PASSIVE DATA COLLECTION THROUGH THE INTERNET OF THINGS

The phrase "going off the grid" was coined to describe a lifestyle that intentionally avoids interacting with technology that leaves a trace of one's activities. As depicted by characters in popular fiction, this has heretofore been accomplished mainly by paying for things with cash instead of credit, using a false name, and talking on pay-as-you-go mobile phones. But how can one stay off the grid when every single physical device in existence has the capacity to gather and transmit digital data?

The IOT's sense of touch: beacons and taggants

As of this writing, Bluetooth Low Energy (BLE) technology is just starting to roll out to the public, most notably in the "iBeacon" feature of Apple's iOS7. It has been seen as a rival to Near Field Communication (NFC) technology (which iOS8 also embraces), or as a convenient way to pipe coupons into your phone. But history will look back at BLE as a major step forward in manifesting the Internet of Things (IOT), and in eroding any remaining illusions of privacy we have in our physical whereabouts.

BLE is a means of transferring data. "Beacons" – devices that use BLE – are tiny, wireless sensors that transmit data within a 10-meter range. At present, they support only low data rates and can only send (and not receive) small data packets, but these are perfect for interacting with iPhones and wearable computing devices such as smart watches and fitness trackers.[47] In light of the current proliferation in such devices, therefore, it's safe to say that in the near future we may carry a half-dozen devices or more that are equipped with BLE or similar technology.

One of the most obvious applications of BLE is micro-location geofencing. GPS technology is great for determining your approximate location to within a few feet, but it relies on satellites that can't see into buildings very well. A mobile device running BLE technology, however, can interact with nearby beacons to determine its precise location, even indoors.

Set up around a store, they can detect shoppers entering and exiting, and send them coupons (customized to your unique shopper profile) or even internal directions – *Minority Report* without the retinal scans. You will soon be able to even pay for goods without ever pulling out your phone, just like the newest vehicles will open their doors even when your key stays in your pocket. PayPal is already developing just such an app using BLE.

The real potential of BLE lies not in coupons, but in the IOT–the burgeoning trend towards making physical objects internet-connected and digitally interactive. Just like humans cannot meaningfully interact with the world around them without their five senses, so too will IOT-enabled objects lack interactivity without some means of sensing and communicating with their surroundings. BLE beacons are a major step toward providing that ability.

[47] Elyse Betters, "Apple's iBeacons explained: What it is and why it matters," *Pocket-Lint*, September 18, 2013, available at http://www.pocket-lint.com/news/123730-apple-s-ibeacons-explained-what-it-is-and-why-it-matters/

In all likelihood, some improved version of BLE technology, or its next-generation replacement with even broader capabilities, will be available either when this book is released, or shortly thereafter. Moreover, as discussed in Chapter 2, the need for digital sensors to precisely locate physical objects may lead to the deployment of beacons or taggants on the micro- or even nano-scale. Each of these devices – including present-day beacons and RFID tags as well as taggants and other future technologies – will be able, in theory, to have its own unique IP address on the internet. The migration begun in 2012 of the Internet Protocol address system from IPv4 to IPv6 increased the total number of IP addresses from a mere 4.3 billion – a number we've already reached – to 340 undecillion (i.e., 340 trillion trillion trillion). Now, literally every Barbie doll, toilet paper roll, and random chatski can have its own unique IP address on the internet. Each becomes a data point capable of reporting its exact physical location on a real-time, global map. Once more people are using this infrastructure, its consequences will become more apparent.

Aggregating our interactions with the IOT

Digitizing our physical interactions will create a digital record of our movements and whereabouts that had never previously existed. For advertisers and retailers, this will be a goldmine of information just like social media was before it–a brand-new trove of personal data that can be used to send out even more precisely targeted commercial solicitations. Without doubt, those providing IOT services will want not only to recognize who we are, but also to remember where we've been.

And just like we do online now, many users will consent to their information being collected in this manner. The convenience factor will be huge. Just as internet browsers use cookies and browsing histories to remember who I am without forcing me to re-type my password every time I re-visit a website, so too will I want my clothing store to remember my size, my restaurant to remember my favorite meals, my grocery store to remember the location of my favorite items, and the news feeds that I'll see projected everywhere to remember my favorite topics.

But others will be remembering that data as well. Thanks to Edward Snowden and others like him, the world is already aware of how much information private companies and the government collect about our emails and other online interactions. Law enforcement already does all it can to track a suspect's physical movements, whether through cellular towers, IP addresses, or GPS trackers. In the near future, the government will likely have access to high-resolution, constantly updated digital maps of the entire planet's surface; the Pentagon's National Geospatial-Intelligence Agency is already at work on an "orthorectified image skin" that would provide the base layer for a next-generation map.[48] Just like GPS and the internet itself, it will only be a matter of time before the private sector gets its hand on this geolocation data (Fig. 3.3).

[48] Ray Locker, *Pentagon Agency Creating Digital Map of the World*, USA Today (October 26, 2013) http://www.usatoday.com/story/nation/2013/10/25/nga-digital-map-world-updated/3189781/.

FIGURE 3.3

The defense agency working on next-generation digital maps.

When the government and the private sector have access to high-fidelity geolocation data and a geolocation-aware sensor infrastructure, merely walking down the street with one or more sensor-enabled devices on our persons will leave behind so much data about our physical location that it may well become possible to create precise maps of our every step going back hours, days, or even longer. Add to that the digital data we'll leave behind in each of the physical objects with which we interacted along the way. Everything we touch – the toothbrush we use in the morning, our clothing, doors through which we pass, the pavement we step on, even the plastic fork from the street-side falafel stand – could potentially be capable of not only recording their interactions with us, but also transmitting that data to one or more servers, which then collect, collate, and make the data available for reporting out.

Even this possibility could one day seem tame if a system of trackable nanotaggants ever truly becomes reality. With that technology, it could become possible for the first time to literally destroy the possibility of privacy altogether–at least when it comes to concealing your physical location. Consider: the nanotaggants that the military is reportedly developing are intended to be sprayed onto enemy combatants so they can be tracked in situations where direct surveillance is impossible, such as urban combat. Because these devices exist on a micro or nano scale, they're invisible to the human eye. Ideally, the soldier won't even know he's been tagged, let alone be able to find or remove all of the devices. The same technology could be used to track anyone. Even if you knew you were tagged, could you remove them all? A human skin pore is 200~250 nanometers wide, which easily allows nano-scale products to be absorbed into the skin. What if you inhaled or ingested them? Like Lady Macbeth, you'd wash and wash, but never get the damned nano-spot out.

Privacy regulations and IOT

Government regulators are only beginning to draw lines of privacy around data accumulated by the IOT. Certainly, where networked devices are used to surreptisously record the words and actions of third parties, existing causes of action for eavesdropping and common law invasion of privacy will be enforced, just as they are now with the "Peeping Tom" cameras that seem to regularly find their way into changing rooms, bedrooms, and other unambiguously private places.

In September 2013, the FTC took its first enforcement action related to IOT-collected information. TRENDnet, a company that markets video cameras designed to allow consumers to monitor their homes remotely, settled FTC charges that its lax security practices exposed the private lives of hundreds of consumers to public viewing online.[49] According to the FTC, TRENDnet marketed its numerous products as being "secure" when, in fact, the cameras had faulty software that left them open to online interception. The complaint further alleged that, in January 2012, a hacker exploited this flaw and made it public, and, eventually, hackers posted links to the live feeds of nearly 700 of the cameras. The feeds displayed babies asleep in their cribs, young children playing, and adults going about their daily lives. Once TRENDnet learned of this flaw, it uploaded a software patch to its website and sought to alert its customers of the need to visit the website to update their cameras.

"The Internet of Things holds great promise for innovative consumer products and services. But consumer privacy and security must remain a priority as companies develop more devices that connect to the Internet," said FTC Chairwoman Edith Ramirez.[50] Under the terms of its settlement with the Commission, TRENDnet was prohibited from misrepresenting the security of its devices or network, and was required to establish a comprehensive information security program designed to address security risks that could result in unauthorized access to or use of the company's devices. The company also was required to obtain third-party assessments of its security programs every two years for the next 20 years.

This first foray into protecting privacy in the IOT – which came only a month before the FTC hosted its first public seminar about the IOT – signaled that the FTC is likely to continue following its existing practices in this new technological field. That is, it will take a proactive role of facilitating public conversations on the topic, while at the same time reacting to the worst offenders in the field in order to set examples

[49] Edward Wyatt, *F.T.C. Says Webcam;s Flaw Put Users' Lives on Display*, The New York Times (September 4, 2013) *available at* www.nytime.com/2013/09/05/technology/ftc-says-webcams-flat-put-users-lives-on-display.html?_r=0.

[50] *Id.*

for the rest of the industry. The FTC has done the same thing in recent years with social media endorsements and other fields that catch its interest.

There is every indication that regulators will continue to have plenty of opportunities to punish lax security practices in the IOT space. A 2014 study by researchers at Hewlett-Packard "identified an alarmingly high number of vulnerabilities" in the most popular IOT devices.[51] These insecurities ranged "from issues that could raise privacy concerns to serious problems like lack of transport encryption, vulnerabilities in the administration Web interface, insecure firmware update mechanisms and weak or poorly protected access credentials."[52] Sixty percent of the devices were vulnerable to common hacking attacks, while 70% used unencrypted networks and 80% used extremely weak passwords. [53] This reflects "the current nature of online services [to] provide[] few mechanisms for individuals to have oversight and control of their information, particularly across tech-vendors."[54] At some point, certain unfair practices may become so prevalent that Congress will feel the need to step in with new legislation.

The IOT will also implicate subject-specific privacy laws. Without question, IOT advancements will allow a greater range of devices to do such things as storing personal health information or sending messages that are intended to be private. When they do, new questions will arise about applying existing, subject-specific privacy laws like HIPAA and the Stored Communications Act. For example, the refrigerator is a device that many IOT enthusiasts talk about being networked. They often cite such advantages as the fridge being able to tell you when you're out of a particular item, or what other ingredient you might need for a recipe. But what if an insurance company sought access to our fridges' data logs to determine how healthy our diets are before determining what our health insurance premiums should be? The same could be asked of the panoply of health statistic-monitoring wearable devices that are now all the rage. In light of how strict many of the current regulations concerning health information already are, it would not be surprising to see the government severely limit who can access such information. The counter-argument will be made, however, that insurers should have access to this data in order to set rates that are fair to everyone.

Geolocation privacy

Geolocation data is something the courts have been trying to wrap their arms around for a few years now, with no clear boundary lines yet emerging. In January 2012, the United States Supreme Court decided *United States v. Jones*,[55] in which it unanimously ruled that the attachment of a GPS tracking device to an individual's vehicle

[51] Lucian Constantin, "Popular Internet-of-Things devices aren't secure," Computerworld, July 30, 2014, available at http://www.computerworld.com/article/2490587/networking/popular-internet-of-things-devices-aren-t-secure.html

[52] *Id.*

[53] *Id.*

[54] "The internet of things - the next big challenge to our privacy," *The Guardian,* July 28, 2014, available at http://www.theguardian.com/technology/2014/jul/28/internet-of-things-privacy.

[55] 565 US ___, 132 S.Ct. 945 (2012),

by police, and subsequent use of that device to monitor the vehicle's movements on public streets, constituted a "search or seizure" within the meaning of the Fourth Amendment. Contrary to many news reports at the time of the decision, however, the *Jones* Court reached no conclusion on whether that search was unreasonable, or whether it required a warrant. The case produced three opinions from overlapping groups of Justices, some of whom found any degree of GPS tracking without a warrant legally dubious, while others would limit only long-term tracking, and still others so no problem with collecting such data as long as the police committed no physical "trespass" onto the person's property. This mish-mash of views illustrates the difficulty in applying eighteenth century legal principles to twenty-first century technology.

At least with regard to data collected by mobile phones, then, courts have generally concluded that "[u]nder existing law, … a user does not have a reasonable expectation of privacy as to geolocation data."[56] This is because, unlike the police-imposed "tracking devices" at issue in *Jones*, consumers carry mobile phones with themselves voluntarily, and are presumed to agree to their carriers' privacy policies that allow collection and sharing of this data. Presumably, mobile AR devices will come with the same broad policy provisions, and the same legal principles will apply to the data they collect.

Regulatory bodies are also paying attention to geolocation data privacy. On May 25, 2012, the Federal Communications Commission (FCC) released a report with the opaque title "Location-Based Services: An Overview of Opportunities and Other Considerations."[57] The report outlines the growing use of location-based services (LBS) in navigation, tracking, social networking, gaming, retail, real estate, advertising, news, weather, device management, and public safety applications, and government and industry efforts to address the privacy issues surrounding such services. It stemmed from a June 2011 workshop that the FCC hosted on the subject.

Like the FTC's efforts, this FCC report offered more general principles than concrete rules. In this case, the report highlighted "notice and transparency," "meaningful consumer choice," "third party access to personal information," and "data security and minimization" as its primary concerns. The FCC ended its report with a warning that it will "continue to monitor industry compliance with applicable statutory requirements and evolving industry best practices," and that "additional steps may be necessary if privacy issues are not met as effectively and comprehensively as possible or within reasonable time frames."[58]

What will be more interesting, though, is determining expectations of privacy in our digital interactions with IOT-connected physical devices. It is one thing to

[56] *In re Smartphone Geolocation Data Application*, 2013 U.S. Dist. LEXIS 62605, at *45 (E.D.N.Y. May 1, 2013); *see also United States v. Caraballo*, Case No. 5:12-cr-105 (D. Ver. August 7, 2013) (collecting cases).

[57] Federal Communications Commission, Location-Based Services: An Overview of Opportunities and Other considerations (May 2012) *available at* http://apps.fcc.gov/edocs_public/attachmatch/DOC-314283A1.pdf.

[58] *Id*. at 2.

follow the legal fiction that everyone visiting a website or opening a particular software program reads and agrees to its terms of use, including the privacy policy that allows personal data to be collected. It will be another thing to apply that presumption to random devices we encounter in the physical world. Expecting every BLE-enabled beacon we will encounter on the sidewalk or within stores to carry a privacy policy that consumers can be expected to read and consent to seems impractical. The companies that provide service to our AR devices will likely seek to obtain from users a blanket consent to data collection on the front end, but even that consent cannot meaningfully apply to every party who will eventually have access to our interactions with the IOT.

USING AR TO ENHANCE PRIVACY

A new approach will need to be found. Here, in addition to new questions, AR also offers potential solutions.

Wearable technology in general has the potential to change individual users' attitudes toward data privacy. On today's internet, the providers of content and services do not go out of their way to offer individuals an opportunity to understand, much less control, how their data is collected or used. In most circumstances, any such effort is only the result of cajoling by regulators, and comes in the form of a dense privacy policy that offers little or no more information beyond what is legally required. After years of operating in this environment, users have become accustomed to the idea that controlling data privacy is beyond their reach.

With wearable and "pervasive computing, [however,] much of the technology becomes tangible and familiar. This makes issues of privacy more readily apparent to users. … If you can physically witness aspects of data collection, it short-circuits what has traditionally been a long feedback loop between privacy risk and cumulative effect. The hope is that the increased awareness inspires action."[59] Moreover, as wearable devices make computing a more personalized experience, "it could also be used to provide individuals with the opportunity to take control of their personal data."[60]

By truly allowing users to *see* the data they exchanges, AR interfaces could go one step further than other wearable devices in bringing about this shift in users' mindset about their data. Because augmented display technologies will allow us to see large displays of virtual data floating in mid-air, rather than relying on size-constrained physical monitors, privacy warnings and dialogues can be made easier to notice. They will also be made easier to understand if they are displayed in physical proximity to the device being warned of, rather than on a remote, two-dimensional privacy document. So, for example, if the manufacturer of my refrigerator wishes to warn me that it will remember all of the food items I place inside the fridge, it can be programmed to display in my AR eyewear a large, red box containing this warning and floating in mid-air in front

[59] "The internet of things - the next big challenge to our privacy," *The Guardian,* July 28, 2014, available at http://www.theguardian.com/technology/2014/jul/28/internet-of-things-privacy.

[60] *Id.*

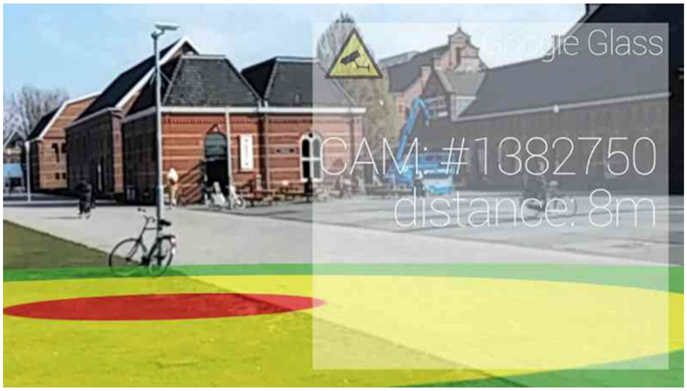

FIGURE 3.4

"Watch Your Privacy" by Sander Veenhoff.

of the refrigerator door. By gesturing a hand (which, at that point, will likely also be equipped with location-aware transmitters for just such a purpose as this) through the dialogue box, I can indicate my assent to this data collection and go about my business. Similarly, as I walk down the sidewalk, my AR eyewear could be programmed to display the geographic boundary lines around each store's BLE sensor network. These could be highlighted in predetermined colors, or annotated with the appropriate warning language, to indicate that by stepping over the line, the store's network will register my physical presence there and be permitted to digitally interact with me. In both examples, the consumer is able to make a decision that is orders of magnitude more informed than anything allowed by present-day digital privacy practice.

Software coder Sander Veenhof has actually already published the first attempt at a digital eyewear application that attempts to enhance an individual's privacy. Called "Watch Your Privacy,"[61] the app "visualises nearby privacy intrusions based on open data about surveillance cameras worldwide."[62] It also claims to map the real-time geolocation of other digital eyewear wearers who are using the app. In both cases, the goal is to inform the user as to the location of video cameras (both stationary and wearable) so that the user can make an informed choice as to whether or not they wish to be filmed. The screen capture included here as Fig. 3.4 demonstrates an augmentation showing red and yellow circles, indicating areas where a camera is or could be pointed, and green areas that are not being surveilled. Presumably, the same approach could be applied to beacons and other sensors capable of reading NFC, Bluetooth, Wi-fi, or other signals. Of course, this early implementation has a number of practical limitations; its database of camera locations will necessarily be incomplete, and the augmentations are likely only approximate. As a proof of concept, however, Veenhof's creation is a marvelous sneak peek at what AR could do to enhance personal privacy.

[61] "Watch Your Privacy," available at http://sndrv.com/watchyourprivacy/.

[62] *Id.*