Yale Journal of Law and Technology

Volume 16
Issue 1 *Yale Journal of Law and Technology*

Article 2

2014

A Theory of Creepy: Technology, Privacy, and Shifting Social Norms

Omer Tene
Rishon Le Zion, Israel

Jules Polonetsky

Recommended Citation

Tene, Omer and Polonetsky, Jules (2014) "A Theory of Creepy: Technology, Privacy, and Shifting Social Norms," *Yale Journal of Law and Technology*: Vol. 16: Iss. 1, Article 2.
Available at: http://digitalcommons.law.yale.edu/yjolt/vol16/iss1/2

A THEORY OF CREEPY: TECHNOLOGY, PRIVACY AND SHIFTING SOCIAL NORMS

Omer Tene and Jules Polonetsky[*]

16 YALE J.L. & TECH. 59 (2013)

I. INTRODUCTION 59
II. WHAT'S CREEPY? 61
A. Ambient social apps 61
B. Social listening 63
C. Personalized analytics 65
D. Data-driven marketing 66
E. New product launches 69
III. THE SHORTCOMINGS OF LAW 71
IV. DRIVERS FOR CHANGE 76
A. Business drivers 77
B. Technological drivers 78
C. Individual drivers 79
V. HOW TO AVOID CREEP 82
A. Against technological determinism 83
B. Against privacy lurch 87
C. Against targeting the superuser 92
D. For turning on the light 94
E. For the golden rule 99
VI. CONCLUSION 100

I. INTRODUCTION

The rapid evolution of digital technologies has hurled dense social and ethical dilemmas that we have hardly begun to map or understand to the forefront of public and legal discourse. In the near past, community norms helped guide a clear sense of ethical boundaries with respect to privacy. We all knew, for example, that one should not peek into the window of a house even if it were left open, nor hire a private detective to investigate a casual date or the social life of a prospective employee.

[*] Omer Tene is Vice Dean of the College of Management School of Law, Rishon Le Zion, Israel; Affiliate Scholar at the Stanford Center for Internet and Society; and Senior Fellow at the Future of Privacy Forum. Jules Polonetsky is Co-chair and Executive Director of the Future of Privacy Forum. The authors would like to thank the participants in the Privacy Law Scholars Conference sessions devoted to discussion of this article.

Yet with technological innovation rapidly driving new models for business and inviting new types of socialization, we often have nothing more than a fleeting intuition as to what is right or wrong. Our intuition may suggest that it is responsible to investigate the driving record of the nanny who drives our child to school, since such tools are now readily available.[1] But is it also acceptable to seek out the records of other parents in our child's car pool, or of a date who picks us up by car?

Alas, intuitions and perceptions of how our social values should align with our technological capabilities are highly subjective. And, as new technologies strain our social norms, a shared understanding of that alignment is even more difficult to capture. The word "creepy" has become something of a term of art in privacy policy to denote situations where the two do not line up.

This article presents a set of social and legal considerations to help individuals, engineers, businesses, and policymakers navigate a world of new technologies and evolving social norms. For businesses that make money by leveraging newly available data sources, it is critical to operationalize these subjective notions into coherent business and policy strategies. These considerations revolve around concepts that we have explored in prior work, including enhanced transparency and the elusive principle of context.[2]

The first part of this article provides examples of new technologies and services that grate against social norms, often resulting in negative public response and allegations of creepiness. The second part discusses the progressively short timeframes available for society—and the law—to react to technological innovation. The third part disentangles the three main drivers of techno-social chaos[3]—businesses, technologies and individuals—but also discusses how they work together to produce the current rupture in social fabric and must each be engaged to make change. The fourth part briefly lays out the highly-charged political environment in which the discussion around privacy takes place, with business groups accusing regulators and competitors of a ploy to destroy innovation, and consumer advocates conjuring specters of a surveillance culture that will end civil society as we know it. The fifth part sets forth several strategies for avoiding creepiness without dampening innovation: it warrants against

[1] *E.g.*, Been Verified, http://www.beenverified.com (last visited Jan. 20, 2014).

[2] Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW J. TECH. & INTELL. PROP. 239 (2013).

[3] We use "techno-social chaos" to refer to the tight and often strained interaction between technological developments and social norms.

technological determinism; suggests that businesses avoid privacy lurch;[4] cautions against targeting the superuser in both products and regulations; advocates for transparency; and, finally, puts a burden on individuals to consider the ages-old golden rule when engaging online.

II. WHAT'S CREEPY?

There seem to be several categories of corporate behavior that customers and commentators have begun to label "creepy" for lack of a better word. These behaviors rarely breach any of the recognized principles of privacy and data protection law. They include activity that is not exactly harmful, does not circumvent privacy settings, and does not technically exceed the purposes for which data were collected. They usually involve either the deployment of a new technology, such as a feature that eliminates obscurity, or a new use of an existing technology, such as an unexpected data use or customization. In certain cases, creepy behavior pushes against traditional social norms; in others, it exposes a rift between the norms of engineers and marketing professionals and those of the public at large; and, in yet others, social norms have yet to evolve to mediate a novel situation.

In this section, we provide examples of business models and activities that have earned companies the unenviable label of creepy.

A. Ambient social apps

Consider the growing field of ambient social apps, technologies that use mobile devices' location awareness to help users obtain information about people around them.[5] With ambient apps, users can get a notification when a friend is near, learn basic information about other people in a bar or at a conference, or post messages into the air for people around them to answer (*e.g.*, "How long is the queue to get on the Eiffel Tower?"; "Is anyone driving back to Palo Alto after the meeting?").

An app called Highlight,[6] for example, detects other users in a user's vicinity and shows their profiles on his or her phone. Users can see each

[4] James Grimmelmann coined the term "privacy lurch" to denote an unexpected change in corporate data practices causing a sense of enhanced privacy risk. *Saving Facebook*, 94 IOWA L. REV. 1137 (2009). Paul Ohm expanded the concept. *See Branding Privacy*, 97 MINN. L. REV. 908 (2013).

[5] Mark Sullivan, *SXSW Preview: The Year of 'Ambient Social' Apps?*, PC WORLD (Mar. 7, 2012), http://www.pcworld.com/article/251455/sxsw_preview_the_year_of_ambient_social_apps_.html.

[6] HIGHLIGHT, http://highlig.ht/about.html (last visited Nov. 19, 2013).

other's names and photos, as well as things they have in common, such as mutual friends or favorite rock bands or TV shows. Highlight can notify a user when people that he does or does not want to run into are nearby. Users can "highlight" other users to show that they are interested in meeting them, and in turn may be "highlighted" back. Banjo,[7] another ambient social app, connects to users' Facebook, Twitter, and Foursquare accounts to send them push notifications when a friend is within a given radius or in a location they specified (such as a rock concert or university campus).[8]

At their core, ambient social apps are passive, drawing information from publicly available sources to create ad-hoc geographical communities. However, in 2012, an app called "Girls Around Me"[9] caused a privacy commotion. The app mapped and disclosed the location and information of "girls" around each user who checked-in through their social networks in that user's vicinity. Critics viewed Girls Around Me as creepy, leading major social networks to remove it from their APIs and ultimately causing its demise.[10] Yet the app did not violate any privacy settings or surface data that was not otherwise publicly available. It simply put data in a context that seemed creepy to some. It was not illegal; it was distasteful.

A new generation of technologies will push boundaries even further. Already, engineers are using ambient light, accelerometers, Wi-Fi or cell tower signal strength, and more to enable mobile devices and third parties to learn where a device is located and what its owner is doing. For example, Color (now defunct pursuant to an acquisition by Apple),[11] a social networking app, which allowed users in the same location to share photos with each other, was reported to turn on the microphone on users' phones in order to let Color users know when another user was in the same room. The app combined the data on ambient noise with color and lighting information from users' cameras "to figure out who's inside, who's outside, who's in one room, and who's in another, so the app can auto-generate spontaneous

[7] BANJO, http://ban.jo (last visited Nov. 19, 2013).

[8] Sarah Perez, *Creepy/Awesome Banjo App Now Pings You When Your Friends Are Nearby*, TECHCRUNCH (Oct. 27, 2011), http://techcrunch.com/2011/10/27/creepyawesome-banjo-app-now-pings-you-when-your-friends-are-nearby.

[9] GIRLS AROUND ME, http://girlsaround.me (last visited Nov. 19, 2013).

[10] Damon Poeter, *Creepy 'Girls Around Me' App Delivers a Privacy Wake-Up Call*, PC MAG (Mar. 30, 2012), http://www.pcmag.com/article2/0,2817,2402457,00.asp.

[11] Color failed to attract a sufficient number of users. *See* Nicholas Carlson, *A Year Later, $41 Million Startup Color Has A Pathetic 30,000 Daily Users*, BUSINESS INSIDER (Mar. 26, 2012), http://www.businessinsider.com/a-year-later-41-million-startup-color-has-30000-daily-users-2012-3; Jenna Wortham, *Color App, Symbol of Silicon Valley Excess, Will Fade Away*, N.Y. TIMES (Nov. 20, 2012), http://bits.blogs.nytimes.com/2012/11/20/color-app-symbol-of-silicon-valley-excess-will-fade-away.

temporary social networks of people who are sharing the same experience."[12] WiFiSLAM, a start-up company recently purchased by Apple, is reported to have developed an indoor navigating service using not just Wi-Fi trilateration, but also a phone's gyroscope, magnetometer, and accelerometers to detect walking speed, turns, and angles.[13] While these new technologies provide valuable innovative services, they also stretch existing social norms about privacy in public and private spaces and therefore challenge traditional perceptions of privacy.

B. Social listening

Social listening—the analysis of social media content to understand user sentiments, improve customer service, and develop early crisis warning—has become a key part of companies' social media and marketing strategies.[14] It allows companies to identify new trends, understand customer needs and complaints, improve services and customer satisfaction, and avert crises. While these goals appear to be beneficial, some companies are seeking to push the boundaries even further, using social listening for purposes like determining individuals' credit risks and setting their loan interest rates.[15]

Even when social listening has clear benefits for consumers, the practice challenges social norms. Imagine being in a private space and calling a friend to tell him about the trouble you are having with your TV, only to have a stranger unexpectedly chime in to explain how to fix the problem. You would likely be startled and view this behavior as creepy, even if it might help you.

A thin line separates legitimate social listening from creepy intrusions into personal communications. The practice grates against two distinct social norms. First, when and to what extent is it acceptable for a

[12] Mike Elgan, *Snooping: It's Not a Crime, It's a Feature*, COMPUTERWORLD (Apr. 16, 2011), http://www.computerworld.com/s/article/print/9215853/Snooping_It_s_not_a_crime_it_s_a_feature.

[13] Matthew Panzarino, *What Exactly WiFiSLAM Is, and Why Apple Acquired It*, THE NEXT WEB (Mar. 26, 2013), http://thenextweb.com/apple/2013/03/26/what-exactly-wifislam-is-and-why-apple-acquired-it.

[14] *See, e.g.*, Marshall Sponder, SOCIAL MEDIA ANALYTICS: EFFECTIVE TOOLS FOR BUILDING, INTERPRETING, AND USING METRICS (McGraw-Hill 2011); Stephen Rappaport, LISTEN FIRST!: TURNING SOCIAL MEDIA CONVERSATIONS INTO BUSINESS ADVANTAGE (Wiley 2011).

[15] *Stat Oil: Lenders Are Turning to Social Media to Assess Borrowers*, THE ECONOMIST (Feb. 9, 2013), http://www.economist.com/news/finance-and-economics/21571468-lenders-are-turning-social-media-assess-borrowers-stat-oil.

company to survey people's conversations? A company scanning publicly posted information to create aggregated reports is considered a commonplace practice. Many companies seek reports on views expressed by social influencers (usually individuals with many followers on Twitter) or by their own customers.

But at what point does social listening become social stalking? British Airways, for example, was castigated for its "Know Me" program, which was intended to provide a more personalized service to frequent fliers and involved airline personnel googling passengers to learn more about them.[16] "Since when has buying a flight ticket meant giving your airline permission to start hunting for information about you on the Internet?" one consumer advocate exclaimed.[17]

Second, when can a company legitimately interject in consumers' online conversations to offer responses or solutions to reported issues? On the one hand, unsatisfied customers would like for the company to handle their complaints and solve their problems promptly; on the other hand, some may find corporate (active or passive) participation in their discussions creepy.

According to a study comprised of surveys of more than 1,000 customers, consumers have a double standard for social listening. Consumer sentiment seems to be along the lines of "listening is intrusive, except when it's not."[18] According to this study, more than half of consumers (51%) want to be able to talk about companies without them listening and 43% think that corporate listening intrudes on their privacy. Yet 48% would allow companies to listen if the goal were to improve products and services. And 58% of consumers believe that businesses should respond to complaints in social media, while 64% want companies to speak to them only when spoken to.[19]

Hence, perceptions of social-media-based customer service are clearly ambivalent. The survey tells us that companies get credit for being responsive to consumer sentiment, but at the same time more than half of customers feel corporate response is creepy and prefer being able to just

[16] Tim Hume, *BA Googles Passengers: Friendlier Flights or Invasion of Privacy?*, CNN (Aug. 22, 2012), http://edition.cnn.com/2012/08/22/travel/ba-google-image-passengers.

[17] *Id.*

[18] Brian Solis, *Are Businesses Invading Consumer Privacy By Listening to Social Media Conversations?*, BRIAN SOLIS BLOG (Feb. 25, 2013), http://www.briansolis.com/2013/02/are-businesses-invading-consumer-privacy-by-listening-to-social-media-conversations.

[19] *Id.*; for the original study, see Netbase & J.D. Power, *Social Listening v. Digital Privacy* (Feb. 12, 2013), http://www.slideshare.net/secret/NqlMQFvbATIfLX (presentation summarizing results).

vent. More complicated yet, social norms around interjecting in a conversation are highly contextual and culture-specific. In the U.S., for example, fans in a sporting match volunteer their opinions and views to one another in a manner uncustomary for spectators at Wimbledon. In Israel, diners in a restaurant freely exchange political views with diners at a nearby table without being considered rude.[20] Online, businesses must contend with a global audience and find a way to deal with various cultures' social norms when determining their policy on social listening.

C. Personalized analytics

Not only social networking services tread the thin line between cool and creepy. Consider personalized analytics, the use of simple data mining and analysis apps by individuals in their daily lives. Few people go to a job interview, business meeting or date these days without first looking their counterparts up on Google. Yet is it socially acceptable to google a person in front of him or her? Zillow is a leading online real estate marketplace,[21] helping homeowners, buyers, sellers, renters, and agents find and share information about homes, real estate, and mortgages. Using that information for that purpose seems fine, but is it appropriate to use Zillow to explore the value of your neighbor's house? Similarly, is it legitimate to run online background checks on the parents of your children's play dates or carpool?

Consider PowerCloud Systems' Skydog, a Wi-Fi router and mobile companion site that lets parents monitor Internet access and even receive text notifications for certain network activity in their home.[22] Parents can scrutinize all of the devices connected in their home through a dashboard on their desktop or mobile device; review detailed information about who is online, which devices are connected, which websites are being accessed and what the bandwidth usage is; and even assign priority bandwidth access or limit use of a specific site (*e.g.*, Facebook) to 30 minutes a day. While parental controls of children's browsing habits are not new and serve important social goals, the privatization of surveillance technologies may be cause for concern. In the past, adolescents could shut the door to their room and enjoy relative autonomy and privacy from their parents' gaze. Given

[20] For cultural nuance surrounding perceptions of privacy, see Omer Tene, *Privacy in Europe and the United States: I Know It When I See It*, CDT BLOG (Jun. 27, 2011), https://www.cdt.org/blogs/privacy-europe-and-united-states-i-know-it-when-i-see-it.

[21] ZILLOW, http://www.zillow.com (last visited Nov. 19, 2013).

[22] Vignesh Ramachandran, *Skydog Lets You Remotely Monitor Your Kids' Internet and Facebook Use*, MASHABLE (May 3, 2013), http://mashable.com/2013/05/02/skydog-monitor-internet-usage.

today's state of technology, what social norms constrain parents from persistently peering into their children's lives?

In the months leading to the 2012 U.S. Presidential elections, the Obama campaign unleashed an app called "Obama for America," to help users identify Democratic households, which were denoted by little blue flags placed on a map.[23] While helping campaign operatives canvas and energize the voter base, the app also allowed users to find out the political affiliation of their neighbors. Interviewed about the app, one voter said: "I do think it's something useful for them, but it's also creepy . . . My neighbors across the street can know that I'm a Democrat. I'm not sure I like that."[24]

D. Data-driven marketing

Another area ripe with ethical ambiguity due to the expansion of big data[25] analysis capabilities is marketing. In February 2012, the *New York Times Magazine* ran a cover story uncovering the data-crunching operations of retail giant Target.[26] The *New York Times* discovered that Target assigns customers a pregnancy prediction score, which is based on their purchase habits, in order to beat its competitors in identifying a precious moment when shopping habits are most amenable to change—the birth of a baby.[27] According to the *New York Times,* Target employed statisticians to sift through buying records of women who had signed up for baby registries. The statisticians discovered latent patterns, such as women's preference for unscented lotion around the beginning of their second trimester or a tendency to buy supplements like calcium, magnesium, and zinc within the first 20 weeks of a pregnancy. They were able to determine a set of products

[23] Lois Beckett, *Is Your Neighbor a Democrat? Obama Has an App for That*, ProPublica (Aug. 3, 2012), http://www.propublica.org/article/is-your-neighbor-a-democrat-obama-has-an-app-for-that.

[24] *Id.*

[25] Big data comprises new tools for analyzing disparate information sets, which have revolutionized our ability to find signals amongst the noise. Big data techniques hold promise for breakthroughs ranging from better health care, a cleaner environment, safer cities, and more effective marketing. Yet, privacy advocates are concerned that the same advances will upend the power relationships between government, business, and individuals, and lead to prosecutorial abuse, racial or other profiling, discrimination, redlining, overcriminalization, and other restricted freedoms. *See generally*, Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 STAN. L. REV. ONLINE 25 (2013).

[26] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAGAZINE, Feb. 16, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[27] *Id.*

that, when grouped together, allowed Target to accurately predict a customer's pregnancy and even her due date. In one case, the *New York Times* reported that a father of a teenage girl stormed into a Target store to complain that his daughter received coupons and advertisements for baby products. A few days later, he called the store manager to apologize, admitting that, "There's been some activities in my house I haven't been completely aware of. She's due in August."[28]

Target did not have to wait for the story to come out to recognize the potentially creepy nature of its actions. It chose to purposefully disguise its knowledge of a customer's pregnancy by burying pregnancy-related advertisements among other unrelated ads. The *New York Times* quoted a former Target employee:

> If we send someone a catalog and say, 'Congratulations on your first child!' and they've never told us they're pregnant, that's going to make some people uncomfortable . . . We are very conservative about compliance with all privacy laws. But even if you're following the law, you can do things where people get queasy. . . . [W]e started mixing in all these ads for things we knew pregnant women would never buy, so the baby ads looked random. We'd put an ad for a lawn mower next to diapers. We'd put a coupon for wineglasses next to infant clothes. That way, it looked like all the products were chosen by chance. And we found out that as long as a pregnant woman thinks she hasn't been spied on, she'll use the coupons. She just assumes that everyone else on her block got the same mailer for diapers and cribs. As long as we don't spook her, it works.[29]

Public opinion censured Target's covert marketing operation.[30] Yet upon deeper reflection, it may become less obvious why marketing to pregnant women is legitimate in one context (*e.g.*, based on subscription to a magazine) but morally distasteful in another (*e.g.*, compiling shoppers' pregnancy prediction score). Is it the sensitive nature of the information

[28] *Id.*

[29] *Id.*

[30] *See, e.g.*, Matt Stanford, *Brilliantly Creepy: Marketing Technology and Your Privacy*, EXPERTS-EXCHANGE (Feb. 21, 2012), http://blog.experts-exchange.com/ee-tech-news/brilliantly-creepy-marketing-technology-your-privacy; *see also* Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012), http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did.

collected by Target? (But notice that the collected information was rather innocuous; it was the *lessons learned* that were sensitive.) Or the novel, unexpected use of existing information?

Another marketing strategy, which has been wrought with controversy, is online behavioral advertising (OBA), that is, the tracking of individuals' online activities in order to deliver tailored advertising.[31] On the one hand, consumers appreciate the immense value of obtaining high-quality content and cutting-edge new services without charge; on the other hand, some view OBA as privacy invasive and "find the idea smart but creepy."[32]

We argue that, in OBA and elsewhere, it is *unexpected* uses of data that are prone to a privacy backlash. One example is price discrimination, that is the offering of different prices to different people based on their perceived willingness to pay.[33] In certain contexts, such as airfare or gasoline prices, price discrimination is considered a legitimate marketing tactic.[34] Yet last year, online travel agent Orbitz was publicly reprimanded for tailoring high-end travel deals to Mac users.[35] One commentator thought that the Orbitz practices demonstrate that marketing is "getting too creepy."[36] Had Amazon engaged in similar customization, tailoring deals to consumers based on their previous purchase history, few consumers would have been surprised, given the giant retailer's clear messaging, user-friendly

[31] FTC, *Self-Regulatory Principles for Online Behavioral Advertising* (2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf; ART. 29 WORKING PARTY, *Opinion 2/2010 on Online Behavioral Advertising (WP 171)* (June 22, 2010), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp171_en.pdf.

[32] Blase Ur et al., *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising* (Jul. 13, 2012), https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12007.pdf.

[33] Omer Tene & Jules Polonetsky, *Judged by the Tin Man: Individual Rights in the Age of Big Data*, ___ J. TELECOM. HIGH TECH. L. ___ (forthcoming 2013) (manuscript at 4-6).

[34] The classic exposition is Richard Schmalensee, *Output and Welfare Implications of Monopolistic Third-Degree Price Discrimination*, 71 AM. ECON. REV. 242 (1981); *see also* Hal Varian, *Price Discrimination and Social Welfare*, 75 AM. ECON. REV. 870 (1985); and in the online context, see Andrew Odlyzko, *Privacy, Economics, and Price Discrimination on the Internet*, (Jul. 7, 2003), http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf; Arvind Narayanan, *Price Discrimination is All Around You*, 33 BITS OF ENTROPY (Jun. 2, 2011), http://33bits.org/2011/06/02/price-discrimination-is-all-around-you.

[35] Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, WALL ST. J. (Aug. 23, 2012), http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html.

[36] Corey Eridon, *Is Marketing Getting Too Creepy?*, HUBSPOT BLOG (Jun. 29, 2012), http://blog.hubspot.com/blog/tabid/6307/bid/33332/Is-Marketing-Getting-Too-Creepy.aspx.

interface, and general brand recognition for targeted marketing. But Orbitz failed to set the tone for its customized sales pitch—and this led consumers to react negatively to its well-intentioned attempt at tailoring a travel package to them.[37]

Companies are increasingly harnessing new technologies to expand tracking for data-driven analytics into the physical world. New tech companies provide retailers with shopper location analytics derived from tracking the movements of cellphones through stores.[38] SceneTap sets up cameras in bars to determine the aggregate age range and gender of a venue's patrons. Digital signage providers place in-store signs that include cameras and have the ability to assess the age range and gender of a shopper standing in front of them in order to deliver instantly targeted advertisements based on their demographic characteristics.[39] Some consumers may view the resulting customization of the shopping experience as "cool," while others will be intimidated by the Minority Report-like surveillance of their offline habits.[40]

E. New product launches

Any innovative technology or new product launch is especially prone to a creepy privacy lurch.[41] Consider the recently unveiled Google

[37] *See* Jennifer Valentino-Devries, Jeremy Singer-Vine & Ashkan Soltani, *Websites Vary Prices, Deals Based on Users' Information*, WALL ST. J. (Dec. 24, 2012), http://online.wsj.com/article/SB10001424127887323777204578189391813881534.html (negative sentiment directed at online retailers who deploy geographically based price discrimination based on users' browsing habits). According to researchers at the University of Pennsylvania, 87% of American adults disagree that "it's OK if an online store I use charges people different prices for the same products during the same hour." *See* Joseph Turow, Lauren Feldmany & Kimberly Meltzerz, *Open to Exploitation: America's Shoppers Online and Offline*, ANNENBERG SCH. FOR COMM'N DEPARTMENTAL PAPERS (ASC) (2005), http://repository.upenn.edu/cgi/viewcontent.cgi?article=1035&context=asc_papers.

[38] Quentin Hardy, *Technology Turns to Tracking People Offline*, N.Y. TIMES (Mar. 7, 2013), http://bits.blogs.nytimes.com/2013/03/07/technology-turns-to-tracking-people-offline; Christopher Matthews, *Private Eyes: Are Retailers Watching Our Every Move?*, TIME, September 18, 2012, http://business.time.com/2012/09/18/private-eyes-are-retailers-watching-our-every-move.

[39] FTC, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, http://www.ftc.gov/reports/facialrecognition/p115406commissionfacialrecognitiontechnologiesrpt.pdf (last visited Nov. 19, 2013).

[40] Tom Warren, *Intel's Creepy Face-Tracking Takes Cues From 'Minority Report' Ads (Hands-on)*, THE VERGE (Feb. 27, 2013), http://www.theverge.com/2013/2/27/4035428/intel-webcam-tv-face-tracking-hands-on.

[41] *See supra* note 4.

Glass, a wearable computer with a head-mounted display—in the form of glasses—which allows the user to use the Internet through a natural language voice recognition interface.[42] Google Glass is designed to let users search as they walk; navigate; record what they see in real time and share it with their friends; translate signs and texts they see; and much more.

Users, who have yet to figure out which pictures to share on Facebook or how to make sure they do not tweet while drunk, are now required to navigate a whole new map of social rules.[43] Should you take off your Google Glass in a public restroom, lest other visitors think you are recording? Is it acceptable to google someone while speaking to them? Should one ask, "Mind if I post the conversation we just had online, I think our friends would love to comment on it?"[44] In this case, the potential lurch threatens the privacy not of the early new product adopters but rather of those who will be observed and recorded. Will users of Google Glass manage to use the product while respecting existing social norms, or will they need to follow a newly invented code of etiquette? Can we expect disruptions and dismay such as those caused by early "Kodakers lying in wait"?[45]

We currently have few tools at our disposal to address these real-life dilemmas. Speaking at Harvard University's Kennedy School of Government, Google's Executive Chairman Eric Schmidt himself recently said, "People will have to develop new etiquette to deal with such products that can record video surreptitiously and bring up information that only the wearer can see. There are obviously places where Google Glasses are inappropriate."[46]

New services that make unexpected use of existing data may also result in backlash. When Google launched its Buzz social network and

[42] GLASS, http://www.google.com/glass/start/what-it-does (last visited Nov. 19, 2012).

[43] Jules Polonetsky, *When Do You Take Off Your Google Glasses?*, LINKEDIN INFLUENCERS (Feb. 21, 2013), http://www.linkedin.com/today/post/article/20130221045735-258347-when-do-you-take-off-your-google-glasses.

[44] *See* Peter Fleischer, *My Favorite Holiday Photos, and a Trillion Others*, PETER FLEISCHER: PRIVACY . . . ? (May 2, 2013), http://peterfleischer.blogspot.co.il/2013/05/my-favorite-holiday-photos-and-trillion.html ("In the near future, can individuals lifeblog photos or videos of everything and everyone they see? Technology will enable it. Some people will love it. So, once again, the question will be how social etiquette evolves in parallel to the technological evolutions.")

[45] Robert E. Mensel, *Kodakers Lying in Wait: Amateur Photography and the Right of Privacy in New York, 1885-1915,* 43 AM. Q. 24 (1991).

[46] Aaron Pressman, *Google's Schmidt Says Talking to Glasses Can be Weird, Inappropriate*, REUTERS (Apr. 25, 2013), http://www.reuters.com/article/2013/04/25/us-google-harvard-idUSBRE93O1FF20130425.

opted Gmail users in by default, many users were taken aback that their email contacts, such as intimate relations or psychiatrists, emerged as publicly-viewable contacts on the nascent network.[47] A privacy storm ensued, leading to a class action lawsuit, which settled for more than $8 million,[48] as well as an enforcement action by the FTC, which was settled in return for Google's commitment to implement a comprehensive privacy program and allow regular, independent privacy audits for the next 20 years.[49]

To sum up, numerous technologies and business models have gained notoriety as creepy. Naturally, identifying creep is more an art than a science. Hence, inductive reasoning based on anecdotal evidence may be the best way forward in theorizing this term. Ambient social apps have created creep by re-contextualizing data based on location. Through social listening, companies surprise users by interjecting corporate voices into what some perceive as private conversations. The democratization of big data capabilities and individual deployment of personalized analytics has led to social interactions being increasingly moderated by mutual data-digging. Data-driven marketing has gone on steroids, enabling retailers to induce sensitive facts from troves of innocuous data. Finally, new products and technologies continue to rub against the grain of existing social norms, creating unforeseen situations labeled creepy.

III. THE SHORTCOMINGS OF LAW

The techno-social ground is shifting, setting a complex interplay between what we *can* learn about each other and what we (or business or government) *should* know or be restricted from knowing. Part of the problem lies in the incongruity between the availability of digital information about individuals and the opacity of the purposes, uses, and intentions of those accessing such information. Another is the lingering indecision among policymakers with respect to the role of regulation in the absence of stable social norms. Should restrictions on conduct be based on law or on softer social norms? Should regulation drive or be driven by volatile individual expectations, market best practices, and social norms? Should we wait for norms to develop to form societal expectations?

[47] Shane Richmond, *How Google Crossed the Creepy Line*, TELEGRAPH (Oct. 25, 2010), http://www.telegraph.co.uk/technology/google/8086191/How-Google-crossed-the-creepy-line.html.

[48] Ben Parr, *Google Settles Buzz Privacy Lawsuit for $8.5 Million*, MASHABLE (Sep. 3, 2010), http://mashable.com/2010/09/03/google-buzz-lawsuit-settlement.

[49] FTC, *FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network*, http://www.ftc.gov/opa/2011/03/google.shtm.

In the past, privacy values and norms took years or even centuries to develop. The biblical Israelites, for example, wandered through the desert for decades, pitching tents along the way, learning with time to set their dwellings so that the openings of the tents did not face each other. When Balaam was sent to curse the Israelites, he looked upon their camp and blessed them instead, saying, "How goodly are your tents, O Jacob, your dwellings, O Israel!"[50] The Talmud teaches that he praised the dwellings of the Israelites because their architecture preserved domestic privacy.[51] Similarly, letter-writing existed as a means of communication for millennia before the synod of Rabbeinu Gershom issued its prohibition against the opening or reading of another person's letters in 1000 AD.[52]

More recently, in 1890, Samuel Warren and Louis Brandeis theorized the modern legal right to privacy as a reaction to the use and abuse of a new technology, "instantaneous photography," which led the *New York Times* in 1902 to decry "Kodakers lying in wait."[53] Yet it took 70 more years for this to impact the law, when William Prosser elucidated four common law torts out of the right to privacy.[54]

And, while the norms around the use of cameras stabilized after a while, the ubiquity of cameras on cellphones has created a new distortion. Most people would not walk around a gym locker room with a digital camera, understanding that they would be violating a social norm. But many continue to carry around their cellphones, which have multiple embedded cameras and may cause discomfort to other visitors. The indeterminacy of social norms in this context has led gyms to post signs warning their patrons not to have a cellphone camera out in the locker room.[55]

Caller ID provides another example of how privacy norms around a new technology can fluctuate. When it was launched in the late 1980s, many people thought that caller ID was a privacy problem, leading some

[50] *Numbers* 24:5.

[51] Nahum Rakover, *The Protection of Privacy in Jewish Law*, 5 ISRAEL Y.B. ON HUMAN RIGHTS 169 (1975).

[52] *Id.*

[53] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); Denis O'Brien, *Right of Privacy*, 2 COLUM. L. REV. 437 (1902).

[54] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960); *also see* Restatement (Second) of Torts § 652D (1977).

[55] Catherine Saint Louis, *Cellphones Test Strength of Gym Rules*, N.Y. TIMES (Dec. 7, 2011), http://www.nytimes.com/2011/12/08/fashion/struggle-to-ban-smartphone-usage-in-gyms.html (last visited Nov. 19, 2013).

U.S. states to regulate against it.[56] Critics thought it was a violation of privacy to see who was calling you, such as in the case of an individual calling an Alcoholic Anonymous clinic or an HIV help line. Today, many users would not answer the phone if the number were not listed. What was initially considered a privacy violation is now considered a privacy-enhancing technology.

As technological innovation accelerates, so does the need to recalibrate individual expectations, social norms, and, ultimately, laws and regulations. But the law is not always the best tool to moderate behavior. Individuals do not poke each other in the head not because of the threat of law enforcement but rather because it is inappropriate. Passengers in an elevator know better than to face each other, typically facing the doors until they reach their destination. Facing other passengers is not illegal, of course, yet it violates social norms and could well be viewed as creepy. When U.S. First Lady Michelle Obama breached royal protocol by touching her hand to Queen Elizabeth's back, she did not violate any legal norms, but the press nevertheless let out a collective gasp at the deviation from social etiquette.[57]

In an environment of rapidly shifting social norms and expectations, the law can be a crude and belated tool. By the time the Supreme Court decided that tracking a suspect with a GPS device required a warrant,[58] law enforcement authorities were already using drones.[59] As multiple circuits continue to debate the minutiae of law enforcement's access to email, users have migrated en masse to new communication technologies such as instant messaging and VoIP. The surge in innovation and socio-technological progress has left entire industries drifting without clear ethical guidelines, as the law fails to catch up with rampant technologies.

These days, the European Union is revamping its privacy laws, introducing highly charged new concepts such as a "right to be forgotten" and a "right to data portability."[60] The U.S. too is considering industry-wide

[56] Steven P. Oates, Note, *Caller ID: Privacy Protector or Privacy Invader?*, 1992 U. ILL. L. REV. 219 (1992).

[57] Howard Chua-Eoan, *The Queen and Mrs. Obama: A Breach in Protocol*, TIME (Apr. 1, 2009), http://www.time.com/time/world/article/0,8599,1888962,00.html#ixzz2R2RJR1Kj (last visited Nov. 19, 2013).

[58] United States v. Jones, 132 S. Ct. 945 (2012).

[59] *See From Jones to Drones: How to Define Fourth Amendment Doctrine for Searches in Public*, Privacy Law Scholars Conference, Washington, DC (June 7-8, 2012), http://www.youtube.com/watch?v=_pGCWZGdq08.

[60] The right to be forgotten, which has recently been rebranded as a "right to erasure" would allow individuals to scrub their data trail clean by requesting service providers to delete certain (assumingly negative) information retained about them. The right to data

privacy legislation based on the White House 2012 Consumer Privacy Bill of Rights.[61]

But will privacy law be subtle enough to distinguish normal practices from creepy ones when social norms in this space have hardly evolved? The European approach—trying to establish a social norm by regulatory fiat—may not fare well in the real world.

Shifting social norms, combined with powerful business interests and technological developments, threaten to make laws irrelevant. The law prohibits texting and driving but the availability of the iPhone in a traffic jam may prove irresistible. In a similar vein, the EU cookie directive,[62] which requires websites to obtain users' affirmative opt-in consent before placing a cookie on their machine, is out of sync with technological and business realities. Individuals simply do not want to be obstructed from reaching their online destination by repetitive notices and prompts for consent. Users are likely to eagerly click through any consent button placed on pop-ups, header bars, or message bars in order to remove the interference with their browsing. Consequently, the benefit of these mechanisms to individuals' privacy is questionable at best.[63] The right to be forgotten is similarly hampered by thorny implementation issues. Taken literally, it could pose a threat to the delicate balance between freedom and regulation on the Internet.

portability would allow individuals to transfer their personal information between service providers, for example, mobilizing their Facebook profile to Google Plus. *See Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [hereinafter GDPR]; Christopher Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, BNA PRIVACY & SECURITY LAW REPORT, Feb. 6, 2012, 11 PVLR 06.

[61] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (Feb. 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter White House Blueprint].

[62] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws, 2009 O.J. (L 337) 11 at 30.

[63] UK INFORMATION COMMISSIONER'S OFFICE, GUIDANCE ON THE RULES ON USE OF COOKIES AND SIMILAR TECHNOLOGIES (May 2012), www.ico.org.uk/~/media/documents/.../cookies_guidance_v3.ashx.

In other words, while the goals of the cookie directive (ensuring transparency and individual consent to online tracking) and of the right to be forgotten (challenging the permanency-by-default of digital data) may be admirable, the laws reflect an awkward attempt to mediate social norms. They will be daunting to operationalize, implement, and enforce. As Peter Fleischer writes, referring to the ubiquity of cameras, "all the rules in the world will do almost nothing, unless individuals exercise self-restraint in what they choose to photograph, or not, and what they choose to share with other people, or not."[64] Laws can nudge behavior, but individuals and businesses will find ways to work around them if they fail to adequately account for changes in technology. For example, the cookie directive is quickly becoming obsolete with the development of server-side surveillance mechanisms such as browser fingerprinting.[65]

In order to gain traction with businesses and individuals, regulation needs to be nuanced and reflect widely accepted social norms. Consider the effort to standardize a Do Not Track (DNT) protocol, which is currently taking place in the Tracking Protection Working Group of the World Wide Web Consortium (W3C). The persistent lack of agreement among W3C stakeholders demonstrates the difficulty in seeking a technological solution when the value of the activity to be proscribed remains widely disputed.[66] The real issue lurking behind the DNT fracas is not whether analytics, measurement, or third party cookie sharing constitutes tracking, but rather whether those activities carry an important social value that we wish to promote, or are negative and thus better killed softly by cookie-blocking default settings. As long as the underlying value question remains open, any efforts to resolve the OBA debate through user-agents and cookie management tools appear prone to fail. And the value judgment is not one for engineers to make. It cannot be discerned from harmonization of network protocols or etymological analysis of the words "track," "de-identified," or "third party," which the W3C has laboriously debated for months on end. It is not a technical or legal question; it is a social, economic, even philosophical quandary. Any regulatory scheme needs to recognize and address each of these dimensions to be successful.

In the techno-social space, adapting to new technologies requires educating individuals and providing companies with incentives to develop

[64] Fleischer, *supra* note 44.

[65] *See, e.g.*, *Panopticlick: How Unique – and Trackable – is Your Browser?*, ELECTRONIC FRONTIER FOUNDATION, https://panopticlick.eff.org (last visited Nov. 19, 2013).

[66] Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J. L. SCI. & TECH. 281, 334-5 (2012).

new business models. For example, music and film piracy were hardly affected by long-standing legal restrictions. People continued to pirate content, even in the face of stern criminal sanctions and aggressive litigation by industry bodies.[67] It was finally consumer education in conjunction with the emergence of new business models such as Apple's iTunes and Amazon Prime that effected change in media markets. Similarly, through a mix of regulation, competitive forces and consumer education, companies could be incentivized not to retain data forever, realizing that certain information (*e.g.*, notepad entries on a mobile device) is expected to be ephemeral while other information (*e.g.*, medical records) is expected to last longer, perhaps forever.

IV. DRIVERS FOR CHANGE

Three main vectors of influence drive the changes that affect individuals' perceptions of privacy and social norms. Businesses do not unilaterally decide to pull the rug out from under existing user expectations, nor does technology just go wild. Rather a combination of factors—including technology, economics, and individual choice—change norms. Consider the sharing of rich personal information, including birthdate, friend connections, photos, location, and various personal, cultural, and consumer preferences on social media. The drivers for such data sharing include *businesses*, which rely on engaging huge numbers of users and therefore promote data flows; *technologies*, such as big data, mobile, and cloud computing, which allow users to store essentially endless volumes of information on remote corporate servers and record their activities and whereabouts in real time through mobile devices; and *individuals*, who choose to communicate with family, colleagues, and friends through social networks and digital tools, engage mobile applications for anything from geographic navigation to medical treatments, and become active producers, consumers, processors and stewards of endless streams of personal information about themselves and others.

This part disentangles the three main drivers for shifting techno-social paradigms.

[67] Daniel Reynolds, Note, *The RIAA Litigation War on File Sharing and Alternatives More Compatible With Public Morality*, 9 MINN. J.L. SCI. & TECH. 977, 989 (2008); *RIAA v. The People: Five Years Later*, ELECTRONIC FRONTIER FOUNDATION (Sept. 30, 2008), https://www.eff.org/wp/riaa-v-people-five-years-later (last visited Nov. 19, 2013).

A. Business drivers

The vast majority of entities operating online and in the mobile space are businesses—not charities or non-profits. They face pressure to demonstrate that they can rapidly grow and engage new users in order to draw funding. In Silicon Valley, the name of the game is user engagement and traction, that is, the ability to not only attract new users but also keep them interacting with the site. Companies offer products and services for free,[68] expecting that profits will flow later through the introduction of a freemium model (*i.e.*, offering a basic service free of charge and then selling advanced features or related products),[69] the addition of ads, or sale of the business to a larger competitor.[70]

This explains why companies are constantly pushing *more* users to engage *more* often and share *more* data, sometimes pushing against social norms and challenging traditional values. Thus some companies design apps that seek to access all of a user's contacts in order to encourage the user to draw others to the service.[71] Other companies press users to share information in ways that may exceed initial expectations.[72] Consider the rapid growth of Viddy and Socialcam, social video-sharing apps that saw their user base grow by 10 million users *per week* after being integrated with Facebook, thus becoming the top Facebook and iOS apps in record time.[73] Alas, many of these new users failed to realize that by clicking to see catchy videos shared by friends, they too were sharing those videos with

[68] CHRIS ANDERSON, FREE: THE FUTURE OF A RADICAL PRICE (2009); *see also* FTC, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (Feb. 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf ("This expanding [online] marketplace has provided many benefits to consumers, including free access to rich sources of information . . . .").

[69] *Freemium*, WIKIPEDIA, http://en.wikipedia.org/wiki/Freemium (last visited Nov. 19, 2013).

[70] Jules Polonetsky, *Would You Pay 10 Cents for this Article?*, LINKEDIN (Apr. 7, 2013), http://www.linkedin.com/today/post/article/20130407183308-258347-would-you-pay-10-cents-for-this-article (last visited Nov. 19, 2013) (third party monetization of data is not a *sine qua non* for online profitability).

[71] Megan Rose Dickey, *It Turns Out Path, Considered a Threat to Facebook, May Just be Really Good at Spamming*, BUSINESS INSIDER (May 1, 2013), http://www.businessinsider.com/path-spamming-users-2013-5 (last visited Nov. 19, 2013).

[72] *See* Fred Stutzman, Ralph Gross & Alessandro Acquisti, *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 4(2) J. PRIV. & CONFID. 7 (2012).

[73] Om Malik, *Facebook Giveth, Facebook Taketh: A Curious Case of Video Apps*, GIGAOM (May 14, 2012), http://gigaom.com/2012/05/14/facebook-giveth-facebook-taketh-a-curious-case-of-video-apps (last visited Nov. 19, 2013).

their entire network, sometimes causing great embarrassment due to the raunchy nature of the viral content.[74]

Businesses choose defaults, game design, and other factors that relentlessly pressure users to accelerate social norms. These trends are reinforced by the online advertising sector, which benefits greatly from the ability to analyze and measure the effectiveness of ad campaigns. Companies are also motivated to use OBA to monetize their products.[75] The more finely tailored the ad, the higher the conversion rates and, thus, the higher the revenues of advertisers, publishers, and ad intermediaries.[76] This means that businesses have strong financial incentives to drive consumers to more freely share information. Yet, regardless of what we think about the prevailing business model, it is not the sole driver of techno-social innovation.

B. Technological drivers

The surge in innovation in data-intensive technologies has revolutionized the socio-technological environment for businesses and individuals in just two or three decades. Computers, once costly and cumbersome machines operated solely by privileged government and research institutions, are now ubiquitous, interconnected, small, and cheap. Less than a decade ago, few had the foresight to imagine that most people today would be walking with tiny devices containing multiple high-resolution digital video and still cameras, microphones, speakerphones, media players, GPS navigation, touch screen, web browser, Wi-Fi and mobile broadband connections, and multiple sensors including an accelerometer, proximity sensor, ambient light, and compass, as well as access to hundreds of thousands of applications, typically offered free of charge or at negligible cost. Developments in cloud computing, medical devices, biometric and genetic data science, smart grid, and robotics have likewise left technology ethicists reeling.

There is little doubt that technology creates immense societal value and empowers individuals, who can now obtain an education and access

[74] *See* Elinor Mills, *Socialcam Closes Hole that Enabled Accidental Sharing*, CNET (May 17, 2012), http://news.cnet.com/8301-1009_3-57436777-83/socialcam-closes-hole-that-enabled-accidental-sharing (last visited Nov. 19, 2013); Wendy Davis, *Socialcam Beefs Up Privacy Features*, MEDIAPOST (May 16, 2012), http://www.mediapost.com/publications/article/174877/#axzz2SAgpHAX9 (last visited Nov. 19, 2013).

[75] *Id,* at 2.

[76] Omer Tene, *Privacy: The New Generations*, 1 INT'L DATA PRIV. L. 15, 16-7 (2011), http://idpl.oxfordjournals.org/content/1/1/15.full.

endless sources of data from their home. At the same time, it facilitates access to less wholesome resources including pornography, gambling, and guns, and permits malicious actors to remotely threaten computer networks as well as critical national infrastructure. Social networking services have fostered political revolutions and the overthrow of malevolent regimes, and provided channels for citizen journalism revealing human rights violations. At the same time, they could facilitate pervasive surveillance and present formidable challenges such as protecting minors from pedophiles, sexting, and cyberbullying.

The point is that technology is neither *good* nor *bad*. It is a forceful tool for change in multiple socio-economic contexts and, when combined with business drivers, exerts formidable pressure on existing social norms. As Peter Fleischer writes, "Expectations of privacy will sometimes collide with the technology, and each will influence the other. Sometimes, technology will just be a few years ahead of the social consensus evolving to accept it. Sometimes, it will be a generation ahead."[77] It is the philosophers and lawyers who need to build the bridges between rapidly evolving technologies and sluggishly forming social and legal norms.

C. Individual drivers

Technology and businesses should serve individuals, but what do individuals really want? We are certainly curious to see friends' photos and follow their whereabouts. And many of us enjoy publicizing our successes and those of our children.[78] After all, Facebook does not post our data; we do. Using brain imaging and behavioral experiments, Harvard scientists have discovered that, when people talk about themselves in public, the same regions of the brain that are associated with rewards from food, money, or sex exhibit heightened activity.[79] Sharing personal information on social media satisfies primal needs and desires.

More complicated yet, individuals' appetites for data sharing are fickle. For example, researchers at Carnegie Mellon University have shown that survey respondents are more willing to divulge sensitive information after being told that previous respondents made similarly sensitive

[77] Fleischer, *supra* note 44.

[78] Alina Tugend, *Etiquette Lessons for the Braggart: Step 1, Don't Pretend to Be Humble*, N.Y. TIMES (Jan. 11, 2013), http://www.nytimes.com/2013/01/12/your-money/the-etiquette-of-celebrating-or-bragging-about-achievements.html (last visited Nov. 19, 2013).

[79] Diana Tamir & Jason Mitchell, *Disclosing Information About the Self is Intrinsically Rewarding*, 109(21) PROC. NAT'L ACAD. SCI. 8038 (May 22, 2012), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3361411.

disclosures.[80] In another experiment, researchers demonstrated that, paradoxically, if individuals are given more control over the publication of their private information, their privacy concerns decrease and their willingness to publish sensitive information increases, even when the probability that strangers will access and use that information stays the same or, in fact, increases.[81]

But when does extroversion (in some cases, exhibitionism) and curiosity become creepy and violate accepted social norms? Is an ob-gyn precluded from posting (anonymous) rants on Facebook about a patient who is always late for appointments?[82] And what about an offended waitress who posts a copy of a non-tipping patron's credit card receipt?"[83] These examples implicate sharing by one individual of others' private information, and also reflect behaviors that may themselves be viewed as socially awkward.

More generally, what is a healthy, socially acceptable level of disclosure on your own Facebook profile? Posting what you had for lunch? Photos of your kids? Location? Music you are listening to? Film reviews? Political views? Is it legitimate to brag about your acceptance to college? For your parents to boast about the same? Clearly, our answers to these questions are all over the map; clear societal norms have simply not yet evolved.

Communications with friends and other social connections are no less frayed by ambiguity. Is it socially acceptable to look at the Facebook profile of your babysitter, or should you use your status as her Facebook friend strictly for sending her direct messages to inquire about her babysitting availability? If it is acceptable to explore her profile, is it also acceptable to comment on (or tag) her photos or posts? Can adults even understand the boundaries of these social networks, or are they destined to

[80] Alessandro Acquisti, Leslie John & George Loewenstein, *The Impact of Relative Standards on the Propensity to Disclose*, 49 J. MKTG. RES. 160 (2012).

[81] Laura Brandimarte, Alessandro Acquisti & George Loewenstein, Misplaced Confidences: Privacy and the Control Paradox (unpublished manuscript) (on file with the Future of Privacy Forum), http://www.futureofprivacy.org/wp-content/uploads/2010/09/Misplaced-Confidences-acquisti-FPF.pdf.

[82] *See* Chris Matyszczyk, *Outcry as Ob-Gyn Uses Facebook to Complain About Patient,* CNET (Feb. 9, 2013), http://news.cnet.com/8301-17852_3-57568540-71/outcry-as-ob-gyn-uses-facebook-to-complain-about-patient (last visited Nov. 19, 2013).

[83] *See* Neetzan Zimmerman, *Pastor Who Left Sanctimonious Tip Gets Waitress Fired from Applebee's, Claims Her Reputation Was Ruined*, GAWKER (Jan. 31, 2013), http://gawker.com/477230335 (last visited Nov. 19, 2013).

be "creepers" in the eyes of children and adolescents, as documented by danah boyd?[84]

Even without the adult-adolescent or employer-employee dynamics introduced in the above example, what individuals want from social networks is unclear. When, for example, do users willingly accept a friend tagging them in a photo, and when is doing so unacceptable? And when does sharing a friend's photo with a larger audience than she had originally intended become untoward? What one individual may view as legitimate, expected behavior, another regards with disdain, creating tensions and conflicts against the backdrop of unsettled norms.

Consider the following story: On Christmas 2012, Randi Zuckerberg, the older sister of Facebook's founder and CEO, posted a photo from a family gathering on Facebook. The photo appeared on the newsfeed of socialite Callie Schweitzer, who subscribes to Randi's feed and is also (incidentally) a Facebook friend of Randi's sister. Schweitzer, who assumed that Randi posted the photo publicly, tweeted it to her nearly 40,000 Twitter followers. In fact, Schweitzer saw the photo (probably) because Randi tagged her sister, who is Schweitzer's friend. Randi reprimanded Schweitzer on Twitter stating: "Digital etiquette: always ask permission before posting a friend's photo publicly. It's not about privacy settings, it's about human decency."[85]

Was Schweitzer wrong to assume the photo was public? Was she required to ask Randi for permission to tweet? Was Randi wrong to tag her sister in the photo? Did she ask for her permission to do so? Was Randi's understanding of digital etiquette accurate or overly conservative? Would digital etiquette have been different on Twitter? How were user expectations different a few years ago and how will they evolve over the upcoming years?

Indeed, consider something as basic as texting. Who can you text? Anyone whose number you have? Only close personal friends? A work colleague if you are running late? If you would call someone's cellphone, does that mean you have achieved the level of intimacy necessary to text them?

[84] danah boyd, Address at the 32nd International Conference of Data Protection and Privacy Commissioners: The Future of Privacy: How Privacy Norms Can Inform Regulation (Oct. 29, 2010), http://www.danah.org/papers/talks/2010/PrivacyGenerations.html.

[85] Kashmir Hill, *Oops. Mark Zuckerberg's Sister Has a Private Facebook Photo Go Public*, FORBES (Dec. 26, 2012), http://www.forbes.com/sites/kashmirhill/2012/12/26/oops-mark-zuckerbergs-sister-has-a-private-facebook-photo-go-public (last visited Nov. 19, 2013).

The answers to these questions implicate delicate, budding relationships between business models, technologies, and individual preferences. Given the pace of technological progress, business leaders, ethicists, and policymakers have little if any time to pause and reflect before they have to make weighty policy choices. Failure to carefully adjust business practices and individual actions to newly-developed technologies in real time can grate against social norms—a phenomenon we colloquially call "creepiness."

V. HOW TO AVOID CREEP

The ongoing haggling over the specifics of a DNT standard exemplifies just how polarized the techno-social debate has become.[86] Mike Zaneis, General Counsel of the Interactive Advertising Bureau (IAB), an industry body representing media and technology companies in the online advertising space, recently called Mozilla's move to block third-party cookies through the latest version of its Firefox browser "a nuclear first strike against the ad industry."[87] Some OBA advocates argue that any non-tailored ads constitute spam.[88] Privacy advocates counter that industry should not assume that individuals are informed about the realities of online tracking or willing to trade off their privacy for more tailored content.[89] Peter Swire, who co-chaired the W3C Working Group, called the ongoing crisis a looming "digital arms race," warning that "if not defused, escalation around these competing interests will create major problems for both individuals and the businesses that depend on the Internet."[90]

[86] *See* Kate Kaye, *Sen. Jay Rockefeller Blasts Ad Industry in Senate Hearing Over Do Not Track*, AD AGE (Apr. 24, 2013), http://adage.com/article/digital/sen-jay-rockefeller-blasts-ad-industry-track/241078 (last visited Nov. 19, 2013).

[87] Laura Stampler, *Firefox Launches 'Nuclear First Strike Against Ad Industry'*, BUSINESS INSIDER (Feb. 25, 2013), http://www.businessinsider.com/firefox-to-block-third-party-cookies-2013-2 (last visited Nov. 19, 2013).

[88] Jessica Guynn, *Top Senate Democrat Calls for 'Do Not Track,' Advertisers Protest*, L.A. TIMES (Apr. 25, 2013) http://articles.latimes.com/2013/apr/24/business/la-fi-tn-top-senate-democrat-calls-for-do-not-track-advertisers-protest-20130424(last visited Nov. 19, 2013) (quoting Bob Liodice, president of the Association of National Advertisers: "Consumers will not see fewer ads, but rather would be on the receiving end of a blizzard of untailored, spam-like ads.").

[89] *See, e.g.*, Lee Tien & John M. Simpson, Community Group comments on W3C DNT, Jan. 8, 2012, http://www.centerfordigitaldemocracy.org/sites/default/files/CommunityDNT-1.8.2012-1.pdf.

[90] Peter Swire, *How to Prevent the 'Do Not Track' Arms Race*, WIRED (Apr. 24, 2013), http://www.wired.com/opinion/2013/04/do-not-track (last visited Nov. 19, 2013).

Consumer advocates, advertisers and ad intermediaries, browser makers, and website owners (publishers) are pitted against one another in a battle over balancing privacy and business needs.[91] Businesses are concerned that policymakers in Washington and Brussels will impose heavy-handed regulation that will dampen economic progress and technological innovation. Regulators view businesses as overly zealous money-making machines eager to monetize individuals' data with little regard for social costs or ethical values.[92] Consumer advocates fear that new technologies will create an infrastructure for mass surveillance where businesses and governments collaborate to impose a high expense on individual privacy rights.[93]

How can we start to defuse the combustive mix of business interests, engineering, and individual rights?

Unfortunately, companies cannot avoid privacy fiascos simply by following the law. Privacy regulation—comprised primarily of the fair information privacy principles (FIPPs)—is a means to an end. When viewed as a stand-alone edifice, privacy regulation becomes almost meaningless, a bureaucratic box-ticking exercise involving notices that few users read and "consent" without information, volition, or choice.[94] In order to avoid creep, companies must engage their consumers in a meaningful conversation to reduce suspicion and align interests and expectations. They need to frame relationships by setting the tone for new products or novel uses of information. This part sets forth several strategies to help businesses absorb rapidly evolving social norms.

A. Against technological determinism

To avoid creep, engineers should refrain from engaging in technological determinism; they should not believe that, just because something has become possible, it should be done. That data *could* be collected and stored forever does not necessarily mean that it *should* be. As

[91] *Id.*

[92] *See, e.g.*, Eric Pfanner, *Google Faces More Inquiries in Europe Over Privacy Policy*, N.Y. TIMES (Apr. 2, 2013), http://www.nytimes.com/2013/04/03/technology/google-to-face-national-regulators-over-privacy-policy.html (last visited Nov. 19, 2013).

[93] *See, e.g.*, Letter from U.S. Consumer Organizations to Jan Philipp Albrecht, Rapporteur, Committee on Civil Liberties, Justice and Home Affairs (Sept. 5, 2012) (on file with EPIC), http://epic.org/privacy/intl/US-Cons-Grps-Support-EU-Priv-Law.pdf; *CDD and USPIRG Urge Commerce Department to Protect Consumers Online*, CTR. FOR DIGITAL DEMOCRACY (Jan. 28, 2011), http://www.democraticmedia.org/cdd-and-uspirg-urge-commerce-department-protect-consumers-online (last visited Nov. 19, 2013).

[94] *See, e.g.*, discussion of EU cookie directive, *supra* notes 62 to 66 and accompanying text.

Jaron Lanier argues in his book *You Are Not a Gadget: A Manifesto*, technology should be designed to serve humans and reflect their values, not the other way around.[95]

In the offline world, there is a degree of impermanence to almost any action; photos and post-it notes are not expected to last forever. And we share an understanding of how permanent any type of action should be: our expectations of the publicity and permanence of a book, for example, differ greatly from those connected to a personal letter or a scrap of paper left on a desk. Yet in the digital realm, emails, tweets, even sexting messages, which are certainly not *intended* for eternity, are nearly impossible to track down, contain, and destroy. They may, and in fact do, come back to haunt us years later, in different contexts and with entirely different audiences.[96] We are being forced to assume that anything digital will last forever and may find its way to the public domain. And this, in turn, may stifle freedom of speech, thought, and organization.

While we should not settle for the oft-heard engineer response: "this is how technology works," the solution is not necessarily regulation that ignores all technological realities and mandates data deletion.[97] Rather, it is to design technologies with prevailing social values in mind.

Consider cloud email providers. Had Gmail not provided more than 10 gigabytes of free storage, users would have been nudged to delete their emails every once in a while; the availability of effectively unlimited storage encourages users to retain email indefinitely. Over the past few years, we have all become hoarders. Individuals and companies retain immense, previously unfathomable amounts of data simply because they *can*. But in the offline world, people who retain objects indiscriminately are considered to be mentally unsound, regardless of whether they have the storage capacity. Normative offline behavior can be emulated in the digital world through appropriate product design.

Consider Snapchat, a photo messaging application that allows users to set a time limit for how long recipients can see a photo or video before it vanishes irretrievably (both from the recipient's device and the company's servers).[98] For people who worry about unflattering photos or embarrassing status updates coming back to haunt them, the app's appeal is obvious.

[95] Jaron Lanier, YOU ARE NOT A GADGET: A MANIFESTO (2010).

[96] *See* Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES (July 21, 2010), http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html (last visited Nov. 19, 2013).

[97] *See, e.g.*, GDPR at Art. 17.

[98] Jenna Wortham, *A Growing App Lets You See It, Then You Don't*, N.Y. TIMES (Feb. 8, 2013), http://www.nytimes.com/2013/02/09/technology/snapchat-a-growing-app-lets-you-see-it-then-you-dont.html.

Similarly, data deletion policies imposed by corporations over their internal email storage or other files prevent the apparent inevitability of universal storage. These methods are not perfect and legal or technical means can defeat them, but they help establish a norm that ensures that data is not readily available.

Woodrow Hartzog and Fred Stutzman call for "obscurity by design," enabling individuals to hide data that is technically public through techniques such as reduced search visibility, access controls, pseudonymous profiles, and obfuscation of observed information.[99] Ryan Calo critiques Facebook's recent introduction of Graph Search[100] as a step in the opposite direction.[101] The natural language search tool allows Facebook users to dig and unearth data hidden in their social graph. Graph Search technically respects existing privacy settings, but it does reduce obscurity and data obfuscation.[102]

Rather than simply institute a tool like Graph Search because it is technologically possible, companies should ask: Does making data that was always available more easily retrievable improve society enough to outweigh the privacy disruptions? By removing friction and practical obstacles that impede data flows, companies enhance user experience at an occasional cost to privacy. And this may impact not only information that the company itself has collected. A good example is access to court records, which democratic societies have always made publicly available. In the past, the practical costs of searching through and retrieving court records provided *de facto* protection for an individual's privacy. Today, it is sufficient to google a litigant's name in order to access his or her court records, which may include sensitive medical, financial, and other details.[103]

[99] Fred Stutzman & Woodrow Hartzog, *Obscurity by Design: An Approach to Building Privacy into Social Media*, CSCW '12 Workshop on Reconciling Privacy with Social Media (2012), http://fredstutzman.com/papers/CSCW2012W_Stutzman.pdf.

[100] *Introducing Graph Search*, FACEBOOK.COM, https://www.facebook.com/about/graphsearch (last visited Nov. 25, 2013).

[101] Jessica Guynn, *Facebook Unveils Search Tool. Will It Find Acceptance?*, L.A, TIMES, Jan. 16, 2013, at B1.

[102] Woodrow Hartzog & Evan Selinger, *Obscurity: A Better Way to Think About Your Data Than "Privacy"*, ATLANTIC (Jan. 17, 2013), http://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283; Ryan Tate, *Creepy Side of Search Emerges on Facebook*, WIRED (Feb. 15, 2013), http://www.wired.com/business/2013/02/creepy-graph-searchers.

[103] Amanda Conley, Anupam Datta, Helen Nissenbaum & Divya Sharma, *Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry*, 71 MD. L. REV. 772, 816 (2012).

The social value of open data and enhanced accessibility is evident—yet so is the price to individual privacy.

The emergence of algorithmic solutions has impacted behaviors that are deeply linked with social values, including recruiting employees,[104] microtargeting political campaigns,[105] grading essays,[106] or even just suggesting friends on social networks. Do we want technological determinism to seep into these actions? Just because we can use data to make these decisions for us, should we?

Friend suggestions—and more broadly, social networking services themselves—inevitably reduce individuals to a set of characteristics (relationship status, geo-location map, music and movies "liked") that in Jaron Lanier's words "underrepresents reality." In Lanier's view, there is no perfect computer analogue for what we call a "person." "In Facebook, as it is with other online social networks, life is turned into a database, and this is a degradation."[107] Some of our ethical and moral criteria are so fragile, nuanced, and culturally dependent that it is not clear that an algorithm will *ever* be capable of appropriately weighing them.[108] Indeed, it is far from clear that we would even *want* computers to obtain the ability to distinguish right from wrong. Such an anthropomorphized machine—a technological singularity[109]—would likely be creepier than the current dumbed-down version.[110]

[104] Matt Richtel, *How Big Data Is Playing Recruiter for Specialized Workers*, N.Y. TIMES (Apr. 27, 2013), http://www.nytimes.com/2013/04/28/technology/how-big-data-is-playing-recruiter-for-specialized-workers.html.

[105] Daniel Kreiss, *Yes We Can (Profile You): A Brief Primer on Campaigns and Political Data*, 64 STAN. L. REV. ONLINE 70 (2012); Natasha Singer & Charles Duhigg, *Tracking Voters' Clicks Online to Try to Sway Them*, N.Y. TIMES (Oct. 27, 2012), http://www.nytimes.com/2012/10/28/us/politics/tracking-clicks-online-to-try-to-sway-voters.html.

[106] Randall Stross, *The Algorithm Didn't Like My Essay*, N.Y. TIMES (June 9, 2012), http://www.nytimes.com/2012/06/10/business/essay-grading-software-as-teachers-aide-digital-domain.html.

[107] Zadie Smith, *Generation Why?*, N.Y. REV. BOOKS (Nov. 25, 2010), http://www.nybooks.com/articles/archives/2010/nov/25/generation-why.

[108] Tene & Polonetsky, *supra* note 2.

[109] Ray Kurzweil, THE SINGULARITY IS NEAR: WHEN HUMANS TRANSCEND BIOLOGY (2006).

[110] Alexis Madrigaljan, *IBM's Watson Memorized the Entire "Urban Dictionary," Then His Overlords Had to Delete It*, ATLANTIC (Jan. 10, 2013), http://www.theatlantic.com/technology/archive/2013/01/ibms-watson-memorized-the-entire-urban-dictionary-then-his-overlords-had-to-delete-it/267047 ("Watson couldn't distinguish between polite language and profanity -- which the Urban Dictionary is full of. . . . In tests it even used the word 'bullshit' in an answer to a researcher's query.

Hence, companies should be careful about launching new services and cool features simply because they *can*. To avoid disrupting ethical norms and possibly straining the social fabric, entrepreneurs should verify that passengers are on board before the train of innovation leaves the station.

B. Against privacy lurch

While engineers should steer clear of technological determinism, businesses should refrain from a "throw-it-up-against-the-wall-and-see-if-it-sticks" approach to new product development.[111] Former FTC Commissioner Pamela Jones Harbour used these harsh words to criticize Google for the launch of a public-facing product (Buzz) piggybacking on a service that users understood as private (Gmail). danah boyd calls the resulting commotion a "privacy fail."[112] Paul Ohm dubs it a "privacy lurch"—that is, an abrupt change a company makes to the way it handles data about individuals.[113] Needless to say, privacy fails or lurches are creepy.

Companies should be extra careful not to startle consumers with unanticipated data grabs, monitoring, or publicity. For example, Path, a popular and rapidly growing mobile social networking service, was discovered to be uploading users' address books without their knowledge and consent.[114] This set off a storm of criticism. Path was accused of "stealing" users' address books,[115] leading to a formal apology by the budding company's CEO,[116] congressional inquiry,[117] and regulatory

Ultimately, Brown's 35-person team developed a filter to keep Watson from swearing and scraped the Urban Dictionary from its memory.").

[111] Pamela Jones Harbour, *Remarks Before Third FTC Exploring Privacy Roundtable*, http://www.ftc.gov/speeches/harbour/100317privacyroundtable.pdf (last visited Nov. 25, 2013).

[112] danah boyd, *Making Sense of Privacy and Publicity*, SXSW, http://www.danah.org/papers/talks/2010/SXSW2010.html (last visited Nov. 25, 2013).

[113] Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 909 (2013).

[114] Arun Thampi, *Path Uploads Your Entire iPhone Address Book to Its Servers*, MCLOV.IN (Feb. 8, 2012), http://mclov.in/2012/02/08/path-uploads-your-entire-address-book-to-their-servers.html (last visited Nov. 25, 2013).

[115] Jason Gilbert, *iPhone App Privacy: Path, Facebook, Twitter and Apple under Scrutiny for Address Book Controversy*, HUFFINGTON POST (Feb. 15, 2012), http://www.huffingtonpost.com/2012/02/15/iphone-privacy-app-path-facebook-twitter-apple_n_1279497.html.

[116] Dave Morin, *We Are Sorry*, PATH BLOG (Feb. 8, 2012), http://blog.path.com/post/17274932484/we-are-sorry (last visited Nov. 25, 2013); *see also* Rafe Needleman*, Path CEO: We Are Sorry, and We've Deleted Your Address Book Data*,

action.[118] Intimidated by the huge public response, developers of other apps, including Instagram, quickly updated their interfaces to request data access when matching contacts.[119] There was little doubt that the data that *Path* uploaded were necessary for the smooth provision of its services, and users would likely have consented to provide their information had they been asked. But just as guests to your house are not welcome to open your refrigerator and help themselves to some pie, even if that same pie had been purchased for them, so too are mobile apps not expected to "help themselves" to users' data without permission.

In Helen Nissenbaum's terms, privacy is all about context.[120] Consumers are unlikely to object to the use of personal information where it is contextually consistent or where strong public policy interests mandate data use. The lesson for companies is that context is key. For any innovation or new product launch, users should be brought along carefully, educated, and given an opportunity to object.[121] Just as friends do not magically transmute into lovers, so should email contacts not automatically become social networking friends. Amazon, for example, may pursue a high degree of customization without violating consumer expectations, given its clear messaging about customization and friendly user interface, whereas Orbitz will surprise users when tailoring specific kinds of travel offers to their browser type.[122]

CNET (Feb. 8, 2012), http://news.cnet.com/8301-19882_3-57373474-250/path-ceo-we-are-sorry-and-weve-deleted-your-address-book-data (last visited Nov. 25, 2013).

[117] Matt Brian, *Congress Sends Letter to Apple Questioning the Path Debacle, Developer Data Access*, THE NEXT WEB (Feb. 15, 2012), http://thenextweb.com/apple/2012/02/15/congress-sends-letter-to-apple-questioning-the-path-debacle-developer-data-access (last visited Nov. 25, 2013).

[118] *Path Social Networking App Settles FTC Charges It Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books*, (Feb. 1, 2013), http://www.ftc.gov/opa/2013/02/path.shtm (last visited Nov. 25, 2013); *see also* Hayley Tsukayama, *FTC, Path Settlement Shows Online Privacy Goes Beyond the Policy*, WASH. POST (Feb. 1, 2013), http://articles.washingtonpost.com/2013-02-01/business/36681778_1_mobile-privacy-app-developers-user-data.

[119] Matt Brian, *Following Path's Contact Fiasco, Instagram Silently Adds a Contact List Access Prompt*, THE NEXT WEB (Feb. 11, 2012), http://thenextweb.com/mobile/2012/02/11/following-paths-contact-fiasco-instagram-silently-adds-a-contact-list-access-prompt (last visited Nov. 25, 2013).

[120] Helen Nissenbaum, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009); *see also* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).

[121] Jules Polonetsky & Omer Tene, *It's Not How Much Data You Have, But How You Use It*, FUTURE OF PRIVACY FORUM (Dec. 5, 2012), http://www.futureofprivacy.org/fpf-white-paper-its-not-how-much-data-you-have-but-how-you-use-it.

[122] Mattioli, *supra* note 35.

To avoid giving the sense of lunging at data, companies need to set the tone for their relationships with users. If a strange man tells you to take your clothes off, you would think he is crazy; if the strange man is a doctor, it would seem appropriate; if it is someone you meet on a first date, it might be abrupt; on the second or third date, perhaps welcome. The point is that social interactions are complex, nuanced, and need to be carefully structured. Individuals have strong intuitions about it; corporations are less agile.

The "respect for context" approach has now been adopted by the White House[123] and FTC.[124] Yet some may argue that it is overly conservative and unnecessarily limits innovation. Nissenbaum herself notes, "By putting forward existing informational norms as benchmarks for privacy protection, we appear to endorse entrenched flows that might be deleterious even in the face of technological means to make things better. Put another way, contextual integrity is conservative in possibly detrimental ways."[125] Thus, context—generally helpful for privacy—may be viewed as an impediment to innovation.

For example, if Facebook had not proactively launched its News Feed feature in 2006 and had instead solicited users' opt-in consent, we would likely not have the Facebook we know today. Some readers may recall that, in the past, when users logged into Facebook all they could see was their face, *i.e.*, their own profile; to view another user's news, they had to actively enter that user's profile. It is only when data started flowing that users became accustomed to the change, which more than a billion users worldwide enjoy today. Another example is Comcast's decision in 2010 to pro-actively monitor its customers' computers to detect malware;[126] more recently, Internet-service providers (ISPs) including Comcast, AT&T, and Verizon have reached out to consumers whose computers had been infected and used by criminals as bots.[127]

In each of these cases—Facebook's News Feed and the ISPs' warnings—companies may have struggled if asked to obtain individuals'

[123] White House Blueprint, *supra* note 61, at 10.

[124] FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, 36-40 (2012), http://ftc.gov/os/2012/03/120326privacyreport.pdf.

[125] *Id.* at 143.

[126] Roy Furchgott, *Comcast to Protect Customer's Computers from Malware*, N.Y. TIMES (Sept. 30, 2010), http://gadgetwise.blogs.nytimes.com/2010/09/30/comcast-to-monitor-customer-computers-for-malware.

[127] Daniel Lippman & Julian Barnes, *Malware Threat to Internet Corralled*, WALL ST. J. (July 9, 2012), http://online.wsj.com/article/SB10001424052702303292204577515262710139518.html.

prior opt-in consent to data practices which were truly innovative, unanticipated, and therefore out of context. In fact, many Facebook users initially reacted negatively to the introduction of News Feed, criticizing the changed user experience.[128] Once they adjusted to this change in context, however, realizing that Facebook is a tool not just for curation of one's profile but also for broadcasting information to one's friends, News Feed became a vital part of the Facebook experience, driving user engagement and playing a crucial role in spreading information globally. And while each of these innovations signified a change in context that benefits consumers and perhaps society at large, it is far from clear that individuals would have opted-in to these practices if asked to do so in advance. As Larry Downes recently observed, "Today's privacy crisis is a function of innovation that happens too quickly. Given the accelerating pace of new information technology introductions, new uses of information often appear suddenly, perhaps overnight. Still, after the initial panic, we almost always embrace the service that once violated our visceral sense of privacy."[129]

Ohm suggests that trademarks could bridge the notice deficiency of corporate privacy practices and thereby prevent a privacy lurch.[130] Ohm's approach would require every company that handles customer information to associate its trademark with a specified set of core privacy commitments, requiring a change of trademark if the company decides to depart from its initial promises. Hence, Ohm appears to view brand development as a top-down exercise where companies shape brand qualities through purposeful, legally-binding commitments.

In contrast, we suggest that while brand recognition has important implications for privacy law, it is in fact a bottom-up process where *users* set their expectations based on their perception of a brand.[131] And while companies can manage their image and brand through advertising and marketing, it is users, not businesses, that inject brands with meaning. Consequently, in order to assess the legitimacy of data practices, regulators should take account of *user expectations* rather than corporate statements.[132]

[128] Michael Arrington, *Facebook Users Revolt, Facebook Replies*, TECHCRUNCH (Sept. 6, 2006), http://techcrunch.com/2006/09/06/facebook-users-revolt-facebook-replies (last visited Nov. 25, 2013); John Leyden, *Facebook Mods Controversial "Stalker-friendly" Feature*, REGISTER (Sept. 8, 2006), http://www.theregister.co.uk/2006/09/08/facebook_climbdown.

[129] Larry Downes, *A Rational Response to the Privacy "Crisis,"* 716 POLICY ANALYSIS 1, 10 (2013), http://object.cato.org/sites/cato.org/files/pubs/pdf/pa716.pdf.

[130] Ohm, *supra* note 113.

[131] Polonetsky & Tene, *supra* note 121, at 1.

[132] Of course, when made clearly and effectively, corporate statements influence user perceptions and expectations.

In some cases, user expectations might indeed limit a new data use, but in other cases they could help support a new product or service.

Users may trust recognized brands more than they do newcomers, but this approach does not imply that recognized brands have a *de facto* license to use data in a manner that start-up businesses do not. Rather, the point is that user perception of a brand can help a company that is proposing new data uses if such uses constitute an extension of the brand that resonates with consumers. For example, a consumer does not ordinarily expect his sneakers to communicate with his phone, but if Nike sold a Nike brand smartphone, consumers would be more likely to expect it to communicate seamlessly with their bluetooth-enabled Nike shoes.

Delineating context is particularly difficult in the social networking world, which is marked by what Alice Marwick and danah boyd call "context collapse."[133] In social media, contacts from different walks of a user's life, such as friends, family members, and co-workers, are lumped together under the (Facebook-selected) title of "friends."[134] Marwick explains that, in the offline world, getting a call from one's boss while on a date requires a quick switch of self-presentation and social role to suit the occasion.[135] This compartmentalizing of self-presentation (essentially identity[136]) is difficult to maintain in social media where users have to navigate multiple networks simultaneously, alternatingly concealing and revealing information to friends, family, colleagues, old classmates, etc.[137] The problem is that roles such as parent-child, employer-employee, or teacher-student reemerge at what Marwick calls "moments of rupture," where offline power structures become manifest (*e.g.*, an employer's

[133] Alice Marwick & danah boyd, *I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience*, 13 NEW MEDIA & SOCIETY 114, 122 (2011).

[134] Context collapse is somewhat reduced in Google Plus, which provides the "Circles" feature, allowing users to disaggregate their online identities by sending updates to certain groups of people (*e.g.*, high school friends, relatives, colleagues or followers) and not to others. *See* Omer Tene, *Me, Myself and I: Aggregated and Disaggregated Identities on Social Networking Services*, 8(2) J. INT'L COMM. L. & TECH. 118 (2013).

[135] Alice Marwick, *Social Surveillance in Everyday Life*, 9(4) SURVEILL. & SOCIETY 378, 386 (2012).

[136] An "identity" comprises essential and unique characteristics that define an individual. For a classic exposition of the concept of digital identity in cyberspace, see Kim Cameron, *The Laws of Identity*, Microsoft Whitepaper, May 2005, http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf; *see also* The White House, *National Strategy for Trusted Identities in Cyberspace*, April 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf; OECD, *Digital Identity Management: Enabling Innovation and Trust in the Internet Economy*, 2011, http://www.oecd.org/sti/ieconomy/49338380.pdf; Tene, *supra* note 134.

[137] Marwick, *supra* note 135, at 385-87.

promotion decision, a school disciplining a child for cyberbullying) often to the detriment of the person lower on the social hierarchy.[138] This means that, despite evident difficulty, context remains key in social media as well. Companies should consider—and make use of—context to avoid privacy lurch.

C. Against targeting the superuser

In his article "The Myth of the Superuser: Fear, Risk, and Harm Online," Paul Ohm cautions against laws and regulations that are addressed at risks created by a legendary, omnipotent, malevolent superuser, who seldom exists in practice.[139] Such laws are inevitably overbroad and ambiguous, and unnecessarily restrict the rights and freedoms of inculpable, ordinary users.[140] For example, the Computer Fraud and Abuse Act (CFAA)[141] and its implementation by law enforcement have been broadly criticized as an overbroad, even draconian criminalization of generally harmless activity.[142] The assumption that every instance of unauthorized access to a computer constitutes a dangerous cyberattack has led to prosecution of individuals for activity that is hardly criminal, sometimes with dire consequences.[143]

In a similar vein, we urge engineers and businesses not to assume that average users of new data-sharing products or services are superusers, that is highly tech-savvy early adopters who read and understand privacy

[138] *Id.* at 386. *See, e.g.*, Rosen, *supra* note 96 (discussing the Stacy Snider "drunken pirate" affair, in which a teacher in training was terminated based on a photo showing her at a party wearing a pirate hat and drinking from a plastic cup).

[139] Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327 (2008).

[140] *See, e.g.*, Orin Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561 (2010).

[141] 18 U.S.C. § 1030 (2010).

[142] *See, e.g.*, Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER, Mar. 18, 2013, http://www.newyorker.com/online/blogs/newsdesk/2013/03/fixing-the-worst-law-in-technology-aaron-swartz-and-the-computer-fraud-and-abuse-act.html ("The Computer Fraud and Abuse Act is the most outrageous criminal law you've never heard of. It bans 'unauthorized access' of computers, but no one really knows what those words mean. Orin Kerr, a former Justice Department attorney and a leading scholar on computer-crime law, argues persuasively that the law is so open-ended and broad as to be unconstitutionally vague. Over the years, the punishments for breaking the law have grown increasingly severe—it can now put people in prison for decades for actions that cause no real economic or physical harm") (last visited Jan. 20, 2014).

[143] Marcia Hofmann, *In the Wake of Aaron Swartz's Death, Let's Fix Draconian Computer Crime Law*, EFF BLOG, Jan. 14, 2013, https://www.eff.org/deeplinks/2013/01/aaron-swartz-fix-draconian-computer-crime-law (last visited Nov. 25, 2013).

policies and manipulate default settings with ease. Typically, individuals get privacy defaults wrong,[144] disseminate content more broadly than they intended or is advisable for their own good,[145] forget passwords or keep them listed on unencrypted files on their laptop,[146] and generally struggle to keep up with the astounding surge in digital economy and culture.

Researchers at Carnegie Mellon University recently investigated the usability of tools to limit OBA. They observed participant behavior as participants installed and used various privacy tools, including opt-out tools, browser settings, and cookie blockers, and recorded their perceptions and attitudes about those tools, finding serious usability flaws in all nine tools examined.[147] The researchers conclude, "There are significant challenges in providing easy-to-use tools that give users meaningful control without interfering with their use of the web. Even with additional education and better user interfaces, it is not clear whether users are capable of making meaningful choices about trackers."[148]

Engineers should be mindful of the fact that products and services that they design are intended (also) for non-engineers. The Silicon Valley culture, dubbed the "hacker way" by Mark Zuckerberg, founder of Facebook,[149] whose corporate credo is "move fast and break things," is not always aligned with broader societal values and expectations. Recently, at an FTC workshop on the "Internet of Things," Vint Cerf, one of the architects of the Internet and currently Google's Chief Internet Evangelist, argued that "privacy may be an anomaly . . . a construct of the modern

[144] Maritza Johnson, Serge Egelman & Steven Bellovin, *Facebook and Privacy: It's Complicated*, SOUPS '12: PROCEEDINGS OF THE EIGHTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY (2012), http://www.cs.columbia.edu/~maritzaj/publications/soups12-johnson-facebook-privacy.pdf; *see also* Fred Stutzman, Ralph Gross & Alessandro Acquisti,
Silent Listeners: The Evolution of Privacy and Disclosure on Facebook, 4 J. PRIVACY & CONFID. 7 (2012).

[145] Kashmir Hill, *Either Mark Zuckerberg Got a Whole Lot Less Private or Facebook's CEO Doesn't Understand the Company's New Privacy Settings*, TRUE/SLANT (Dec. 10, 2009), http://trueslant.com/KashmirHill/2009/12/10/either-mark-zuckerberg-got-a-whole-lot-less-private-or-facebooks-ceo-doesnt-understand-the-companys-new-privacy-settings (last visited Nov. 25, 2013).

[146] Cormac Herley, P. C. van Oorschot & Andrew Patrick, *Passwords: If We're So Smart, Why Are We Still Using Them?*, FIN. CRYPT. AND DATA SEC. 230, 237 (2009).

[147] Pedro Leon et al, *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising*, in Proc. CHI 2012, ACM Press 2012, 1, 5, http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf.

[148] *Id.* at 4.

[149] Mark Zuckerberg, *Letter to Investors: 'The Hacker Way'*, WIRED (Feb. 1, 2012), http://www.wired.com/business/2012/02/zuck-letter.

industrial age."[150] Critics responded by showing that privacy is in fact a deeply embedded value with roots going back to prehistoric times, while it is unfettered technological innovation that may be anomalous in a historical perspective.[151]

D. For turning on the light

Louis Brandeis once wrote, "Sunlight is said to be the best of disinfectants."[152] A dark basement is creepy; turn on the lights and it becomes a pool-table delight. The more transparent businesses are about their data practices, purposes, and needs, the less creepy they seem. Google stumbled into a privacy fail when its mapping of Wi-Fi networks in order to enhance the company's geo-location services was discovered to have logged some users' web activity.[153] The massive global outcry seems to have been driven as much by surprise about the practice of logging Wi-Fi routers by driving through the streets as it was by the collection of sensitive data that was being beamed into the public streets from nearby houses and businesses. We are certain that a greater level of advance public awareness about the necessity of mapping Wi-Fi routers in order to provide valuable location services would have framed this privacy failure differently. Consider that, even after Google provided users with an opportunity to opt

[150] Gregory Ferenstein, *Google's Cerf Says "Privacy May Be An Anomaly", Historically He's Right,* TECHCRUNCH (Nov. 20, 2013), http://techcrunch.com/2013/11/20/googles-cerf-says-privacy-may-be-an-anomaly-historically-hes-right (last visit Jan. 20, 2014).

[151] Omer Tene, *Vint Cerf is Wrong. Privacy Is Not An Anomaly*, PRIVACY PERSPECTIVES, Nov. 22, 2013, https://www.privacyassociation.org/privacy_perspectives/post/privacy_is_not_an_anomaly (last visited Jan. 20, 2014).

[152] Louis Brandeis, *What Publicity Can Do*, HARPER'S WEEKLY, Dec. 20, 1913, http://3197d6d14b5f19f2f440-5e13d29c4c016cf96cbbfd197c579b45.r81.cf1.rackcdn.com/collection/papers/1910/1913_12_20_What_Publicity_Ca.pdf (last visited Nov. 19, 2013).

[153] Google's privacy snafu is still being investigated by regulators around the globe; yet, it concerns the capture by Google of unencrypted payload (content) data—not the practice of mapping Wi-Fi networks. *See* Martyn Williams, *Google to Pay $7 Million to US States for Wi-Fi Eavesdropping*, PC WORLD, Mar. 13, 2013, http://www.pcworld.com/article/2030705/google-to-pay-7-million-to-us-states-for-wi-fi-eavesdropping.html; *Google Fined by German Data Protection Agency for Illegally Recording Unsecured WiFi Info*, A.P., Apr. 22, 2013, http://www.foxnews.com/tech/2013/04/22/google-fined-by-german-data-protection-agency-for-illegally-recording-unsecured (last visited Nov. 19, 2013).

their routers out of the mapping scheme, it is doubtful that many users have actually done so.[154]

In April 2011, Apple's iOS 4 was revealed to include an unencrypted location tracking log file providing rich insight into the whereabouts of unsuspecting iPhone users.[155] Alarmist press reports raged, warning that "iOS devices store a list of the device's location and time stamps for when the location information was gathered, and do it all using a file that can be easily read by just about anyone."[156] Senator Al Franken wrote a letter to Apple's then-CEO Steve Jobs, expressing concern that "anyone who gains access to this single file could likely determine the location of a user's home, the businesses he frequents, the doctors he visits, the schools his children attend, and the trips he has taken—over the past months or even a year."[157] European privacy regulators were set to investigate.[158] Apple responded, formally stating, "Apple is not tracking the location of your iPhone. Apple has never done so and has no plans to ever do so."[159] It explained that rather than track the location of an iPhone, the stored file was maintaining a database of Wi-Fi hotspots and cell towers around the phone's location to help it rapidly and accurately calculate its location when requested.

Admitting that its main blunder was one of miscommunication, Apple stated, "Users are confused, partly because the creators of this new technology (including Apple) have not provided enough education about

[154] Kevin O'Brien, *Google Allows Wi-Fi Owners to Opt Out of Database*, N.Y. TIMES, Nov. 15, 2011, http://www.nytimes.com/2011/11/16/technology/google-allows-wi-fi-owners-to-opt-out-of-database.html (last visited Nov. 19, 2013).

[155] Alasdair Allen & Pete Warden, *Got an iPhone or 3G iPad? Apple is Recording Your Moves*, O'REILLY RADAR, Apr. 20, 2011, http://radar.oreilly.com/2011/04/apple-location-tracking.html; Jacqui Cheng, *How Apple Tracks Your Location Without Consent, and Why It Matters*, ARSTECHNICA, Apr. 20, 2011, http://arstechnica.com/apple/2011/04/how-apple-tracks-your-location-without-your-consent-and-why-it-matters (last visited Nov. 19, 2013).

[156] Darrell Etherington, *Apple Tracks and Logs iPhone and iPad Location Data in iOS 4, GIGAOM*, Apr. 20, 2011, http://gigaom.com/2011/04/20/apple-tracks-and-logs-iphone-and-ipad-location-data-in-ios-4 (last visited Nov. 19, 2013).

[157] Letter from Al Franken, U.S. Senator, to Steve Jobs, CEO of Apple (Apr. 20, 2011), http://www.franken.senate.gov/files/letter/110420_Apple_Letter.pdf (last visited Nov. 19, 2013).

[158] Charles Arthur, *iPhones and Android Phones Building Vast Databases for Google and Apple: Italy, France and Germany to Investigate Smartphone Tracking Software Amid Privacy Concerns*, GUARDIAN, Apr. 22, 2011, http://www.guardian.co.uk/technology/2011/apr/22/iphone-android-location-based-services (last visited Nov. 19, 2013).

[159] *Apple Q&A on Location Data*, APPLE PRESS INFO (Apr. 27, 2011), http://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html (last visited Nov. 19, 2013).

these issues to date."[160] This is a good example of the need for companies to shine the light in order to prevent creepiness. Had it provided transparency into its data practices, Apple could have been a privacy hero rather than location-tracking villain. Apple could have depicted local storage of location data as a privacy-enhancing solution, even a fun consumer feature, preferable from a privacy (if not data security) standpoint to server-side surveillance. In fact, even with Apple's communications errors, *Forbes*' technology reporter Kashmir Hill pondered whether the locally stored location tracking file was "cool or creepy."[161] Apple's main competitor, Google, seems to have learned from this mishap, providing users of its Google Now personal assistant service with a feature that displays a detailed map of their location history, thus framing the technology as a service rather than a creepy surprise.[162]

OBA too has suffered from misperceptions and opaqueness.[163] Users have been unaware of the breadth and depth of the market for personal information. Even industry veterans struggle to explain the intricacies of the data flows between supply and demand side markets, data exchanges, analytics experts, optimizers and data brokers.[164] For example, retargeting, that is the practice of showing an ad to a user after he has left the advertiser's website, may leave privacy-conscious users with a sense of unease. Interviewed for the *New York Times*, one user stated, "For days or weeks, every site I went to seemed to be showing me ads for those shoes. It is a pretty clever marketing tool. But it's a little creepy, especially if you don't know what's going on."[165] If the industry enhanced transparency,

[160] *Id.*

[161] Kashmir Hill, *Cool or Creepy? Your iPhone and iPad Are Keeping Track of Everywhere You Go, And You Can See It*, FORBES, Apr. 20, 2011, http://www.forbes.com/sites/kashmirhill/2011/04/20/cool-or-creepy-your-iphone-and-ipad-are-keeping-track-of-everywhere-you-go-and-you-can-see-it (last visited Nov. 19, 2013).

[162] *Manage Location in Google Settings*, GOOGLE, https://support.google.com/gmm/bin/answer.py?hl=en&answer=1650337 (last visited Nov. 19, 2013).

[163] Chris Hoofnagle, Jennifer Urban & Su Li, *Privacy and Modern Advertising: Most US Internet Users Want 'Do Not Track' to Stop Collection of Data About Their Online Activities*, Amsterdam Privacy Conference, Oct. 8, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2152135 (last visited Nov. 19, 2013).

[164] *Before You Even Click . . .*, FUTURE OF PRIVACY FORUM (Apr. 29, 2010), www.futureofprivacy.org/2010/04/29/before-you-even-click (graphically illustrating the complexity of the online ecosystem) (last visited Nov. 19, 2013).

[165] Miguel Helft & Tanzina Vega, *Retargeting Ads Follow Surfers to Other Sites*, N.Y. TIMES, Aug. 29, 2010, http://www.nytimes.com/2010/08/30/technology/30adstalk.html (last visited Nov. 19, 2013); Jack Marshall, *Is Retargeting the New Pop-up?*, DIGIDAY, Apr. 17, 2013, http://www.digiday.com/publishers/is-ad-retargeting-the-new-pop-up (last visited Nov. 19, 2013).

users would likely be less surprised or intimidated by advertisements that follow them around the Web.

It has become abundantly clear that transparency does not mean more, better, shorter (or longer) privacy policies. Written by lawyers *for* lawyers, privacy policies have failed to provide users with meaningful insight into corporate data practices. In his book *Code Version 2.0*, Larry Lessig explains, ”Cluttering the web with incomprehensible words will not empower consumers to make useful choices as they surf the Web. If anything, it drives consumers away from even attempting to understand what rights they give away as they move from site to site.”[166] Ryan Calo calls this “notice skepticism” and instead advocates for “non-linguistic notice,” or designing websites and apps in a way that places the user on guard at the moment of collection or demonstrates to the consumer how her data is actually being used in practice.[167] He calls this “visceral” notice, similar to reintroducing engine noise into otherwise silent electric cars to alert pedestrians, or camera shutter sounds into mobile phone cameras to notify individuals they are being photographed.[168]

Lorrie Cranor, Alessandro Acquisti, and a group of researchers at Carnegie Mellon University are working on what they call “privacy nudges”—software that “essentially sits over [users’] shoulder[s] and provides real-time reminders—such as short on-screen messages—that information [they are] about to send has privacy implications.”[169] Behavioral economists endorse such soft paternalistic interventions, noting that significant changes in human behavior can be provoked by design decisions, such as placing health food at eye level in a cafeteria and demoting fattening food to lower levels.[170]

[166] LAWRENCE LESSIG, CODE: VERSION 2.0 228 (2006).

[167] M. Ryan Calo, *Against Notice Skepticism*, 87 NOTRE DAME L. REV. 1027, 1046, 1051 (2012) (recalling that the Roman emperor Caligula acknowledged the need to create and publish the law, “but it was written in a very small hand, and posted up in a corner so that no one could make a copy of it”) (citing Screws v. United States, 325 U.S. 91, 96 (1945)).

[168] *Id.* at 1027, 1034-5.

[169] Rebecca Balebako et al., *Nudging Users Towards Privacy on Mobile Devices*, Workshop on Persuasion, Influence, Nudge and Coercion Through Mobile Devices (PINC at CHI-11), http://ceur-ws.org/Vol-722/paper6.pdf (last visited Nov. 19, 2013); *see also* Alessandro Acquisti, *Nudging Privacy: The Behavioral Economics of Personal Information*, IEEE SECURITY & PRIVACY, Nov-Dec. 2009, 82, 84 (describing the benefits of a soft paternalistic approach of “nudging” privacy); Yang Wang et al., *Privacy Nudges for Social Media: An Exploratory Facebook Study*, PSOSM 2013, Rio de Janeiro, Brazil, http://precog.iiitd.edu.in/events/psosm2013/9psosm6-wang.pdf (last visited Nov. 19, 2013).

[170] Richard Thaler & Cass Sunstein, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 1–5 (2008).

A similar strategy is to embed critical design into data processing systems in order to engage users in a dialogue about the values embedded in those systems and cue them into action.[171] One example is Collusion, a Firefox browser extension that animates the extent to which websites collaborate in tracking user behavior by visualizing cookies and the relationships among the multiple parties that issue them.[172] By displaying the complex network of data monetization intermediaries, Collusion encourages users to reflect on the fundamentals of the data-for-service exchange. A group of researchers at Cornell University tested various design strategies intended to provoke user reflection about data collection and use.[173] One of the strategies, which they call "make it creepy," displays to users the sensitive and highly personal aspects of their gathered data, focusing on data that might be uncomfortable for the user to confront (*e.g.*, "Did you know that we've been recording your activity for 5 days? In that time, we've seen you online for 200 total hours, and recorded more than 200 sites you've visited"). The researchers tested reactions to such notices, concluding that critical design can effectively raise awareness and promote enhanced user control over personal data.[174]

An additional strategy for increasing transparency is the privacy dashboard. Initially introduced as a data registry by data management company Bluekai,[175] privacy dashboards have since been launched by online leaders such as Google[176] and Yahoo[177] to allow users to access categories of data maintained about them and opt-out of marketing

[171] Evgeny Morozov, *Machines of Laughter and Forgetting*, N.Y. TIMES, Mar. 30, 2013, http://www.nytimes.com/2013/03/31/opinion/sunday/morozov-machines-of-laughter-and-forgetting.html (last visited Nov. 19, 2013).

[172] *Lightbeam*, http://www.mozilla.org/en-US/lightbeam/ (last visited Nov. 19, 2013).

[173] Vera Khovanskaya et al., *"Everybody Knows What You're Doing": A Critical Design Approach to Personal Informatics*, *in* PROC. CHI 2013: THE ACM, http://stephen.voida.com/uploads/Publications/Publications/khovanskaya-chi13.pdf (last visited Nov. 19, 2013).

[174] For additional work in this field, see Karen P. Tang, Jason I. Hong & Daniel P. Siewiorek, *Understanding How Visual Representations of Location Feeds Affect End-user Privacy Concerns*, *in* Proc. UbiComp: The ACM 207 (2011), http://delivery.acm.org/10.1145/2040000/2030141/p207-tang.pdf?ip=130.132.173.99&id=2030141&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF1811B42933DD4E8A45D88D5B9224167B1&CFID=261906414&CFTOKEN=24122349&__acm__=1384907210_59efa3cdd142df40fb90fb3d812a2b23 (last visited Nov. 19, 2013).

[175] *See Registry*, http://www.bluekai.com/registry (last visited Nov. 19, 2013).

[176] *Ads Settings*, www.google.com/ads/preferences (last visited Nov. 19, 2013).

[177] *Ad Interest Manager*, info.yahoo.com/privacy/us/yahoo/opt_out/targeting (last visited Nov. 19, 2013).

campaigns.[178] Google explains, "With this tool, users can view, add and remove the categories that are used to show them interest-based ads (sports, travel, cooking, etc.) when they visit one of our AdSense partners' websites or YouTube."[179]

Extending the rationale underlying the privacy dashboard, our article *Big Data for All: Privacy and User Control in the Age of Analytics* promotes two distinct types of transparency.[180] First, organizations should provide individuals with practical, easy-to-use access to their information in machine-readable format, so they can become productive participants in the data economy.[181] Second, organizations should be transparent about the decisional criteria underlying their data processing activities, allowing individuals to challenge, or at the very least understand, how decisions about them are made.[182]

E. For the golden rule

Finally, the role of individuals themselves, as both producers and consumers of personal information, should no longer be ignored. Individuals today play a far greater role than they did in the past in generating and disseminating personal information, raising new issues regarding the impact they are having on their privacy and the privacy of others.[183] Posting data on social networking sites that refer to third parties or uploading or tagging photographs of others are a few of the examples where individuals disclose the personal data of third parties, sometimes to their surprise or chagrin.

Indeed, the environment in which individuals participate online is often one of "public by default, private through effort."[184] For example, not all users of social networking sites fully understand that third party applications they use have access not only to their personal information but also to the personal information of their friends on that network.

[178] Erick Schonfeld, *Google Gives You a Privacy Dashboard to Show Just How Much It Knows About You*, TECHCRUNCH (Nov. 5, 2009), http://techcrunch.com/2009/11/05/google-gives-you-a-privacy-dashboard-to-show-just-howmuch-it-knows-about-you (last visited Nov. 19, 2013); Nicole Wong, *Giving Consumers Control Over Ads*, GOOGLE PUB. POL'Y BLOG, (Mar. 11, 2009), http://googlepublicpolicy.blogspot.com/2009/03/giving-consumers-control-over-ads.html (last visited Nov. 19, 2013).

[179] Wong, *supra* note 178.

[180] Tene & Polonetsky, *supra* note 2.

[181] *Id*. at 263-69.

[182] *Id*. at 270-72.

[183] Jonathan Zittrain, *Privacy 2.0*, 2008 U. CHI. LEGAL F. 65 (2008).

[184] Boyd, *supra* note 112.

Consequently, as information producers, individuals should be aware that when they post or upload personal information to a public or semi-public online space, such information might be disseminated beyond their initial expectations. In such cases, individuals may not be able to retrieve personal information that was initially posted or uploaded voluntarily. Individuals should carefully select what personal information they share with others and with whom they share it. In their role as information consumers, individuals should treat others' information as they wish their own information to be treated. This derivative of the golden rule means that users should observe others' privacy choices, respect them, and act responsibly when allowing third parties to access not only their own personal information but also others' information to which they have access themselves.

For example, Alice Marwick discusses "Facebook stalking," the common practice of visiting other users' Facebook profiles to browse through their photos, posts and interactions.[185] Marwick observes, "Facebook stalking, more generally, is simply *using Facebook*."[186] Indeed, who has not rummaged through the photos of an ex-girlfriend or current colleague? Yet the connotation associated with Facebook stalking is clearly negative (*e.g.*, it is not called "Facebook courtesy visiting"); and it is no coincidence that unlike LinkedIn, its business-focused competitor, Facebook keeps information about who visited your profile a closely guarded secret. On LinkedIn, expanded capability to see who has viewed your profile is a premium feature, since social norms for business networking seem to support this type of browsing. The rules of engagement on "stalking" or visiting other profiles have yet to be written. And this further muddles the boundary between ethical and unsavory social media behavior.

VI. CONCLUSION

Businesses, individuals, policymakers, and society at large are struggling to react to an avalanche of technological innovations, which destabilize the very core of techno-social values and norms. As businesses roll out new products and services, we continue to witness crisis after crisis, with company after company stumbling as it tries to navigate consumer

[185] Marwick, *supra* note 135, at 387; *see also* Allison McCann, *Facebook is Normalizing Creepy Behavior*, BUZZFEED, Jun. 28, 2012, http://www.buzzfeed.com/atmccann/facebook-is-normalizing-creepy-behavior (last visited Nov. 19, 2013).

[186] *Id*. at 387 (emphasis in original).

expectations and regulatory requirements and having to deal with the fallout, which includes bad press, investigations, and class action lawsuits.

Silicon Valley engineers and entrepreneurs tend to embrace certain assumptions: Progress, efficiency, and speed are good. Technology can solve most things. Change is inevitable; disruption is not to be feared. Appropriately, one of the tech world's main annual conferences is called "Disrupt." Individuals deliver mixed messages, on the one hand decrying the erosion of privacy and rapid societal change, and on the other hand generously pouring personal information into new products and apps. To mediate the market and achieve a desirable balance between the interests and needs of all parties, policymakers need to pursue a nuanced and sophisticated path. They should recognize that social norms are rarely established by regulatory fiat, and that laws that fail to reflect techno-social reality may not fare well in the real world. Whether legislating or encouraging self-regulation, understanding how social norms are evolving is essential in order to avoid crude or heavy-handed interventions. Regulation should not be viewed as an obstacle to innovation and progress.[187] Rather it should be used strategically to incentivize companies to proceed with caution and educate users to act responsibly on the new data frontier.

Companies will not avoid privacy backlash simply by following the law. Privacy law is merely a means to an end. Social values are far more nuanced and fickle that any existing (and most likely future) laws and regulations. In order to avoid creep, companies should resist the temptation to act with chutzpah,[188] even though brazen and audacious behavior constitutes a hallmark of Silicon Valley entrepreneurship culture.[189] The challenge is for companies to set the right tone when seeking intimate relationships with consumers.

Companies should avoid technological determinism. Engineers should design technologies to mesh well with social values and consumer expectations. Companies should be cautious of privacy lurches, instead engaging their consumers in the evolution of products and carefully navigating shifts in context. Engineers should focus on the average—as opposed to super—user, bearing in mind that consumers never read privacy policies, misunderstand privacy settings, and fall back on embedded design

[187] *Cf.* Leila Abboud, *France calls for EU to regulate web giants to counter dominance*, REUTERS, Sept. 19, 2013, http://www.reuters.com/article/2013/09/19/us-france-eu-webgiants-idUSBRE98I14E20130919 (last visited Jan. 20, 2014).

[188] *Chutzpah*, WIKIPEDIA, http://en.wikipedia.org/wiki/Chutzpah (last visited Nov. 19, 2013).

[189] SHERYL SANDBERG, LEAN IN: WOMEN, WORK, AND THE WILL TO LEAD (2013).

principles to avert personal embarrassment as a result of unwittingly sharing personal information.[190] As with all matters creepy, shining the light is the ultimate strategy, providing individuals with access to their information and insight into the data practices deployed. Finally, individuals should be educated to treat their own data and that of their peers with respect, realizing that in a digital environment prior prudence and restraint are far more effective than any *ex post* clean up effort.

[190] Fred Stutzman, Ralph Gross & Alessandro Acquisti, *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 4(2) J. PRIVACY & CONFIDENTIALITY 7 (2012).