers now have an option where the user can choose to ask all the websites they visit not to track them.[139] The FTC announced support for the program back in 2010, but even then the agency noted that it could not unilaterally mandate such a system.[140] As mentioned above in Part II, California passed a law requiring websites to disclose how they respond to these "Do Not Track" signals, so users can read websites' privacy policies to find out what companies do when they receive individuals' requests.[141] More likely than not, the website does nothing. Major websites like Google and Facebook ignore "Do Not Track" requests.[142] They claim it is unclear what the users really want (they probably want some cookies to be placed, lest they have to sign in again every time they want to check their Facebook newsfeed,) and it is not always clear that the browser is expressing the user's true preference, since some browsers have "Do Not Track" set as the default.[143] While there have been some news stories

---

[136] Lorrie Faith Cranor, *Internet Explorer Privacy Protections Also Being Circumvented by Google, Facebook, and Many More*, TECHNOLOGY | ACADEMICS | POLICY (Feb. 18, 2012), http://www.techpolicy.com/Cranor_InternetExplorerPrivacyProtectionsBeingCircumvented-by-Google.aspx.
[137] *See, e.g.*, ELECTRONIC PRIVACY INFORMATION CENTER, PRETTY POOR PRIVACY: AN ASSESSMENT OF P3P AND INTERNET PRIVACY, *supra* note 121.
[138] CENTER FOR DEMOCRACY AND TECHNOLOGY, LOOKING BACK AT P3P: LESSONS FOR THE FUTURE, *supra* note 119, at 8.
[139] Thorin Klosowski, *Everywhere You Can Enable "Do Not Track"*, LIFEHACKER (Aug. 5, 2013), http://lifehacker.com/everywhere-you-can-enable-do-not-track-1006138985.
[140] Edward Wyatt & Tanzina Vega, *F.T.C. Backs Plan to Honor Privacy of Online Users*, N.Y. TIMES (Dec. 1, 2010), http://www.nytimes.com/2010/12/02/business/media/02privacy.html.
[141] *See, e.g., CNN Privacy Statement, How We Respond to Do Not Track Signals*, http://www.cnn.com/privacy.
[142] Elise Ackerman, *Google and Facebook Ignore "Do Not Track" Requests, Claim They Confuse Consumers*, FORBES (Feb. 27, 2013), http://www.forbes.com/sites/eliseackerman/2013/02/27/big-internet-companies-struggle-over-proper-response-to-consumers-do-not-track-requests/.
[143] *Id.*

about companies not honoring "Do Not Track,"[144] as with P3P, there has been no wave of public outcry over the loss of a potentially valuable privacy mechanism.

AdChoices is likely the least effective privacy enhancing regime in effect today. In 2010, the Digital Advertising Alliance introduced a turquoise AdChoices triangle that could be placed in advertisements.[145] If users click the triangle, they are given the choice to opt out of behavioral tracking by many third parties.[146] However, very few consumers know what the triangle signifies or choose to click on it.[147] The system is flawed in that AdChoices works based on an "opt-out" cookie which will be deleted if the user deletes their cookies at some point, and even if they do not delete the cookie, they may still end up being tracked.[148]

B. Why Pursue A New Notice Regime?

The domestic regimes listed above share a few problems in common: companies' participation was not mandatory, public pressure was insufficient to force companies to participate, and the information provided to consumers was often unclear.

This is unfortunate, as notice has multiple benefits as a regulatory tool. First, if you can make your notice mechanism visible and easy to understand, you get consumers who are empowered to make informed choices. In some cases, consumers may feel they do not have much of a choice – if you want to be on a social network with your friends, you probably have to join Facebook. However, huge websites like Facebook will be constrained to an extent by media

---

[144] *See id.*, Elizabeth Dwoskin, *Yahoo Won't Honor 'Do Not Track' Requests From Users*, WALL STREET JOURNAL (May 2, 2014), http://blogs.wsj.com/digits/2014/05/02/yahoo-wont-honor-do-not-track-requests-from-users/.
[145] Tanzina Vega, *For Online Privacy, Click Here*, N.Y. TIMES (Jan. 19, 2012), http://www.nytimes.com/2012/01/20/business/media/the-push-for-online-privacy-advertising.html.
[146] *Id.*
[147] Lauren E. Willis, *Why Not Privacy by Default?,* 29 BERKELEY TECH. L.J. 61, 127 (2014); *see also* Alina Tugend, *Key to Opting Out of Personalized Ads, Hidden in Plain View*, N.Y. TIMES (Dec. 20, 2015), http://www.nytimes.com/2015/12/21/business/media/key-to-opting-out-of-personalized-ads-hidden-in-plain-view.html?_r=0.
[148] Cranor, *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, *supra* note 52, at 301.

coverage.[149] Lower profile websites like news outlets or travel search engines are relatively interchangeable, and therefore could be seriously affected by a mandatory notice and choice regime. Second, notice regimes discourage practices that are obviously objectionable from a privacy standpoint, because companies do not want to tell customers they engage in such practices. Even with the current lengthy and opaque privacy notices we have now, the FTC is able to catch companies who violate their own privacy policies.[150] Companies write privacy policies that restrict their own actions because they want to be able to reassure their customers that they do take some steps to protect their users' privacy.

Third, and most importantly, a notice regime can force companies to take more responsibility for what happens to individuals' data. California's law mandating privacy policies only requires that companies tell users what categories of personally identifiable information they collect, and what categories of companies they share that information with.[151] The law does not tell consumers *what happens to their data* once it is passed on to a third party. If a notice law mandated that companies must inform consumers what *uses* their data will be put towards, then companies could be forced to vet the third parties they share data with. They would need to make sure that the third parties were only using their customers' data for the uses specified in the company's privacy policy. Otherwise the company would be subject to the same sort of enforcement action the FTC conducts now against companies that break the promises in their

[149] Facebook has often been in the news because of its privacy practices, and often changed course when the public responded negatively. *See* Bobbie Johnson & Afua Hirsch, *Facebook Backtracks After Online Privacy Protest*, THE GUARDIAN (Feb. 18, 2009), http://www.theguardian.com/technology/2009/feb/19/facebook-personal-data; Reed Albergotti, *Facebook Changes Real-Name Policy After Uproar From Drag Queens*, Wall Street Journal (Oct. 2, 2014), http://www.wsj.com/articles/facebook-changes-real-name-policy-after-uproar-from-drag-queens-1412223040.

[150] *See, e.g.,* Elizabeth Dwoskin, *FTC Delivers Mixed Warning on Location-Tracking*, WALL STREET JOURNAL (Apr. 23, 2015), http://www.wsj.com/articles/ftc-delivers-mixed-warning-on-location-tracking-1429820925, Press Release, Federal Trade Commission, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises, *supra* note 75.

[151] Cal. Bus. & Prof. Code § 22575(b)(1).

privacy policies. Companies would in a sense be "trustees" for their customers' data:[152] they would be free to put people's personal information to a variety of commercial uses, as long as they take responsibility for what happens to it.[153] Third parties like data brokers would consequently be limited to selling individuals' information for only specific permitted purposes, instead of the current free-for-all.

In crafting the specifics of a notice and choice regime, it is important to consider the research that has been done on how privacy notices affect consumers. For example, if a website simply asks users what information they would like to share, users feel empowered and will actually share more information than in other scenarios where they are not given explicit control over sharing their information.[154] Consumers tend to narrowly focus on the act of sharing their data with one party, rather than thinking about who else might be able to access their data, or what their data might be used for later.[155] This narrow focus is another consequence of the intuition gap between the physical and online worlds. In the physical world, if you tell a friend a sensitive piece of information, the worst likely outcome is that your friend proves untrustworthy, and shares your sensitive information with other mutual friends. Therefore, it makes sense to

---

[152] For an interesting discussion of creating a trustee model to prevent "data abuse," *see* Benjamin Wittes & Wells C. Bennett, *Databuse and a Trusteeship Model of Consumer Protection in the Big Data Era*, BROOKINGS INSTITUTE (June 2014), http://www.brookings.edu/~/media/research/files/papers/2014/06/04-data-abuse-privacy-wittes-bennett/wittes-and-bennett_databuse.pdf.

[153] The 1995 Data Protection Directive ostensibly gives Europeans the right to know who is receiving their data and what their data is being used for, however, the right announced in the Directive has not led to the kind of robust enforcement that the FTC is capable of. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247, 309-10 (2011) (comparing the FTC's "entrepreneurial use of its enforcement power" with the relatively weak European enforcement agencies, and noting the surprising lack of initiative shown by European privacy advocacy organizations in utilizing the Directive's protections). *See also* EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, DATA PROTECTION IN THE EUROPEAN UNION: THE ROLE OF NATIONAL DATA PROTECTION AUTHORITIES 6 (2010), *available at* http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf, (noting that in many EU countries, prosecutions for violations of the data protection laws are limited or non-existent).

[154] Eoin Carolan & M. Rosario Castillo-Mayen, *Why More User Control Does Not Mean More User Privacy: An Empirical (and Counter-Intuitive) Assessment of European E-Privacy Laws*, 19 VA. J.L. & TECH. 324, 326 (2015).

[155] Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox*, SOCIAL PSYCHOLOGICAL AND PERSONALITY SCIENCE 4 (2012).

focus on the moment you share your information with your friend – that is the one moment you can control, and the privacy risks are obvious and tied to that moment. However, sharing your information online contains hidden privacy risks, which are tied to unknown individuals accessing your information later. When you share sensitive information online, the worst outcome could be that countless corporations you are unaware of later buy and sell your information, and possibly even discriminate against you because of it. This is a far worse outcome than the average consumer is intuitively aware of when sharing information online. A new notice and choice regime must focus on closing the intuition gap, so that consumers will be encouraged to exercise control over how other companies may access and use their data in the future.

Instead of a notice and choice regime, some commentators might advocate for outright prohibitions on certain practices, or prefer an opt-in only regime for tracking.[156] There are areas where we do not allow consumers to make certain choices, because the government makes a policy judgment that the harm is just too great. For example, you cannot buy very cheap but slightly rancid meat in a supermarket. The government will not allow you to make that bargain. There are arguably bargains that people should not be able to make with their data either. A data bargain may be egregiously bad (i.e. a cookie I can never delete in exchange for reading a single news article), or we may wish to protect the wide swaths of people who would ignore even an incredibly well-designed notice regime to consistently make mediocre bargains for their data.

I would personally like to see certain data practices outlawed. For example, I do not think companies should be able to use purchasing data to make medical assessments about their

[156] 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, 734-35 (2013).

customers, such as Target using algorithms to figure out which of their customers is pregnant.[157] I do not think a website that deliberately solicits self-incriminating legal information (such as OKCupid asking if you do illegal drugs)[158] should be able to share that information with any third parties. However, these are my own personal policy preferences. I have no way of knowing if a poor young pregnant woman who could really use some coupons for baby clothes would mind terribly that Target analyzed her data to determine she was pregnant to send her those coupons. As noted in Part I, individuals are quite inconsistent in how they respond to surveys about privacy.[159] Because current data practices are so opaque to consumers, we have no way of knowing what trade-offs they might be willing to make. Nearly costless actions like turning on the "Do Not Track" signal or occasionally deleting cookies do not tell us how consumers would react to options that both actually stopped tracking and have real costs.

One final benefit to a notice and choice regime is that it can provide companies and policy makers with data points on how much consumers really value privacy. In Dr. Cranor's experiment, where consumers could see how protective online sellers were of their privacy before they bought an item, individuals changed their behavior based on the privacy notices.[160] Rather than a lengthy privacy notice tucked away on a website, her experiment gave users notice right in their search engine, in an easy-to-comprehend privacy meter next to the seller's links.[161] There were four boxes, and if the boxes were all green, the site was very protective of privacy, and if they were all white, the site was not at all protective of the user's privacy.[162] An effective notice regime like that, which successfully gives consumers an immediate sense of how a

[157] Duhigg, *supra* note 12.
[158] Zwerdling, *supra* note 3.
[159] *See See, e.g.,* Tene & Polonetsky, *supra* note 37, at 64.
[160] Cranor, *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, *supra* note 52, at 292-93.
[161] Lorrie Faith Cranor, *Understanding Users*, CARNEGIE MELLON UNIVERSITY CYLAB (June 2014), https://www.cylab.cmu.edu/news_events/events/fopnac/pdfs/cranor-slides.pdf.
[162] *Id.* at 6.

website treats their data, produces useable data about how much more consumers will pay for privacy. Once we acquire such data on a large scale, we can start to intelligently craft policies where some uses of personal information may be prohibited or strictly regulated.

C. The Outlines of a Mandatory Notice and Choice Regime

The Obama Administration has proposed a Consumer Privacy Bill of Rights that would give consumers notice about what information a website or app collects about them, and what they do with that information.[163] However, this proposal has been attacked by privacy advocates and the head of the FTC's Bureau of Consumer Protection for being full of loopholes and allowing companies to police themselves.[164] To overcome the shortcomings of the previous notice regimes, a new regime must be mandatory, strictly enforced by the FTC, and provide clear information to consumers. The first step is for Congress to pass a statute that requires all companies that collect consumer data via the internet (be it a website, app, or part of the "internet of things"[165]) to publish a privacy policy. Going beyond California's law, regulatory authority must be given to the FTC to craft a uniform machine-readable policy for all companies to use.[166] Policies need to detail what data the company collects, what the company uses individuals'

---

[163] ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015, *available at* https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

[164] Elizabeth Dwoskin, *Consumer Protection Official Blasts White House Privacy Proposal*, Wall Street Journal (Mar. 9, 2015), http://blogs.wsj.com/digits/2015/03/09/federal-consumer-protection-official-blasts-white-house-privacy-proposal/.

[165] More and more household appliances are connected to the internet for convenient remote control, energy efficiency, and numerous other purposes. *See In the Privacy of Your Own Home*, CONSUMER REPORTS (Apr. 30, 2015), http://www.consumerreports.org/cro/magazine/2015/06/connected-devices-and-privacy/index.htm. For any item that collects your data and transmits it outside your home, the item's privacy policy could be published on its packaging, with emails sent to the consumer if the policy changes at a later date.

[166] There is a potential First Amendment issue here, but the government is at minimum able to compel commercial speech when it is purely factual and uncontroversial, and appropriate to prevent deception. Zauderer v. Office of Disciplinary Counsel of Supreme Court of Ohio, 471 U.S. 626, 651 (1985). Privacy notices arguably fall under "preventing deception," but the D.C. Circuit also has held that other substantial interests besides combatting deception could also justify compelled commercial speech. Am. Meat Inst. v. U.S. Dep't of Agric., 760 F.3d 18, 27 (D.C. Cir. 2014). I believe protecting Americans' personally identifiable information is clearly a substantial government interest.

personal information for, and any third party uses of customers' data. Companies that violate their own policies, intentionally or unintentionally (by sharing data with an unreliable third party) must be subject to enforcement actions. A negligence standard should be put in place where if a company vetted a third party, contracted to share data with them for a certain purpose, and the third party violated the agreement by using the data for another purpose, then the FTC would have to pursue that third party. However, if a company agreed to share data under a vague contract, or with a fly-by-night third party who was obviously not a legitimate business, the primary company would be on the hook for the violation.

In designing a uniform privacy policy, simplicity is vital. Consumers cannot be expected to spend time reading detailed policies. They need an easy way to comprehend and compare policies. Dr. Cranor has come up with an excellent model for privacy notices: nutrition labels.[167] A graphic is available in the previous footnote, but essentially the format is a grid, with "information we collect" along the vertical axis, and "ways we use your information" along the horizontal axis. Each box in the grid represents a particular type of data, and a particular use of that data, such as "contact information" for "marketing purposes." Categories under "information we collect" include "demographic information" and "health information." Categories under "ways we use your information" include "provide service and maintain site" and "profiling." The precise categories could be tweaked, and designed to provide more detailed information when the user hovers over or clicks on each category. Each box may be red, to indicate that the company collects and uses your information for a given purpose, or white to indicate they do not.

After the "ways we use your information" categories, Dr. Cranor has an additional section called "Information sharing" that I would title "ways other companies can use your information." Such categories could include specific uses such as "targeted advertising" and

[167] Lorrie Faith Cranor, *Understanding Users*, *supra* note 145, at 7.

"background checks." The categories should be worded in such a way that is not negatively slanted,[168] but also makes clear exactly what may be done with your data. The number of categories would need to be limited to ensure that the grid does not become impossible to take in at a glance. Even if the consumer does not read all of the category names, however, they would still be able to get a general sense of the privacy policy of the site by immediately noticing if the grid is predominantly red or predominantly white. Since every website and app would have the same grid, consumers would become faster at reading the grid if they looked up different private policies over time.

In most instances, consumers would not even need to view the privacy grid. By having a mandatory machine-readable policy, the system could work the way P3P was meant to: with the user inputting their privacy preferences into their browsers one time, and their browsers then looking at the policy for every site.[169] With every website forced to participate and fill out the same grid, there would not be the same loopholes there were with P3P, where companies could provide bogus policies. Users could simply fill in their own grids, and choose to only visit sites that match their preferences. There is a question of what the browser should do when the user tries to visit a site that does not match their privacy settings. The browser could be set to block the site entirely, or to provide a pop-up to warn users what aspect of their privacy settings the site does not adhere to, and let them click "OK" to visit the site anyway. For many webpages, the pop-up could also offer the user one or two alternative webpages that are very similar to the one the user was planning to visit. If I am searching for some news item on Google, it is rare that I

[168] It would be a First Amendment problem to compel commercial speech that is not "purely factual." *See* Zauderer v. Office of Disciplinary Counsel of Supreme Court of Ohio, 471 U.S. 626, 651, 105 S. Ct. 2265, 2281, 85 L. Ed. 2d 652 (1985).

[169] For apps, users could set their preferences in their smart phones, and the phone could read the privacy policy of any app they buy. For the "internet of things," consumers would need to glance themselves at the privacy grid on the item's packaging, which should be a lesser burden considering the relative infrequency of buying new appliances vs. buying new apps or visiting new websites.

see a link and think "this is the single article that covers the news story I was searching for." One search result is often as good as another, and users may not mind going to a different page with a single click.

There is also no reason users should have to set their own detailed privacy preferences if they do not wish to. Browsers could offer simple "low," "medium," and "high" privacy settings, or trusted organizations like the ACLU could sponsor plug-ins that choose certain settings for the user, based on what data uses the ACLU believes are the most harmful.

If consumers are dissatisfied with the number of pop-up warnings they are getting, they could obviously choose a less-stringent privacy setting, but they could also opt to receive notice at an earlier stage in the process. Google could offer a plug-in that shows a website's privacy rating right next to the search result, as in Dr. Cranor's custom search engine. That way individuals could select a relatively privacy-friendly result at the outset, rather than risk dealing with a pop-up.

IV. CONCLUSION

Americans should not have to settle for "creepy" or unfair privacy practices. We should not have to feel perpetually uneasy about what our personal information is being used for. The above notice and choice regime significantly empowers consumers. If we force companies to disclose precisely what they do, and what they enable third parties to do with their customers' data, they will engage in more privacy-protective practices to avoid "spooking" their customers. Journalists will report on major companies whose grids are a sea of red. Consumers will change companies' behavior by reacting to what the privacy grids reveal. Exposure works: when Instagram announced it was changing its terms of service in such a way that enabled it to sell

users' photos, there was a massive outcry and Instagram had to hastily reverse itself.[170] Consumers have the power to change the way companies handle their data. They just need to know about it first.

[170] Craig Timberg, *Instagram Outrage Reveals a Powerful But Unaware Web Community*, WASH. POST (Dec. 21, 2012), http://www.washingtonpost.com/business/technology/instagram-outrage-reveals-a-powerful-but-unaware-web-community/2012/12/21/b387e828-4b7a-11e2-b709-667035ff9029_story.html.