Idaho Law Review

Volume 51 | Number 3 Article 3

March 2019

Privacy Without Screens & the Internet of Other People's Things

Meg Leta Jones

PRIVACY WITHOUT SCREENS & THE INTERNET OF OTHER PEOPLE'S THINGS

MEG LETA JONES*

TABLE OF CONTENTS

I. INTRODUCTION

This is an essay about the future, and as such, it is speculative and optimistic. The future is connected, populated by smart things, people, and places. The Consumer Electronic Show 2015 was full of smart devices, from consumer drones[1] to auto-adjusting beds.[2] A number of startups are creating new forms of connectivity. For instance, AdhereTech's smart pill bottle is intended to increase adherence to medication schedules and help healthcare providers and pharmaceutical companies gain important insight,[3] while Chul's facial recognition technology replaces keys, passwords, and codes, allowing users to disarm a security system with the unique features of their face, even as it changes.[4] Established players like Samsung have been pushing the trend of connectivity with smart lighting systems to wine collection management.[5] Not just information technology companies are players in the smart future; companies like General Motors and Whirlpool are adding intelligence and autonomy to existing technologies like cars[6] and washing machines.[7] We are

* Assistant Professor, Georgetown University, Communication, Culture, & Technology. Thanks to Jill Dupre and Laura Moy for thinking through this future with me.

1. Jim Fisher, *CES 2015: Drones, Drones, Drones*, PC MAG (Jan. 9, 2015), http://www.pcmag.com/article2/0,2817,2474885,00.asp.

2. Devindra Hardawar, *The Smartest 'Smart Bed' Auto-Adjusts Throughout the Night*, ENGADGET (Jan. 6, 2015), http://www.engadget.com/2015/01/06/rest-smart-bed/.

3. Jeff Vance, *10 Hot Internet of Things Startups*, CIO (Sept. 4, 2015), *http://www.cio.com/article/2602467/consumer-technology/10-hot-internet-of-things-startups.html.*

4. *Id.*

5. Rachel King, *Samsung at CES 2015: Internet-of-Things is Not Science Fiction, but 'Science Fact*,' ZDNET (Jan. 6, 2015), http://www.zdnet.com/article/ces-2015-samsung-internet-of-things/.

6. Doron Levin, *GM Takes a Public Step into Driverless Car Tech*, FORTUNE (Sept. 9, 2014), http://fortune.com/2014/09/09/gm-driverless-cars/.

quickly creating an environment not full of more screens of different sizes, but one of tangible, ambient computing. Boo-Keun Yoon, President and CEO of Samsung Electronics stated flatly, "It's not science fiction anymore. It's science fact."[8] This essay takes the present one step further into a near future wherein these systems are widely used and interconnected—a future without screens.

Screens have formed the foundation of our experience with connected content, and information exchange agreements adhere to this comfortable arrangement. While screens complicated information collection and privacy, a lack of screens promises to further complicate the arrangement. Notice and choice, wherein an information collector notified information subjects of what would be gathered and how it would processed, is incredibly challenging in a screen world and is even more challenging in a smart world without screens.[9] The focus of the essay is not on individuals operating with a screen, nor on the initial operator of a device in the smart world that may adapt information and use settings or agree to terms of service found in the box the product was delivered in, but on everyone else that may be exposed to numerous smart devices in a smart world. It focuses on information preferences in the internet of other people's things.

The United States and European Union are approaching these issues differently. The American Federal Trade Commission released a report in January 2015 that emphasized security and acknowledged the serious problems presented to the notice and choice model of information collection and processing by the Internet of Things (IoT).[10] The E.U. has proactively sought to get in front of a smart world, expressing challenging regulatory expectations but also putting resources toward developing innovations as well as policy.[11] While these institutions are preparing for a future where privacy is more vulnerable, perhaps through this transition privacy never available in a world with screens is achievable. What both approaches share is more interesting than how they differ. Both consider the Internet of Things an extension of the internet and big data—it is not all that new.

By framing the smart future as new, based not on the technology but on the experience of users and the inability to utilize the notice and choice foundation of information policy, an opportunity to rethink privacy and information preferences presents itself.

---

7. Drew Harwell, *Whirlpool's "Internet of Things" Problem: No One Really Wants a "Smart" Washing Machine*, WASH. POST (Oct. 28, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/28/whirlpools-internet-of-things-problem-no-one-really-wants-a-smart-washing-machine/.

8. King, *supra* note 5.

9. *Infra* Part III.

10. INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, FTC STAFF REPORT (Jan. 27, 2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

11. Press Release, European Commission, When Your Yogurt Pots Start Talking to You: Europe Prepares for the Internet Revolution, IP/09/952 (June 18, 2009), *available at* http://europa.eu/rapid/press-release_IP-09-952_en.htm?locale=en; Article 29 Data Protection Working Party, Opinion 8/2014 on Recent Developments on the Internet of Things (Sept. 16, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf [hereinafter Article 29 Data Protection].

What does privacy look like after the screen? Certainly, it may (and is expected to) not look good.[12] Smart technologies create an ever-public wherein information is relentlessly collected and processed. Although information practices are changing and exposure to information gathering and processing has increased dramatically, there is room for optimism for a new form of privacy could present itself when traditional notice and choice is no longer a crutch.

There is opportunity as we transition from a world without screens to flip notice and choice on its head and build a smart world on choice and notice, wherein the privacy choices provided by the user must be noticed by smart devices. This will require significant efforts to build an infrastructure that supports user choice and places the burden on the collector to take notice. This will require the smart world infrastructure to create or account for a yet to develop shift in expectations. Administrative efforts to support privacy without screens will need to be as innovative as the innovation itself, but do not necessarily need to move away from existing privacy principles—just reimagine them.

II. SMART PUBLICS

This section paints a picture of a connected society—it presents an image of smart publics created by smart objects, people, and spaces. Many connected devices are currently being developed for the home, like smart toothbrushes and washing machines. These devices will send data from the device in the home out to the cloud, leaving their private nature uncertain, and many others will be designed to operate outside the home, like driverless cars, wearables, and smart retailers. Pew's Director of Internet, Science, and Technology Research Lee Rainie investigated the future of the internet and found experts agreeing, "[B]asically . . . life in public is the new norm now . . . . Privacy is an activity to be achieved in havens or in special circumstances with lots of effort. The default condition of humans in the post-industrial world is you're in public all the time."[13] The Internet of Things is the beginning of this future, but "smart publics" describe an experience wherein individuals move through a networked environment they are a part of—a connected reality that is somewhat different than being connected through numerous screens, as we experience today.

A. Smart Things

Generally, the goal of the Internet of Things is to enable ubiquitous connection. "A world where the real, digital and the virtual are converging to create smart environments that make energy, transport, cities and many other areas more intelligent."[14] In the smart public, things connect regardless of the time, place, path, net-

12. Lee Rainie & Janna Anderson, *Digital Life in 2025: The Future of Privacy*, PEW RESEARCH CENTER 28 (Dec. 18, 2014), http://www.pewinternet.org/files/2014/12/PI_FutureofPrivacy_1218141.pdf.

13. John P. Mello Jr., *Experts Forecast the End of Privacy as We Know It*, TECH NEWS WORLD (Dec. 18, 2014), http://www.technewsworld.com/story/81501.html.

14. INTERNET OF THINGS: FROM RESEARCH & INNOVATION TO MARKET DEPLOYMENT, EUROPEAN RESEARCH CLUSTER ON THE INTERNET OF THINGS (IERC) (Ovidiu Vermasen & Peter

work, or service. In order for this to occur, physical objects must contain embedded technology to sense and communicate. As wireless protocols become more efficient and sensors and processors become smaller and less expensive, anything can become smart. In 2011, there were already more Internet-connected devices than human beings.[15] The IoT is estimated to be the largest device market in the world, with 23.3 billion active IoT devices by 2019 (twice the combined number of active PCs, smartphones, and tablets).[16] These objects may be designed for a single user, like the Oral B smart toothbrush that shows brush habits like time, pattern, and quality,[17] or Hum, the robotic sex toy that claims to be the "iPhone of vibrators."[18] Smart security cameras, doorbells, locks, planters, light bulbs, window shades, and motion sensors may be for shared spaces like an office or home. Smart objects may also be placed in traditionally public spaces the way sidewalk trash cans[19] and driverless cars are intended.[20]

B. Smart People

Connected devices are more than stationary, adapted, everyday objects that may now meet needs in a more personalized way. They move around with us and are known as wearables.[21] The Fitbit wristband is a physical activity tracker designed to help wearers be more active, eat better, and sleep more soundly.[22] Lifelogger claims to be the next GoPro, selling wearable technology to support memory and record keeping.[23]

Smaller markets are booming with smart technologies. Blake Uretsky's "B" Maternity Wearables fashion line for pregnant women incorporates conductive fiber technology into the fabric to record vital signs like heart rate, blood pressure, temperature, and respiration.[24] Mimo makes wearable onesies for infants that moni-

---

Friess eds. 2014), *available at* http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2014_Ch.3_SRIA_WEB.pdf.

15. *Id*.

16. John Greenough, *The 'Internet of Things' Will Be The World's Most Massive Device Market And Save Companies Billions Of Dollars*, BUSINESS INSIDER (Apr. 14, 2015), http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10#ixzz3UyZXjwpm.

17. Darrell Etherington, *Oral-B's Bluetooth Toothbrush Offers App Features It Doesn't Necessarily Need*, TechCrunch (Feb. 17, 2015), http://techcrunch.com/2015/02/17/oral-b-pro-7000-smartseries-with-bluetooth-review/#bJxWo1:5Ud8.

18. EJ Dickson, *Meet Hum, The World's First Artificially Intelligent Vibrator*, DAILYDOT (Dec. 11, 2014), http://www.dailydot.com/technology/hum-smart-sex-toy/.

19. Eileen Brown, *The Internet of Things: Talking Socks and RFID Trash*, ZDNET (Oct. 4, 2012), http://www.zdnet.com/article/the-internet-of-things-talking-socks-and-rfid-trash/.

20. Timothy B. Lee, *Self-Driving Cars Are a Privacy Nightmare. And It's Totally Worth It*, WASH POST. (May 21, 2013), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/05/21/self-driving-cars-are-a-privacy-nightmare-and-its-totally-worth-it/.

21. Rosalind W. Picard & Jennifer Healey, *Affective Wearables*, 1:4 PERSONAL TECHNOLOGIES 231 (1997), *available at* http://affect.media.mit.edu/projectpages/archived/TR-432/TR-432.html.

22. Activity Monitoring Sys. & Methods of Operating Same, U.S. Patent No. 8,386,008 (filed Nov. 15, 2011) (issued Feb. 26 2013).

23. Eric Steiner, *Could This Tiny Stock be the Next Big Thing?*, VENTURE CAPITAL NEWS, http://www.venturecapitalnews.us/home/post/is-this-tiny-stock-the-next-big-thing/582?utm_source=taboola&utm_medium=futureplc-techradarus (last visited May 29, 2015).

24. Olivia Lutwak, *Student Creates Smart Maternity Wear*, CORNELL DAILY SUN (Jan. 25, 2015), http://cornellsun.com/blog/2015/01/25/student-creates-smart-maternity-wear/.

tors and tracks the baby's breathing, body position, sleep activity, and skin temperature.[25]

Preventing injury in sports is another big area for wearables. Smart socks, made by Heapsylon are infused with textile pressure sensors paired with a set of proprietary electronics that not only accurately track steps, speed, calories, altitude gain, environmental temperature, and distance, but also track cadence, foot landing technique, center of balance, and weight distribution on the foot to help prevent foot injuries for the large niche market of twenty-five million American runners.[26] Head injuries in contact sports have also been of tremendous concern over the last year.[27] Football helmets embedded with sensors that measure the force of collisions can send alerts to the sideline when a player's health may be in danger.[28] Rugby players on the Saracens English Premiership team wore small xPatch sensors taped behind their ears that gauge the impact of hits by rotation, title, movement, and speed of the head in a January match.[29]

Smart devices can also blur the lines of what is real creating an "augmented reality experience."[30] Smart glass like Google Glass[31] and Lumus DK-40[32] intend to enhance the experience of the everyday physical world by overlaying digital information onto the real world, providing additional content to the wearer as she moves through the environment. Microsoft's HoloLens "blends your digital world with your real world" through holograms providing not only new ways to interact with the real world but new ways of computing.[33] Microsoft's vision for HoloLens is to merge cyberspace with physical world:

> You used to compute on a screen, entering commands on a keyboard. Cyberspace was somewhere else. Computers responded to programs that detailed explicit commands. In the very near future, you'll compute in the physical world, using voice and gesture to summon data and layer it atop physical objects. Computer programs will be able to digest so much data that they'll be able to handle far more complex and nuanced situations. Cyberspace will be all around you.[34]

---

25. MIMO, http://mimobaby.com (last visited May 15, 2015).

26. Gregory Ferenstein, *Sensoria is a New Smart Sock that Coaches Runners in Real Time*, TECHCRUNCH (Jan. 7, 2014), http://techcrunch.com/2014/01/07/sensoria-is-a-new-smart-sock-that-coaches-runners-in-real-time/.

27. Patrick Hruby, *The NFL Dodges on Brain Injuries*, THE ATLANTIC (Sept. 4, 2014), http://www.theatlantic.com/entertainment/archive/2014/09/the-nfls-concussion-settlement-not-acceptable/379557/.

28. Brandon Griggs, *'Smart' Football Helmet May Help Detect Concussions,* CNN (June 9, 2014), http://www.cnn.com/2014/06/09/tech/innovation/smart-football-helmet-concussions/.

29. Peter Evan, *U.K. Rugby Team Tests Collision Sensor*, WALL ST. J. DIGITS (Jan. 5, 2015), http://blogs.wsj.com/digits/2015/01/05/u-k-rugby-team-tests-tackle-impact-sensor/.

30. AURASMA, http://www.aurasma.com/aura/ (last visited Apr. 22, 2015).

31. Taylor Hatmaker, *Google Explains Why and How Glass Failed*, DAILY DOT (Mar. 17, 2015), http://www.dailydot.com/technology/google-glass-failure-astro-teller/; Matt Mills, *Image Recognition that Triggers Augmented Reality*, TED TALK (June 2012), http://www.ted.com/talks/matt_mills_image_recognition_that_triggers_augmented_reality?language=en.

32. LUMUS OPTICAL, http://www.lumus-optical.com/ (last visited May 15, 2015).

33. Jessie Hempel, *Project Hololens: Our Exclusive Hands-On With Microsoft's Holographic Goggles*, WIRED (Jan. 21, 2015), http://www.wired.com/2015/01/microsoft-hands-on/.

34. *Id.*

Others are putting devices directly into the body, not on top of it. Ultimately, these devices can go beyond hand-held or wearable technology, augmenting the physical self through implanted microchips. Radio-frequency identification (RFID) microchips are used to access subways, busses, phones, and bank accounts.[35] Dangerous Things sells an RFID tag and injection kit for $57,[36] and the Cyborg Foundation "aims to help people become cyborgs."[37] Cyborg Foundation projects explore the use of implants and prosthetics to allow users to hear colors, perceive the exact speed of movements, and feel the approach of people behind them.[38]

C. Smart Spaces

Smart things and smart people will not exist in a vacuum. They will be out, interacting with and in smart spaces. Information infrastructure will increasingly be a source of competition between cities.[39] Cities are looking to the smart technologies to cope with fluctuating populations and are being used to support three main issues: energy consumption, waste, and congestions.[40] Intelligent buildings, lighting, emergency systems, transportation, etc. contribute to improving these issues. For example, "[a] fire alarm would not simply call out fire engines: it could determine their best route, redirect traffic away from it, warn downwind schools to close their windows and make sure that there were no nearby water mains shut down for maintenance."[41] Smart street lights that dim automatically when no one is around save electricity; water mains can inform city managers when to replace or repair them; and parking spaces signal to nearby cameras that they are empty and available to drivers.[42]

The "Bristol is Open" project makes Bristol the "world's first programmable city," according to Professor Dimitra Simeonidou, Professor of High Performance Networks at the University of Bristol, which partnered with the city for the initiative.[43] Barcelona has plans to use smart lighting systems for more than power savings; the city intends to utilize data to identify open parking spots, lines at museums, full garbage cans, and "suspicious movements of people."[44] Every car that enters central London is already logged by the traffic congestion system and every

35. Frank Swain, *Why I Want a Microchip Implant*, BBC (Feb. 10, 2014), http://www.bbc.com/future/story/20140209-why-i-want-a-microchip-implant.

36. xEM Glass RFID Tag + Injection Kit, DANGEROUS THINGS, https://dangerousthings.com/shop/xemi-em4200-2x12mm-injection-kit/ (last visited May 15, 2015).

37. THE CYBORG FOUNDATION, http://cyborgism.wix.com/cyborg (last visited May 15, 2015).

38. Frank Swain, *Cyborgs: The Truth About Human Augmentation*, BBC (Sep. 24, 2014), http://www.bbc.com/future/story/20140924-the-greatest-myths-about-cyborgs.

39. *The Multiplexed Metropolis*, ECONOMIST (Sept. 7, 2013), http://www.economist.com/news/briefing/21585002-enthusiasts-think-data-services-can-change-cities-century-much-electricity.

40. Peter High, *The Top Five Smart Cities in the World*, FORBES (Mar. 9, 2015), http://www.forbes.com/sites/peterhigh/2015/03/09/the-top-five-smart-cities-in-the-world/.

41. *The Multiplexed Metropolis*, *supra* note 39.

42. Shalene Gupta, *Cites Dream of a "Smart" Sci-Fi Future*, FORTUNE (Jan. 26, 2015), http://fortune.com/2015/01/26/kansas-city-smart-city/.

43. Doug Drinkwater, *Bristol Launches 'Smart' City Amid Privacy Doubts*, SC MAGAZINE (Mar. 12, 2015), http://www.scmagazineuk.com/bristol-launches-smart-city-amid-privacy-doubts/article/403099/.

44. *The Multiplexed Metropolis*, *supra* note 39.

street corner in Chongqing and Dubai are equipped with CCTV.[45] Navigating these smart publics entails the opportunity for an unprecedented amount of data creation, collection, and processing and new hurdles for controlling and managing personal information.

III. PRIVACY IN PUBLIC

Law scholar and privacy expert Joel Reidenberg has extrapolated on an ever-public reality by breaking down the recent socio-technical changes into three stages.[46] The first stage is when private information was secured through obscurity and was not readily available as a practical matter.[47] The second is when that information became accessible through digital and surveillance technologies.[48] The last stage has occurred when accessible information became transparent and received wide publicity through search technologies, personalized notifications, and integrated social media platforms.[49] This shift places significant strain on existing privacy concepts and practices that depended on a boundary between private and public.[50]

A. Notice & Choice

Performing the boundary work necessary to managing one's information becomes increasingly difficult as we move deeper into the Information Age. Currently, we have the luxury of screens to click through and determine whether a site or service collects and processes personal information in ways we are comfortable with and accept those terms by utilizing the site or service. The notice and choice model involves notification to users on terms of service pages or pop-ups and users may choose to engage with the site or service or move on to another.[51]

45. *Id.*
46. Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141 (2014).
47. *Id.* at 148.
48. *Id*. at 148–50.
49. *Id*. at 150–52.
50. Privacy scholars have taken up the challenge of theorizing privacy in public. Helen Nissenbaum has also been working on protecting privacy in public since the late 1990s. Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW AND PHILOSOPHY 559 (1998). In her 2010 book, Nissenbaum emphasizes reliance on norms to protect privacy in public. Under this context-based concept of privacy, when information flow expectations are violated, whether in traditionally public environments or information sharing relationships, contextual integrity is violated and a privacy violation has occurred. *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009). Julie Cohen reimagines privacy as gaps in the digital world that would otherwise be seamless and opaque. These gaps are necessary to human flourishing by allowing for unpredictability, creativity, and critical subjectivity. *See* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012).
51. *See* Scott McCoy et al., *The Effects of Online Advertising*, COMMUNICATIONS OF THE ACM, Mar. 2007, at 84–88.

FIGURE 1. University of Idaho Web Site Usage notice.

The screenshot above shows the large number of tabs regularly open and the terms of service for the University of Idaho website, which states "Before using the Website it is your responsibility to read these standards."[52] The page then links to specific ways in which the site uses cookies and beacons. This model has been heavily criticized since the early days of the internet and is increasingly condemned the more entrenched connected devices become in everyday life.

Daniel Solove concisely describes the strain on notice and choice in his article *Privacy Self-Management and the Consent Dilemma*.[53] He explains "Privacy self-management takes refuge in consent. Consent legitimizes nearly any form of collection, use, or disclosure of personal data… [I]t is being tasked with doing work beyond its capabilities. Privacy self-management does not provide people with meaningful control over their data."[54] This is because it is difficult to inform users about information practices in a way that is comprehensible.[55] Individuals remain

52. UNIVERSITY OF IDAHO, POLICIES AND COPYRIGHTS, http://www.uidaho.edu/policiesandcopyrights/usage (last visited May 15, 2015).

53. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 26 HARV. L. REV. 1880 (2013).

54. *Id.* at 1880.

55. *Id.* at 1882–88.

uninformed because reading of the terms of services one encounters in a day is unrealistic.[56] Lorrie Faith Cranor and Aleecia McDonald found that users would need to spend seventy-six work days a year just reading privacy policies for pages visited.[57] Even if one were able to do so, terms of services are difficult to understand; even when simplified, data processing, trading, and future uses are challenging to communicate accurately and understandably.[58] *And even if* people could read and understand privacy terms of services, it is difficult to assess abstract and uncertain future harms.[59]

The traditional notice and choice model, as flawed as it may be, is not available as individuals move through smart publics. Walking through a grocery store equipped with cameras that recognize customers and track their movements throughout the space, sensors that identify and weigh individual products, and automatically charge you for your items as you walk out the door is an experience not conducive to providing notice and consent in a similar way to having numerous screens and apps open at any given time is not conducive to reading long and confusing terms of service – but the smart public is full of data collection devices the individual may not even be aware of.

Smart publics expose us to objects, people, and places that we interact with but may be beyond our control or awareness. For instance, getting into another's driverless car, going to another's home that utilizes a Jibo (a family robot to assist in running a household by using facial recognition and creating a profile for each person with the goal of connecting to other devices in the home),[60] and walking into a lobby that utilizes the NeoFace[61] facial recognition system moves the user beyond the realm of control.

While individuals may be able to choose not get into a very smart driverless car, go over to a Jibo house, and networked retailers or buildings, it is difficult to combat the way in which smart equipment is utilized in traditional public spaces by others. Walking through a park may expose you to any number of smart people (like Google Glass or LifeLog wearers), smart objects (from police vehicles equipped with cameras[62] to public transportation systems[63]), or smart spaces (including technology currently in place which utilizes facial recognition, license plate readers, and audio analytics).

There is no opportunity for notice and choice in smart publics or any smart shared space. This form of governance is simply not available in the internet of other people's things. This is a challenge that has not been overlooked by privacy agencies.

---

56. *Id.*

57. Aleecia McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4:3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 540 (2008).

58. Solove, *supra* note 53, at 1882–88.

59. *Id.*

60. *See* JIBO, http://www.jibo.com (last visited May 15, 2015).

61. *See* NEOFACE FACIAL RECOGNITION, http://au.nec.com/en_AU/solutions/security-and-public-safety/biometrics/neoface-facial-recognition-overview.html (last visited May 15, 2015).

62. Lindsay Hiebert, *How Internet of Things is Transforming Public Safety*, CISCO BLOG (Apr. 21, 2015, 3:54 PM), http://blogs.cisco.com/ioe/how-internet-of-things-is-transforming-public-safety.

63. *Bringing the Internet of Things to the London Underground*, MONEYCONTROL.COM, http://www.moneycontrol.com/video/it/bringinginternetthings-tolondon-underground_1242062.html (last visited May 15, 2015).

B. United States

In anticipation of this challenging environment, networked by 50 billion devices by 2020, the FTC hosted a workshop in November, 2013 and released an accompanying report in January of 2015.[64] The report noted that security is of utmost importance, but not the particular focus of this paper. Three other principles of the Fair Information Practices Principles, relied on for decades now were also emphasized: data minimization, notice, and choice.[65] Data minimization refers to the principles that data collects should limit the data collected and retained to the purpose for which it is collected when it is no longer needed.[66] It limits security threats by providing a less valuable data source to hack and the risks that information will be used a way the user would not expect or want.[67] The FTC staff concluded that data collectors can decide (1) not to collect data at all; (2) collect only the fields of data necessary for the product or service offered; (3) collect less sensitive data; (4) deidentify the data collected; or (5) get consent for additional unexpected categories of data.[68]

As discussed above, notice and consent schemes are incredibly challenging in this landscape – it has been challenging to rely on this gold standard for a number of years, but working through the other options reveals challenges as well. Options (3) and (4) are problematic because the combination of data sources can quickly turn mundane information into sensitive information and deidentified information into identifiable information. Collecting no data at all seems to defeat the purpose. Choice (2) resembles the purpose specify principle that has begun to wane in light of big data practices but could certainly be revitalized moving forward.

Dissenting from the report was Commissioner Joshua Wright. He disapproves of the production of policy recommendations through the workshop process, which he explains usually only "synthesize the record developed during the proceedings."[69] More importantly, Commissioner Wright is

> …unconvinced that the proposed framework described in the Workshop Report – a combination of Fair Information Practice Principles as well as other concepts such as 'security by design' – is the proper framework to apply to the still-nascent Internet of Things… To the extent concepts such as security by design or data minimization are endorsed at *any* cost – or without regard to whether the marginal cost of a particular decision exceeds its marginal benefits – then application of these principles will result in greater compliance costs without countervailing benefit. Such costs will be passed on to consumers in the form of higher prices or less useful prod-

64. INTERNET OF THINGS, *supra* note 10.
65. *Id.*
66. *Id.*
67. *Id.*
68. *Id.*
69. JOSHUA D. WRIGHT, DISSENTING STATEMENT OF COMMISSIONER JOSHUA D. WRIGHT: ISSUANCE OF THE INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD STAFF REPORT 1 (2015) *available at* https://www.ftc.gov/system/files/documents/public_statements/620701/150127iotjdwstmt.pdf.

> ucts, as well as potentially deter competition and innovation among firms participating in the Internet of Things.[70]

Commissioner Wright is not the only one wary of regulating this still-blossoming field of technological development. FTC Commissioner Maureen K. Ohlhausen argued in a 2013 speech,

> [T]he success of the Internet has in large part been driven by the freedom to experiment with different business models, the best of which have survived and thrived, even in the face of initial unfamiliarity and unease about the impact on consumers and competitors… It is… vital that government officials, like myself, approach new technologies with a dose of regulatory humility, by work hard to educate ourselves and others about the innovation, understand its effects on consumers and the marketplace, identify benefits and likely harms, and if harms do arise, consider whether existing laws and regulations are sufficient to address them, before assuming new rules are required.[71]

C. European Union

Although a pro-innovation stance may be preventing some anticipatory governance in the U.S., the European Union has been working on IoT since 2009 (with a press release entitled "When Your Yogurt Pots Start Talking to You: Europe Prepares for the Internet Revolution")[72] and created initiatives, including the European Research Cluster on the Internet of Things (IERC) that has produced a number of events and documents[73] that build off its work on RFID technologies in the mid-2000s.[74] The E.U. also perceives the smart world as big innovation and big money:

> Whereas in the first run Internet of Things referred to the advent of barcodes and Radio-frequency identification (FID), helping to automate inventory, tracking and basic identification, the second current wave of IoT sees a strong verve for connecting sensors, objects, devices, data and applications. The next wave could be called a "cognitive IoT", facilitating object and data reuse across application domains, leveraging on hyper-connectivity, interoperability solutions and semantic enriched information distribution, incorporating intelligence at different levels, in the objects,

---

70. *Id*. at 4.

71. Maureen K. Ohlhausen, Comm'r, FTC, The Internet of Things and the FTC: Does Innovation Require Intervention?, Remarks Before the U.S. Chamber of Commerce 3–4 (Oct. 18, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/internet-things-ftc-does-innovation-require-intervention/131018chamber.pdf.

72. Eur. Comm'n, *Future Networks and the Internet – Early Challenges to the Internet of Things* (Sept. 29, 2008) (unpublished working paper), *available at* http://ec.europa.eu/information_society/policy/rfid/documents/earlychallengesIOT.pdf.

73. Press Release, Eur. Comm'n, When Your Yogurt Pots Start Talking to You: Europe Prepares for the Internet Revolution, (June 18, 2009), *available at* http://europa.eu/rapid/press-release_IP-09-952_en.htm?locale=en.

74. *See* Press Release, Eur. Comm'n, Commission Launches Public Consultation on Radio Frequency ID Tags, (Mar. 9, 2006), *available at* http://europa.eu/rapid/press-release_IP-06-289_en.htm?locale=en; *see also* Press Release, Eur. Comm'n, Commission Proposes a European Policy Strategy for Smart Radio Tags, (Mar. 15, 2007), *available at* https://ec.europa.eu/digital-agenda/en/news/commission-proposes-european-policy-strategy-smart-radio-tags.

> devices, network(s), systems and in the applications for evidence-based decision making and priority setting. Economically, it could generate billions of Euros that easily translate into growth and employment, provided it ensures trust and security for the European citizens and businesses.[75]

Like in the U.S., E.U. industry stakeholders find no need for new rules and most citizens and consumers find the existing framework insufficient. Unlike in the U.S., however, notice and choice remains central to E.U. data protection.

The Article 29 Working Party (A29WP), an independent body made up of representatives from the data protection authorities across the E.U. to provide expert advice to member states and the Commission, published an opinion focused mainly on wearable and other quantified self technologies, as well as household automation devices from smart light bulbs to toasters.[76] The Opinion emphasized six concerns about personal information: lack of control and information asymmetry, quality of consent, inferences derived from data, patterns and profiling, limitations on anonymity, and security risks.[77]

The A29WP was able to provide specific recommendations to a number of parties.[78] They include:

- All stakeholders should: prepare privacy impact assessments, delete data when no longer necessary, implement privacy by design and default, allow users to control their data, and provide user friendly consent regimes.
- Operating system and device manufacturers should: hold responsibility for limiting as much data as possible from leaving smart devices, offer a "do not collect" option, inform other stakeholders immediately when consent is withdrawn, provide a way for individuals to access and move their data, be able to distinguish between users, and engage with standards bodies to establish common protocols and enable to use of proxies to store and process data on the device, as opposed to the cloud.
- App developers should: practice data minimization, provide access and data portability, and provide notice.
- Social media platforms should: prohibit default publishing or search indexing of content and provide ways for users to better understand when and how information will be shared.
- Standards bodies should: develop security and privacy protocols.
- Operators should: maintain control of the device where she is the owner in a contractual relationship, but all data subjects should be able to access and oppose data collection and processing.

---

75. *The Internet of Things*, Digital Agenda for Eur., http://ec.europa.eu/digital-agenda/en/internet-things (last visited Feb. 17, 2015).

76. Article 29 Data Protection, *supra* note 11.

77. *Id*. at 1–9.

78. *Id*. at 21–24.

While one may think that policy approaches to smart worlds would be more situated in the geographical, physical realm, the A29WP opinion emphasized the virtual aspects of these devices and the compliance requirements for all data controllers that use "equipment" located in a member state.[79] Suppliers of smart equipment will be deemed to be established in the E.U. under Article 4.1(d) of the Data Protection Directive, according to the Opinion.[80] A greater reach is included the opinion; even if device manufacturers do not collect and process data on the equipment they manufacture, the Opinion suggests that the manufactures may be considered a data controller, because by designing the device, the manufacturer determines the means and purposes for which data is collected and processed and may be classed as a data controller.[81] This application of the Directive would make smart device manufactures liable for the subsequent uses of data.

The Opinion references the recent (May 2014) "right to be forgotten" case, which held Google Inc.'s subsidiary in Spain sufficient to extend jurisdiction to the parent company and declared Google a data controller for the purposes of its search operations, to explain how broadly the A29WP would interpret the Directive in an IoT setting.[82] If U.S. companies want to provide smart services and/or a piece of the European smart data pot and the U.S. government to promote international interoperability, they will need to find a way to meet or change E.U. standards.

D. Newness

While the FTC and the A29WP approach the internet of other people's things differently, both treat the smart future as extensions of the cyber and big data sociotechnical policy issues. The entities describe the smart public by the detailing the underlying IoT, which are simply *connected* devices that are *smart* by utilizing big data. When considering, debating, and regulating emerging technology, framing matters. Various legal cultures reflect, what science and technology studies scholar Sheila Jasanoff calls, diverse "civic epistemologies" that shape the way in which policy issues are framed,[83] but in this instance, there is little variation in the way in which the technology itself is framed. This is a missed opportunity on both sides of the Atlantic.

Of course IoT is an extension of the internet, big data, robotics, algorithmic living, and a number of other computational shifts, all of which present new forms of newness every day, but smart futures present an experience wherein the foundational system for information sharing is not even an option. It is new in a way that matters to law and policy. This line of reasoning should not be confused with exceptionalism, which focuses on the way in which technology presents new capabilities signaling a need to overhaul the law or the development of a new field of study.[84] Instead, what I mean by newness is a moment of departure in what Thomas

79. *Id*. at 10.
80. *Id*. at 10–12.
81. *Id*. at 11.
82. Article 29 Data Protection Working Party, *supra* note 11, at 15.
83. SHEILA JASANOFF, THE DESIGNS OF NATURE: SCIENCE AND DEMOCRACY IN EUROPE AND THE UNITED STATES 247 (2005).
84. Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CAL. L. REV. (forthcoming 2015); Jack M. Balkin, *The Path of Robotics Law*, 103 CAL. L. REV. (forthcoming 2015).

Hughes calls technological momentum.[85] As new radical technologies are introduced, they are socially deterministic,[86] meaning value and ethical disputes arise, risks and benefits are revisited, numerous competitors are engaged in yet to be defined markets, and whether and how rules apply is unclear. As technologies gain momentum, standards, expectations, business models, and investments contribute to a shift toward technological determinism,[87] wherein it is very challenging to change course or pass new laws that would significantly disrupt the technology as usual.

The newness that matters here is the loss of the screen. Framing the smart future as new unties the hands of policy-makers, designers, users, and scholars to reimagine information arrangements moving forward – it places IoT on a new cycle of technological momentum and in a discourse of social, as opposed to technological, determinism. By ignoring this newness, agencies are stuck within the framework of existing information challenges. They miss the opportunity to achieve what both appear to be pursuing – establish meaningful digital privacy for the smart future.

IV. SMART PRIVACY

The smart future has been called "a legal nightmare"[88] and perhaps the "the death of privacy,"[89] but there is room for innovating privacy along with smart publics. There is a great deal of time and energy devoted to imaging the potential for this future, but just as much time should be devoted to imaging innovative privacy regimes. One response to this lack of control over personal information is to limit the use of smart products and systems, like the small anti-google glass movement that occurred upon the wearable's release and prompted signs to be posted in shop windows.[90] Limiting data collection, by type or amount, may limit the benefits and functionality networked devices and smart worlds can provide and has proven to an uphill battle as big data debates about the purpose-specificity principle continue. Currently the options are presented as privacy or innovation – either but not both.

"By 2025, the current debate about privacy will seem quaint and old-fashioned," wrote Hal Varian, Google's chief economist, in the comments of a survey administered by Pew Research Center and Elon University.[91] In many ways privacy's dichotomous crisis is reminiscent of the copyright crisis in the late 1990s when music was free and illegal and expensive.[92] Then iTunes and other

85. Thomas P. Hughes, *Technological Momentum*, *in* DOES TECHNOLOGY DRIVE HISTORY? 101 (Merritt Roe Smith and Leo Marx, eds. 1994).

86. *Id*.

87. *Id*.

88. T.C. Sottek, *The Internet of Things is Going to be a Legal Nightmare*, THE VERGE (Jan. 27, 2015, 10:35 AM), http://www.theverge.com/2015/1/27/7921025/will-self-regulation-be-a-huge-problem-for-privacy-in-the-internet-of.

89. Klint Finley, *Hacked Fridges Aren't The Internet of Things' Biggest Worry*, WIRED (Mar. 12, 2015, 8:00 AM), http://www.wired.com/2015/03/hacked-fridges-arent-internet-things-biggest-worry/.

90. *Strategic Pause*, STOP THE CYBORGS (Jan. 20, 2015), http://stopthecyborgs.org/.

91. Rainie & Anderson, *supra* note 12, at 28.

92. *See* Matthew Green, Note, *Napster Opens Pandora's Box: Examining How File-Sharing Services Threaten the Enforcement of Copyright on the Internet*, 63 OHIO ST. LJ 799, 801–02 (2002); Rebecca J. Hill, Comment, *Pirates of the 21st Century: The Threat and Promise of Digital Audio Technology on the Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 311, 324 (2000); Ariel Berschad-

platforms came along with an infrastructure that supported the middle.[93] Whether this saved or killed the music industry is still up for debate,[94] but these platforms created a legitimate, easy to use competitor to piracy and "[i]n less than 10 years, iTunes has become so embedded in people's everyday lives that it has all but disappeared into the overall fabric of our digital commerce."[95] The privacy debates may seem quaint and old fashioned not because things will get more complex, but because a platform for the middle will mitigate the drama of dichotomy.

We are currently in a phase where data about us is created, shared, and analyzed at every turn and mechanisms of control have been futile, but that does not have to be the future. Without the ability to rely on notice from the data collector and choice by the user, a new opportunity is presented. There is potential for more privacy in smart spaces than in the screen world. It is early enough in the process to establish a foundation of functionality and privacy. One way of shaking up the privacy paradigms is to put operators of smart systems on notice of user choice through commonly used controls and predictive analytics. Supported by the development of adaptive participation infrastructure, such a system would allow individuals to push their privacy preferences into smart publics. Data protection agencies would then play an important role in supporting and enforcing of these preferences.

A. Choice & Notice

Moving the internet beyond the screen is an opportunity for privacy. It does not have to be the death rattle or stall innovation. We have learned a great deal from privacy with screens, particularly as more and more screens invaded our lives. Building an infrastructure that promotes a new model of notice and choice could bring in a new era of privacy to match a new era of connectivity.

The current model of notice and choice places the burden on the user to understand and accept data practices articulated by the collector. This burden has been criticized as discussed above. Although Solove criticizes continued attempts to improve self-management models,[96] perhaps the lessons gained from privacy with screens can help innovate self-management for privacy without screens. There is an opportunity to flip notice and choice on its head and place the burden on the collector to take notice of the choice made by the user. The user first choices their privacy preferences and then notifies the system.

---

sky, *RIAA v. NAPSTER: A Window onto the Future of Copyright Law in the Internet Age*, 18 J. MARSHALL J. COMPUTER & INFO. L. 755, 766 (1999).

93. Nathan Ingraham, *iTunes Store at 10: How Apple Built a Digital Media Juggernaut*, THE VERGE (Apr. 26, 2013, 11:56 AM), http://www.theverge.com/2013/4/26/4265172/itunes-store-at-10-how-apple-built-a-digital-media-juggernaut.

94. Ed Nash, Op-Ed., *How Steve Jobs Saved the Music Industry*, WALL ST. J., Oct. 21, 2011, at A15; Andrew Leonard, *The Music Industry is Still Screwed: Why Spotify, Amazon and iTunes Can't Save Musical Artists*, SALON (Jun. 20, 2014), http://www.salon.com/2014/06/20/the_music_industry_is_still_screwed_why_spotify_amazon_and_itunes_cant_save_musical_artists/.

95. Alex Pham & Glenn Peoples, *Seven Ways iTunes Changed the Music Industry*, BILLBOARD (Apr. 25, 2013, 4:34 PM), http://www.billboard.com/biz/articles/news/1559622/seven-ways-itunes-changed-the-music-industry.

96. Solove, *supra* note 53.

Unlike many privacy enhancing technologies (PETs), this system would not be designed to better inform the user of how their information will be used like P3P[97] or simplified privacy labels.[98] Nor is it like legal solutions that simplify terms of service, conspicuously inform the user of any abnormalities, or otherwise nudge their behavior.[99] These efforts sought to improve notice and choice – ways in which the *collector may signal to the user* how they will collect and process data. Instead, choice and notice would signal the privacy preferences of the *user to the collector* through the connected devices.

97. Lorrie Faith Cranor, *P3P: Making Privacy Policies More Useful*, 1(6) IEEE SECURITY & PRIVACY 50 (2003), *available at* http://users.ece.cmu.edu/~adrian/630-f05/readings/cranor-p2p.pdf.

98. Patrick Gage Kelley et al., *A "Nutrition Label" for Privacy*, *in* PROCEEDINGS OF THE 5TH SYMPOSIUM ON USABLE PRIVACY AND SECURITY (2009), *available at* https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf.

99. *See* Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1033 (2012).

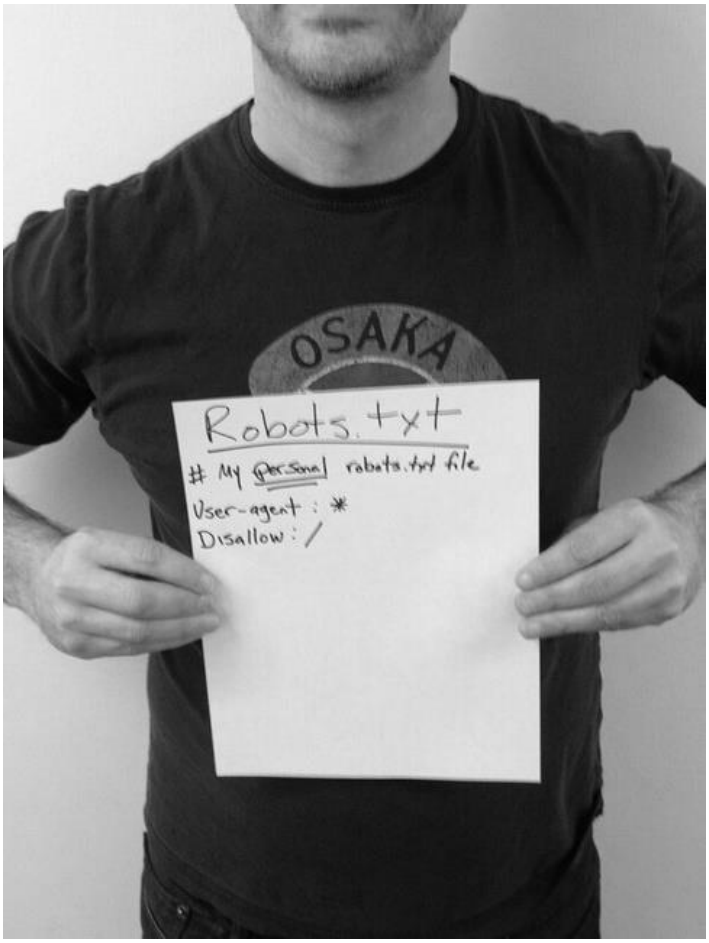

FIGURE 2. Greg Vincent low-tech version of a signaling protocol for wearables presented in Quora forum.[100]

In order for choice and notice to work, individuals will need user controls that they understand and regularly engage with, like Facebook's privacy management tools.[101] These are tools that allow users to become active and sophisticated managers of their identity and associated information in the social media context.[102]

100. *What are Some Potential Solutions to Issues Regarding Google Glass and Privacy?*, QUORA (Mar. 12, 2013), http://www.quora.com/What-are-some-potential-solutions-to-issues-regarding-Google-Glass-and-privacy.

101. Danah Boyd & Eszter Hargittai, *Facebook Privacy Settings: Who Cares?*, FIRST MONDAY (Aug. 2, 2010), http://firstmonday.org/ojs/index.php/fm/article/view/3086/2589; Zeynep Tufekci, *Facebook, Youth and Privacy in Networked Publics*, *in* PROCEEDINGS OF THE SIXTH INTERNATIONAL CONFERENCE ON WEBLOGS AND SOCIAL MEDIA (2012), *available at* https://www.aaai.org/ocs/index.php/ICWSM/ICWSM12/paper/download/4668/5001.

102 *Id.*

FIGURE 3. Facebook mobile privacy settings display.[103]

Danah Boyd and Eszter Hargittai find that young adult Facebook users regularly engage in managing their privacy settings.[104] The company initiated a privacy checkup tool in 2014 to nudge users to manage those settings and align their expectations with the actual sharing settings.[105]

103. Matt Hicks, *More Control on Mobile*, Facebook (Dec. 8, 2010), https://www.facebook.com/notes/facebook/more-control-on-mobile/463829602130.

104. Danah Boyd & Eszter Hargittai, *Facebook Privacy Settings: Who Cares?*, FIRST MONDAY (Aug. 2, 2010), http://firstmonday.org/ojs/index.php/fm/article/view/3086/2589.

105. Vindu Goel, *Some Privacy, Please? Facebook, Under Pressure, Gets the Message*, N.Y. TIMES (May 22, 2014), http://www.nytimes.com/2014/05/23/technology/facebook-offers-privacy-checkup-to-all-1-28-billion-users.html?_r=0.

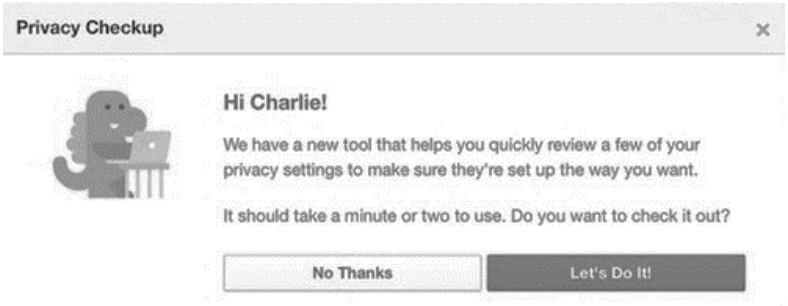

FIGURE 4. Facebook Privacy Checkup tool.[106]

Pushing these types of preferences out of the social media context and into a world without screens involves a change in default from notice and choice to choice and notice.

Of course, this sounds similar to Do Not Track[107] but has two distinct differences. The first is that preferences are not all or nothing – they are nuanced preferences which are significantly less political than default rules about opt-in or opt-out.[108] The second is that Do Not Track suffered greatly under the pacing problem.[109] The initiative could not get its stakeholders to agree on changes once they were so heavily invested in the way the internet worked.[110] The smart world is not yet upon us—invested parties have not yet to establish "business as usual"—and the time is ripe to encourage and develop a system that adheres to information preferences.

---

106. Zach Miners, *New Facebook Tool Walks Users through a Privacy Settings Checkup*, PC WORLD (Sept. 4, 2014), http://www.pcworld.com/article/2602843/new-facebook-tool-walks-users-through-a-privacy-settings-checkup.html.

107. Do Not Track is described as follows: "Do Not Track is a technology and policy proposal that enables users to opt out of tracking by websites they do not visit, including analytics services, advertising networks, and social platforms. At present few of these third parties offer a reliable tracking opt out, and tools for blocking them are neither user-friendly nor comprehensive. Much like the popular Do Not Call registry, Do Not Track provides users with a single, simple, persistent choice to opt out of third-party web tracking." *Do Not Track: Universal Web Tracking Opt Out*, DO NOT TRACK, http://donottrack.us/ (last visited May 28, 2015); Peter Swire, *How to Prevent the 'Do Not Track' Arms Race*, WIRED (Apr. 24, 2013), http://www.wired.com/2013/04/do-not-track/.

108. Swire, *supra* note 107; Katy Bachman, *W3C Group Rejects Industry Do Not Track Proposal Consensus Elusive as Adoption Deadline Nears*, ADWEEK (July 16, 2013), http://www.adweek.com/news/technology/w3c-group-rejects-industry-do-not-track-proposal-151185; Scott Gilbertson, *Yahoo, Microsoft Tiff Highlights the Epic Failure of 'Do Not Track'*, WIRED (Nov. 29, 2012), http://www.wired.com/2012/10/yahoo-microsoft-tiff-highlights-the-epic-failure-of-do-not-track/.

109. Gary E. Marchant, *The Growing Gap Between Emerging Technologies and the Law*, *in* THE GROWING GAP BETWEEN EMERGING TECHNOLOGIES AND LEGAL-ETHICAL OVERSIGHT 19–33 (Gary E. Marchant, Braden R. Allenby, and Joseph R. Herkert eds., 2011).

110. For details of the derailed effort *see, e.g.*, David Goldman, *Do Not Track Proposal is DOA*, CNN MONEY (July 16, 2013), http://money.cnn.com/2013/07/16/technology/do-not-track/; Natasha Singer, *Do Not Track? Advertisers Say 'Don't Tread on Us*,' NY TIMES (Oct. 13, 2012), http://www.nytimes.com/2012/10/14/technology/do-not-track-movement-is-drawing-advertisers-fire.html?_r=0.

Even with these controls, users will not be able to create a setting for every conceivable use of their information. The system will need to guess sometimes. These should be good guesses based on the existing user settings provided and what is known about the user – predictive privacy preferences. For instance, my privacy settings may explicitly signal that I am sensitive to health information. Knowing that, in addition to the fact that I am a female of a certain age with certain interests and other information practices should give the system an idea about whether to collect or use my information in a particular way. We are all different, but often not all that different, which is why predictive advertising, hiring, and loans are so appealing in the first place. These types of predictive privacy profiles have been ignored in favor of understanding what users may want to buy. Target is able to determine when a customer is pregnant if she buys a certain set of items.[111] The company can tell how far along in a pregnancy a woman is, but does not know that such knowledge would be considered invasive.[112] Solving this gap in knowledge should be (and will need to be) a goal of privacy without screens.

Finally, there is a need for a backend structure that affords a form of accountability, retroactive participation, and levels of anonymity. There must be a way to determine whether data is being used in accordance with preferences and enforce preferences as data moves downstream to other data processors. Even though few users engage in this type of backend self-management, its availability remains important for accountability.

B. Caveats

There are three significant problems with this infrastructure. The first is that it relies on the smart phone to be the control device for identity management. If an individual does not have a control device, they are susceptible to the invasive information practices. Smart privacy systems may need to function similarly to a default do not track setting in that if no signal of privacy preferences is made, no collection should take place to avoid abuse of individuals not carrying or wearing such devices.

The next problem relates to the existing observational surveillance systems. Currently, systems in place turn observations, such as face details, into data.[113] These systems would need to be altered to look for signaled privacy preferences prior to turning observations into data.

Additionally, it would be difficult for a phone to send a signal to a camera like the gigapixel camera developed by the Israeli start-up, Adaptive Imaging Technologies, which won the "Most Promising Startup" award from Global Security Challenge in 2009.[114] While most cameras in use have a resolution of around 1-15 megapixels, with a resolution of 1,000 megapixels, gigapixel can replace entire

111. 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/.

112. *Id.*

113. *See, e.g.*, NEOFACE FACIAL RECOGNITION, *supra* note 611.

114. Ben Hartman, *Israeli Start-Up Expects Success After Win at Int'l Competition*, THE JERUSALEM POST (Nov. 30, 2009), http://www.jpost.com/Health-and-Sci-Tech/Israeli-start-up-expects-success-after-win-at-intl-competition.

surveillance systems, usually made up of several cameras in one area.[115] In 2013, DARPA revealed its Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS-IS), which utilizes a 1.8 gigapixel camera.[116] These long-distance surveillance systems may need to be legally restricted to not identify individuals.

The final problem is that this infrastructure may lead to centralized control of information and favors incumbents. Companies that users are already comfortable with will be the most likely to take their identity management systems beyond the screen. They will also have the most data to perform predictive privacy preferences, and so are in the best position to implement and operate these infrastructures, giving them even more power and control.

C. Role of Law

In this imagined privacy future, the role of governmental agencies is limited to encouraging the development of such an infrastructure and enforcing the system. It appears that the U.S. is somewhat behind the E.U. in terms of treating smart publics systematically. The U.S. remains bound to FIPPs but inclined to weaken notice and choice requirements and favor putting use restrictions in place. The FTC report explains:

> Staff acknowledges the practical difficulty of providing choice when there is no consumer interface and recognizes that there is no one-size-fits-all approach. Some options include developing video tutorials, affixing QR codes on devices, and providing choices at point of sale, within set-up wizards, or in a privacy dashboard. Whatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents.[117]

Although there is a reference to a privacy dashboard, these recommendations ask the company to make choices about how they are going to treat consumer information—all consumer information—and a number of ways to provide notice.[118] These forms of notice have the same shortcomings as screen-based notices. Choice is not necessary for data collection within user expectations and context, according to the report, which then emphasizes restrictions on use, making clear it will not utilize a pure use-based model.[119] Use-based models are intended to address the information asymmetry between collector and user, and relieve the overburdened user from unreasonable participation requirements.[120] The White House Big Data Report emphasized the importance of use:

---

115. *Id.*

116. Nicole Lee, *DARPA's 1.8-Gigapixel Cam Touts Surveillance from 20,000 Feet*, ENGADGET (Jan. 28, 2013, 9:46 PM), http://www.engadget.com/2013/01/28/darpa-argus-is-surveillance/.

117. INTERNET OF THINGS, *supra* note 10, at v.

N118. *Id.*

119. *Id.*

120. *See, e.g.*, "Accountability in Action: The Microsoft Privacy Program," Microsoft White Paper (Feb. 2012); Mary J. Culnan, *Accountability as the Basis for Regulating Privacy: Can Information Security Regulations Inform Privacy Policy?*, PRIVACY LAW SCHOLARS CONFERENCE (2011), available at https://www.futureofprivacy.org/wp-
con-

> Putting greater emphasis on a responsible use framework has many potential advantages. It shifts the responsibility from the individual, who is not well equipped to understand or contest consent notices as they are currently structured in the marketplace, to the entities that collect, maintain, and use data. Focusing on responsible use also holds data collectors and users accountable for how they manage the data and any harms it causes, rather than narrowly defining their responsibility to whether they properly obtained consent at the time of collection.[121]

The A29WP took a stance against this movement away from user choice in September of 2014 stating, "[U]sers must remain in complete control of their personal data throughout the product lifecycle, and when organisations rely on consent as a basis for processing, the consent should be fully informed, freely given and specific."[122]

Although the U.S. approach is seemingly more innovative (accepting a big data world and focusing on use) than the European approach, the European's hold on notice and consent requires the concept to be reimagined, and in the end, may incentivize smart publics that promote greater innovation than in the U.S. The European approach is also more systematic, providing guidance for a number of stakeholders involved in any future infrastructure, but also extends compliance and liability throughout that infrastructure in a way that may significantly restrict innovation of smart devices. Both have remained tied to previous models, but privacy without screens will require regulatory models and information practices to be reimagined. The essay presents only one imagined future for privacy without screens; there should and will be others to integrate into the policy discussion.

---

tent/uploads/2011/07/Accountability%20as%20the%20Basis%20for%20Regulating%20Privacy%20Can%20Information%20Security%20Regulations%20Inform%20Privacy%20Policy.pdf; "Demonstrating Privacy Accountability," IAPP Daily Dashboard (Apr. 28, 2011), https://privacyassociation.org/news/a/demonstrating-privacy-accountability/.

121. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 56 (2014), available at http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

122. Comm'n Opinion (EC), 08/2014, Art. 29: Data Protection Working Party, on *Recent Developments on the Internet of Things* 3, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.