SO YOU WANT TO BUILD A CYBERSHOE: MINIMIZING LIABILITIES AS AN INTERNET OF THINGS PRODUCT DEVELOPER

Kyra Lomonosoff

THE RISE OF THE INTERNET OF THINGS

In recent years, the modern lifestyle has come to resemble something out of *Star Trek*. You arrive home and want the lights on and music to start playing—merely issue the commands to your Google Home device and it is so. New lights designed to work with Google's software brighten or dim in accord with either the voice commands picked up by a Google Home unit or commands issued the increasingly old-fashioned way—by hand from a smartphone app. Meanwhile, music from Spotify's library begins playing from speakers connected to your home's smart ecosystem, as the smartwatch on your wrist keeps track of our pulse and combines that information with weight data to create a snapshot of your health, one that you can check on your phone at any moment.

The beating heart of all this activity is the internet, which plays host to the vast array of personal data and login credentials users offer to gain access to myriad services, as well as to the data those services create. When the phrase "Internet of Things" was coined by Kevin Ashton in 1999, it was primarily used to describe the growing market of products using RFID chip technology.[1] The expression, however, did not enjoy its current popularity until the early to mid-2010s, when it became the theme of international technology shows and Google corporate acquisitions.[2] As used today, the Internet of Things ("IoT") collectively refers to the group of items and appliances connected to the internet and potentially to each other through the internet.[3]

Experts and corporate executives have estimated that, by 2030, there will be between 20 and 50 billion IoT devices in use across the private, commercial, and government spheres.[4] Spurred

---

[1] Knud Lasse Lueth, *Why the Internet of Things Is Called Internet of Things: Definition, History, Disambiguation*, IOT ANALYTICS (Dec. 19, 2014), https://iot-analytics.com/internet-of-things-definition/.
[2] *Id.*
[3] *Id.*
[4] Amy Nordrum, *Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated*, IEEE SPECTRUM (Aug. 18, 2016, 5:00 PM), https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated; Jennifer Daniels & David Oberly, *What to Know About New Calif. Connected Devices Law*, JD SUPRA (Mar.

on by the explosive growth of this market, manufacturers have been keen to integrate IoT systems into their products, from household items like speakers and robotic vacuums, to larger ones like cars,[5] and even houses themselves.[6] As businesses attempt to integrate "smart" IoT technology into "dumb" devices,[7] however, they open themselves to new liabilities that may not have confronted them before entering the IoT world. A smartwatch, for instance, may be subject to hacking or other forms of cyber attack that could not reach an analog watch. The extent to which a manufacturer may be liable for such breaches has not yet been settled on a national level, but federal guidelines, as well as developments on the state level and recent legal action, may indicate the measures necessary to avoid successful lawsuits.

In order to explore what product designers can do to minimize liability, let us imagine the designer of an internet-connected shoe. Having recently studied programming at MIT and passed a footwear design course at Milan's Arsutoria School, our entrepreneur is keen to take advantage of the growing IoT market by creating her first product: the CyberShoe.[8] Worn like normal shoes, CyberShoes monitor their wearer's weight, heartrate, step count, and location. Through a companion application ("app") available on Google's Play Store and Apple's App Store, wearers are able to keep track of this information and modify the structure of the shoe to suit individual tastes by, for instance, changing the firmness of the insole. Finally, third-party developers can create

---

28, 2019), https://www.jdsupra.com/legalnews/what-to-know-about-new-calif-connected-74765/; *Strategy Analytics: Internet of Things Now Numbers 22 Billion Devices but Where Is the Revenue?*, STRATEGY ANALYTICS (May 16, 2019), https://news.strategyanalytics.com/press-releases/press-release-details/2019/Strategy-Analytics-Internet-of-Things-Now-Numbers-22-Billion-Devices-But-Where-Is-The-Revenue/default.aspx.

[5] Frederic Paul, *How BMW's New Annual Fee for Apple CarPlay Could Define the IoT*, NETWORK WORLD (July 24, 2019, 2:06 PM), https://www.networkworld.com/article/3411478/how-bmws-new-annual-fee-for-apple-carplay-could-define-the-iot.html.

[6] Patrick Sisson, *As Smart Home Market Booms, Builders See Plug-and-Play Tech as a Standard Feature*, CURBED (July 22, 2019, 2:05 PM), https://www.curbed.com/2019/7/22/20701080/alexa-new-smart-home-homebuilder-brilliant.

[7] Brian X. Chen, *In an Era of 'Smart Things, Sometimes Dumb Stuff Is Better*, N.Y. TIMES (Fed. 21, 2018), https://www.nytimes.com/2018/02/21/technology/personaltech/smart-things-dumb-stuff.html?emc=edit_tnt_20180221&nlid=9433836&tntemail0=y&mtrref=undefined.

[8] Not to be confused with Cybershoes actually manufactured for use with virtual reality products. CYBERSHOES, https://www.cybershoes.io/.

apps that work with the shoe, like an app that records a user's credit card information to streamline payment for products at cashier-less stores.[9] In the end, what she has made is an IoT product that monitors and stores personal data and functions with apps through a connection to the internet. What liabilities might such a shoe create for our entrepreneur? What measures can she take to minimize those liabilities? There is, unfortunately, no royal road to lawsuit-immunity, but there is an increasingly clear set of rules and guidelines, buttressed at the national level by the Federal Trade Commission (FTC) and pending legislation, and at the state level by regulations signed into law in California. Note that this paper will not be addressing broader data privacy concerns, such as would be covered by the California Consumer Privacy Act[10] or any General Data Protection Regulation[11]-like legislation passed by Congress.

RELEVANT FORMS OF LIABILITY

Before going over potential countermeasures to cyber attacks, it is essential to address the potential cybersecurity threats any IoT device faces. If inadequately protected, an IoT product that collects or uses personal information may enable unauthorized users to access that data, regardless of those users' knowledge.[12] To use our CyberShoe as an example, unprotected credit card information stored on the shoe could be skimmed and used to make unauthorized purchases. Other personal data—names, addresses, and so on—stored in a device could be used to facilitate identity theft or fraud.[13] For a user of IoT products, this risk increases with the number of products used, as well as with exposure to other networks in the course of a user's day (municipal sensors, for instance, may track an

---

[9] Andrew Liptak, *Amazon is Reportedly Testing its Cashier-less Technology in Larger Stores*, VERGE (Dec. 2, 2018, 5:34 PM), https://www.theverge.com/2018/12/2/18122772/amazon-testing-larger-cashier-less-stores-report. Amazon is planning to open 3,000 such stores by 2021. *Id.*

[10] *See* California Consumer Protection Act, CAL. CIV. CODE §§ 1798.100–1798.199 (Deering 2019).

[11] *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1) [hereinafter GDPR].

[12] FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 26 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [hereinafter FTC Report].

[13] *Id.* at 27.

IoT product's location and record that data on city servers).[14] Litigation in such an event would focus on manufacturers whose products failed to take "reasonable" security measures, where the level of "reasonable" protection is determined by the quality of the personal information at risk and the potential harms its theft may result in for the user.[15]

Inappropriate measures to govern the privacy of an IoT product's data can also result in liability. Although not an IoT product, it is worth considering the consequences faced by Facebook following revelations that data analytics firm Cambridge Analytica harvested user profile data from 50 million users without permission.[16] As of this writing, a privacy class action lawsuit against Facebook is still proceeding slowly through the courts.[17] A successful lawsuit could result in billions of dollars in damages, in addition to a $5 billion settlement that the company has already paid to the FTC.[18] In the case of Cambridge Analytica, the company collected data *en masse* to determine the personalities of users (then used to create targeted political advertisements). For an IoT product like the CyberShoe, unauthorized data harvesters could construct a medical profile of a user by analyzing weight and heart rate collected over time, or they could use location data and step counts to predict a user's schedule and means of transport. Such unauthorized access

---

[14] *Id.*

[15] Daniels & Oberly, *supra* note 4.

[16] Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. *See also* Info. Comm'r Off., Press Release, ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information (Oct. 25, 2018), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/; Meera Narendra, *Italian data protector fines Facebook*, GDPR.REPORT (Jul. 1, 2019), https://gdpr.report/news/2019/07/01/italian-data-protector-fines-facebook/; FTC, Press Release, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (Jul. 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[17] In re Facebook, Inc., Consumer Privacy User Profile Litigation, 402 F. Supp. 3d 767 (N.D. Cal. 2019).

[18] Jonathan Stempel, *Judge Lets Facebook Privacy Class Action Proceed, Calls Company's Views 'So Wrong'*, REUTERS (Sept. 9, 2019, 6:22 PM), https://www.reuters.com/article/us-facebook-lawsuit-privacy/judge-lets-facebook-privacy-class-action-proceed-calls-companys-views-so-wrong-idUSKCN1VU2G2; Ruchi Gupta, *Privacy Lawsuit: Facebook's Billions Could Be on the Line Again*, MARKET REALIST (Sept. 11, 2019), https://articles2.marketrealist.com/2019/09/privacy-lawsuit-facebooks-billions-on-the-line/.

would constitute a major privacy breach. California's Security of Connected Devices Act mandates that companies take measures "to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or *disclosure*, as specified [emphasis added]."[19]

Hackers, however, need not target the IoT product's user for a designer to be liable. Those wishing to launch a Distributed Denial of Service (DDoS) attack against a website increasingly do so through IoT products owned by unrelated companies or private users.[20] In a DDoS attack, hackers attempt to disrupt a targeted site by overwhelming it with internet traffic from a variety of originating sources and rendering the targeted site inaccessible to other visitors.[21] In the IoT context, this is achieved by exploiting IoT product internet connections to have devices send, for instance, thousands of refresh requests to a given site.[22] In October 2016, users on the East Coast were unable to access Twitter, Spotify, Netflix, and other major websites when the dynamic domain name service provider Dyn was subject to a DDoS attack.[23] The attack was launched from hijacked IoT devices like routers, security cameras, and baby monitors.[24] Thus far, litigation tied to DDoS attacks has targeted either the victim company (on behalf of users harmed in some way by the incident) or the hackers themselves, bypassing manufacturers of IoT devices that may have been used in

---

[19] Security of Connected Devices Law, CAL. CIV. CODE §§ 1798.91.04–1798.91.06 (Deering 2019).

[20] *See* A10 Staff, *IoT and DDoS: Cyberattacks on the Rise*, A10 (Aug. 14, 2018), https://www.a10networks.com/blog/iot-and-ddos-cyberattacks-rise/; Ajay Rane, *IoT Security: Current Threats and How to Overcome Them*, SECURITY TODAY (Aug. 7, 2019), https://securitytoday.com/articles/2019/08/07/iot-security-current-threats-and-how-to-overcome-them.aspx.

[21] *See What is a DDoS Attack?*, CLOUDFARE, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (last visited Aug. 7, 2019).

[22] *See* A10 Staff, *5 Most Famous DDoS Attacks*, A10 (Aug. 15, 2018), https://www.a10networks.com/blog/5-most-famous-ddos-attacks/.

[23] Nichole Perlroth, *Hackers Used New Weapons to Disrupt Major Websites Across U.S.*, N.Y. TIMES (Oct. 21, 2016), https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html.; Horia Ungureanu, *Massive Dyn DDoS Attack: Experts Blame Smart Fridges, DVRs and Other IoT Devices Why Your Internet Went Down*, TECH TIMES (Oct. 24, 2016, 12:17 AM), https://www.techtimes.com/articles/183339/20161024/massive-dyn-ddos-attack-experts-blame-smart-fridges-dvrs-and-other-iot-devices-why-your-internet-went-down.htm.

[24] *See id.*

the attack.[25] But litigation may eventually target manufacturers whose product security measures are unreasonably poor.

Finally, there is the risk that unauthorized parties gain access to an IoT device and modify its settings in such a way as to cause direct harm to its owner. One participant in an IoT workshop hosted by the FTC indicated that he was able to access insulin pumps remotely and cause them to stop delivering medicine.[26] Needless to say, the resulting hyperglycemia would be a potentially lethal danger to patients who rely on the regularly delivered insulin to lower their blood sugar.[27] Other instances of IoT product manipulation can threaten more than one individual at once. Alarmingly, researchers have demonstrated the hackability of a car's internal computer systems, which can grant hackers the ability to control the engine and brakes of the vehicle.[28] As with unauthorized access to personal data, liability concerning unwanted software modifications is largely tied to notions of what is a reasonable level of protection given the abilities of the IoT product.[29] An automobile or pacemaker with internet connectivity

---

[25] *See Legal Implications of DDoS Attacks and the Internet of Things (IoT)*, NORTON ROSE FULBRIGHT DATA PROTECTION REPORT (Dec. 5, 2016), https://www.dataprotectionreport.com/2016/12/legal-implications-of-ddos-attacks-and-the-internet-of-things-iot/.

[26] FTC Report, *supra* note 12, at 12. Civil, and especially, criminal cases are rare when it comes to remote access of devices; however, there is some similarity with cases involving port scanning. Port scanning is used to determine which network ports on a system are open, and therefore potentially vulnerable to attack. Cyberpedia, *What is a Port Scan?*, PALOALTO NETWORKS, https://www.paloaltonetworks.com/cyberpedia/what-is-a-port-scan (last visited Jun. 4, 2020). The most notable of these cases occurred in 1999: Scott Moulton worked as a contractor for the Cherokee County, Georgia emergency 911 system. Moulton v. VC3, No. 1:00-CV-434-TWT, 2000 U.S. Dist. Lexis 19916, at *3–*4 (N.D. Ga. 2000). While connecting a police station to the e911 system, Moulton ran a port scan to detect vulnerabilities. *Id.* at *4. This scan touched the network of a competing company; the company then instituted a civil suit claiming Moulton allegedly violated the Computer Fraud and Abuse Act of America Section 1030(a)(5)(B). *Id.* at *4, *6. The act applies to anyone who "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage ... ." 18 U.S.C. § 1030(a)(5)(B). The court ruled in Moulton's favor because in this case, his scan did not cause damage to the plaintiff's system. *Moulton*, 2000 U.S. Dist. Lexis 19916, at *20–*21. However, this would likely not be the case with malicious remote access of medical devices—such action would seem to be designed to cause damage.

[27] *See* AM. DIABETES ASS'N, *Diagnosis and Classification of Diabetes Mellitus*, 35 DIABETES CARE S64, S64 (2012).

[28] FTC Report, *supra* note 12, at 12.

[29] Dick O'Brien, *The Internet of Things: New Threats Emerge in a Connected World*, SYMANTEC (Jan. 20, 2014), https://www.symantec.com/connect/blogs/internet-things-new-threats-emerge-connected-world/.

will warrant a significantly higher degree of protection than our shoemaking protagonist's CyberShoe because modification of those devices has the potential to cause greater harm. Although someone remotely hacking the CyberShoe to alter the insole's firmness would be concerning, it is comparatively innocuous.

FEDERAL LEGISLATION, THE FTC GUIDELINES, AND CALIFORNIA'S SECURITY OF CONNECTED DEVICES ACT

Congress has yet to pass legislation explicitly governing IoT products, but any bill mandating IoT-product safeguards will likely find a basis, not only in guidelines published in 2015 by the FTC,[30] but also in California's Security of Connected Devices Act (effective from the start of 2020)[31] and in the National Institute of Standards and Technology (NIST) Recommendations for IoT Device Manufacturers.[32] Indeed, the "IoT Cybersecurity of Act of 2019" currently pending in the House and Senate contains no such rules, but instead mandates that NIST publish guidelines relating to the use of IoT products by the federal government.[33] Although such a bill, if passed, would lead to the creation of guidelines regarding "minimum information security requirements," those guidelines would themselves require further crystallization into rules and would, at the outset, govern only those devices used by the government.[34] The FTC Staff Report on IoT security and California's Security of Connected Devices Act, on the other hand, already contain guidelines and rules that are meant to apply to IoT products manufactured for every sphere of use—commercial, private, or government (save those devices already covered by the Health Insurance Portability and Accountability Act of 1996

[30] FTC Report, *supra* note 12.
[31] *See* CAL. CIV. CODE §§ 1798.91.04–1798.91.06 (Deering 2019); Deborah A. George, *IoT Manufacturers—What You Need to Know About California's IoT Law*, N AT'L L. REV. (Jan. 28, 2020), https://www.natlawreview.com/article/iot-manufacturers-what-you-need-to-know-about-california-s-iot-law.
[32] NAT'L INST. STANDARDS & TECH., RECOMMENDATIONS FOR IOT DEVICE MANUFACTURERS: FOUNDATIONAL ACTIVITIES AND CORE DEVICE CYBERSECURITY CAPABILITY BASELINE (2020) [hereinafter NIST RECOMMENDATIONS].
[33] Internet of Things Cybersecurity Improvement Act of 2019, S. 734, 116th Cong. § 5 (2019).
[34] *Id.* § 3.

(HIPAA)[35]).[36] Our IoT-shoemaking protagonist could learn some key lessons from these rules and recommendations.

First, the FTC report, although containing a number of "best practices" in IoT design, does not call for IoT-specific legislation at a national level.[37] Instead, it calls for the adoption of a more generalized law along the lines of the European Union's General Data Protection Regulation (GDPR)[38] or the California Consumer Privacy Act (CCPA).[39] Of more immediate interest to a prospective IoT-product designer would be the "best practices" agreed upon by those who attended the Federal Trade Commission workshop. Broadly speaking, these best practices can be described as:

- implementing "security by design" in the product design stage;
- promoting secure personnel practices;
- ensuring out-of-company service providers also embrace effective security practices;
- designing "defense-in-depth"[40] barriers to protect particularly sensitive systems;
- limiting the ability of unauthorized users to access a consumer's device; and
- maintaining product security throughout its lifecycle.[41]

California's Security of Connected Devices Act, on the other hand, represents concrete regulation of IoT product design and manufacture, and builds on data protections for consumers already

---

[35] *See* The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. No. 104-191, 110 Stat. 1938 (1996).

[36] *See generally* CAL. CIV. CODE §§ 1798.91.04-1798.91.06 (Deering 2019); FTC Report, *supra* note 12.

[37] FTC Report, *supra* note 12, at vii. Participants in the conference disagreed over whether IoT-targeting legislation would be appropriate, the FTC representatives ultimately agreeing with those who suggested that any lawmaking would be premature.

[38] GDPR, *supra* note 11.

[39] CAL. CIV. CODE §§ 1798.100–1798.199 (Deering 2019).

[40] "Defense-in-depth" entails using a multi-layered security system to protect data, where, should one layer be breached by an attacker, additional layers will remain in place to safeguard, for instance, sensitive information. *What is Defense in Depth*, FORCEPOINT, https://www.forcepoint.com/cyber-edu/defense-depth. The term itself derives from First World War-era German defense strategy, also known as 'elastic defense,' which embraced the use of multiple trench lines to prevent or slow down a breakthrough by Entente forces (roughly analogous to its present use in the field of cybersecurity). *See* MAJ. TIMOTHY A. WRAY, STANDING FAST: GERMAN DEFENSIVE DOCTRINE ON THE RUSSIAN FRONT DURING WORLD WAR II: PREWAR TO MARCH 1943 1–6 (1986).

[41] FTC Report, *supra* note 12, at 28–32.

included in the CCPA. At its most basic level, the Security of Connected Devices Act, which targets only manufacturers, mandates that security features on IoT products be "reasonable" in relation to the data they collect or maintain, as well as to the capabilities of the product.[42] Notably, the law also does not apply to any devices that would otherwise be subject to regulation under federal law.[43] Products subject to HIPAA[44] are also excluded.[45]

The least defined part of the Act is the necessity for protections to be "reasonable," but the legislation nevertheless includes four criteria to be considered when implementing security features:

(1) measures must be appropriate to the nature and function of the device;
(2) they must be appropriate to information that is collected, maintained, or transmitted by the device;
(3) they must be designed to limit the ability of unauthorized users to access the device; and
(4) devices usable outside of a local area network (LAN) must have unique preprogrammed passwords or require that users generate new passwords on initial set-up.[46]

While the rule regarding passwords is fairly clear, one sees room to argue in the other criteria. What constitutes, for instance, an "appropriate" level of protection? How much limitation is necessary to satisfy the requirement to limit unauthorized access? There is, unfortunately, no clarity provided outside the term "reasonable," but there are a number of best practices advocated by cybersecurity experts (including those attending the FTC IoT workshop), which will be of use to anyone seeking to enter the market.

PROTECTING THE CYBERSHOE: WHAT CAN DESIGNERS DO?

If the FTC guidelines and California regulation are a guide, then liability for faulty or insecure devices will, at the outset, lie with manufacturers rather than retailers of the IoT product in question. Though traditional product liability suits have the potential to involve retailers as well, California's Security of Connected Devices

[42] CAL. CIV. CODE § 1798.91.05 (Deering 2019). The law defines a manufacturer as one "who manufactures, or contracts with another person to manufacture on the person's behalf, connected devices that are sold or offered for sale in California." *Id.*
[43] Daniels & Oberly, *supra* note 4.
[44] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) P.L. No. 104-191, 110 Stat. 1938 (1996).
[45] CAL. CIV. CODE § 1798.91.06 (Deering 2019); Daniels & Oberly, *supra* note 4.
[46] CAL. CIV. CODE § 1798.91.04 (Deering 2019).

Act limits its focus to product manufacturers or those who contract for the manufacture of an IoT product.[47] The FTC report, meanwhile, suggests that enforcement by the FTC will "help incentivize appropriate privacy and security-protective practices by companies manufacturing *and* selling connected devices"[48] [emphasis added]. This is not to say that an IoT product could not be subject to a normal product liability suit based on its analog aspects, but the focus is on the digital elements of the product. The consistent focus on manufacturers makes it clear that our intrepid and liability-conscious product-designer will have to exercise caution from the start. This challenge is defining what form such caution should take.

As described above, the experts participating in the FTC's IoT workshop advocated for "security by design."[49] As the name implies, "security by design" entails consideration of cybersecurity at every level of the products design. Timesys, a company that works with product manufacturers in the development and maintenance of secure IoT systems, has suggested a number of best practices in the realm of secure design.[50] First, our shoemaker will want to ensure that the boot-up process of her product is as secure as possible, eliminating the chance that malicious code could be activated upon system start-up.[51] Secure design here may entail having the boot-up process assess the authenticity of software before executing it, preventing altered software from being activated at all.[52] Risk assessments, determining where and how one's product can be attacked and taking steps to mitigate that risk, are another essential secure design practice.[53] Such risk assessments should also examine

---

[47] *Product Liability—The Basics*, STIMMEL, STIMMEL & SMITH, https://www.stimmel-law.com/en/articles/product-liability-basics; SECURITY & CONNECTED DEVICES LAW § 1798.91.04 (defining "Manufacturer" as "person who manufactures, or contracts with another person to manufacture on the person's behalf, connected devices that are sold or offered for sale in California").
[48] FTC Report, *supra* note 12, at 53.
[49] *Id.* at 28. This is a concept evolved from the "privacy by design" approach, developed by Ann Cavoukian, the third Information and Privacy Commissioner of Ontario, in collaboration with the Dutch Data Protection Authority and the Netherlands Organisation for Applied Scientific Research. *See, e.g.*, Ann Cavoukian, *Privacy by Design: The Definitive Workshop—A Foreword*, 3 IDENTITY INFO. SOC'Y 247 (2010).
[50] Adam Boone, *The New Focus on 'Security by Design'*, TIMESYS (Nov. 30. 2018), https://www.timesys.com/security/focus-security-design/.
[51] *Id.*
[52] *Id.*
[53] *Id.*

any third-party software being adopted by the product designer by examining the published vulnerabilities of those systems.[54]

"Security by design" is not merely a process that ends after the product is designed and shipped to retailers, but is a practice that must be continually undertaken during the course of the IoT product's lifecycle.[55] To this end, our shoemaker will want to continue to assess her CyberShoe after it enters the market, locating vulnerabilities and pushing updates to eliminate them or reduce the damage of a successful cyber attack.[56] Naturally, a product developer will also want to pay attention to disclosures related to newly found software vulnerabilities published by other organizations and integrate changes into her product when relevant.[57] Our product designer need not do this herself—insofar as California's Security of Connect Devices Act calls for "reasonable" protections, it is likely sufficient for her to contract these duties to companies specializing in them, particularly if her company lacks the capacity to ensure a reasonable level of security on its own.[58] Developers should be upfront with consumers about how long they intend to continue supporting a given product, allowing users to make informed choices about what products they purchase and when they should consider replacing them (what counts as a reasonable life-span will vary with the nature of the product and the data it collects).[59]

Regarding systems with significant privacy or safety risks, product designers should implement additional defense-in-depth[60] measures, particularly if there are concerns about the product user's own network security.[61] Given that the CyberShoe gathers not only locational data, but sensitive health-related data as well, its designer may want to take further steps to encrypt that data such that, in the event it is acquired by an unauthorized party, it is harder to access and to cause harm to the product's user.[62] She will also want to ensure that any user data collected and stored by the company is

---

[54] *Id.*
[55] FTC Report, *supra* note 12, at 31.
[56] *Id.*; Boone, *supra* note 47.
[57] Boone, *supra* note 47.
[58] CAL. CIV. CODE § 1798.91.04 (Deering 2019).
[59] FTC Report, *supra* note 12, at 31–32.
[60] *See supra* note 40 and accompanying text.
[61] FTC Report, *supra* note 12, at 30.
[62] *Id.*

similarly secure, that excess data is not gathered, and that there is a system in place to delete unnecessary or out-of-use data.[63]

When IoT appliances were harnessed in the attack on Dyn, the key vulnerability the hackers exploited was the use of default passwords by those devices' manufacturers.[64] In other words, manufacturers were sending out entire product stocks accessible with a single password.[65] Though it seems not to have been apparent to product designers at that time, it is clear now that designers should, when possible, avoid the use of such skeleton key-like passwords. Indeed, California's Security of Connected Devices Act requires that preprogrammed passwords be unique to each individual IoT device.[66] Panelists at the FTC IoT workshop called on designers to require strong authentication measures before a device could be permitted to interact with other systems, though not so strong as to impede the use of the device.[67] Similarly, the Connected Devices law mandates that, upon a device's first use, users be required to change the preprogrammed password before full access to the device can be gained.[68] With that in mind, our enterprising shoe-designer will want to a) make sure each CyberShoe product is shipped with a unique factory password and b) make users change that password to one of their own choosing before they can use the CyberShoe's digital functions.

Adequate cybersecurity measures may involve more than just the product itself—the FTC report also suggests that companies designing IoT products have their employees and IT departments employ safe practices in the course of everyday business to avoid the intrusion of malicious parties.[69] This may involve ensuring that an executive-level employee has responsibility for security, encouraging the adoption of good practices throughout the organization and allowing security to be taken into account during hiring.[70] Among other techniques for enhancing security in the workplace are:

---

[63] *Id.*
[64] *See* Perlroth, *supra* note 22; Ungureanu, *supra* note 22.
[65] Michael Kan, *IoT Botnet Highlights the Dangers of Default Passwords*, CSO (Oct. 4, 2016), https://www.csoonline.com/article/3127263/iot-botnet-highlights-the-dangers-of-default-passwords.html.
[66] CAL. CIV. CODE § 1798.91.04 (Deering 2019).
[67] FTC Report, *supra* note 12, at 31.
[68] § 1798.91.04.
[69] FTC Report, *supra* note 12, at 29.
[70] *Id.*

(1) adopting biometric security measures (such as requiring fingerprint scanning before accessing sensitive data);
(2) ensuring that the responsibilities of those assigned to corporate security are clearly delineated;
(3) assessing the risks of the company's security structure and attempting to mitigate them;
(4) backing up data regularly;
(5) ensuring that any IoT products being used by the company are themselves secure;
(6) using multi-factor authentication to access devices and storing password information safely; and
(7) adopting the "principle of least privilege."[71]

In particular, in a least-privilege system, users obtaining company IT profiles—new employees, for example—begin with the least possible amount of access to their organization's network, and are granted access as necessary by the IT department.[72] This prevents those without clearance from accessing company matters they have no business seeing.[73] An internal report by NIST, released in January 2020, echoes these techniques in broad terms and further describes in more specific detail what a company can do at the technological level to mitigate the risk of unauthorized data access.[74] That level of detail, however, falls outside of the scope of this particular Article, which is intended to summarize generally the liabilities at play and the considerations IoT product designers should keep in mind.

In addition to the primary company behind the IoT product, secondary companies, such as those handling user data, are likely also covered by the requirement for reasonable security measures. Indeed, the fact that California's Security of Connected Devices Act explicitly rules out application to developers of "unaffiliated third-party software or applications that a user chooses to add to [their] device" suggests that developers of the device's primary applications, or handlers of data collected by the device through its intended functions, are covered by the requirement for adequate security.[75] This is largely in line with the conclusion to which experts at the FTC workshop arrived.[76] To protect her CyberShoe, our shoemaker will want not only to use reasonably secure service-

[71] *12 Best Cybersecurity Practices in 2019*, EKRAN (May 30, 2019), https://www.ekransystem.com/en/blog/best-cyber-security-practices.
[72] *Id.*
[73] *Id.*
[74] *See* NIST RECOMMENDATIONS, *supra* note 31, at 6–23..
[75] CAL. CIV. CODE § 1798.91.06 (Deering 2019).
[76] FTC Report, *supra* note 12, at 30.

providers, but also to maintain a level of oversight to ensure that these providers are in fact reasonably secure in their practices.[77]

THE BOTTOM LINE AND THE PATH AHEAD

Perhaps the most important take-away from California's Security of Connect Devices Act and the FTC workshop conclusions—both of which are almost certain to influence any future federal legislation—is the notion of "reasonableness." Not every IoT-enabled device has to be the cybersecurity equivalent of Fort Knox. Rather, the level of security that a device requires will be linked to both the sensitivity of data the device collects or uses, and the potential dangers the device could pose if commandeered by malicious parties.

A second theme that recurs throughout the regulation and any IoT security recommendation, is "security by design"—the general idea being that the security of an IoT product should not be an afterthought. Security should be a prime consideration not only in the design of the product itself, but also in the IT practices of any companies responsible for the product's development, data analytics, or maintenance.

Finally, a designer's responsibility for an IoT product's security does not end the moment it leaves the factory or retail shelf. Throughout the item's lifecycle, the developer must ensure that newly discovered security flaws are addressed as thoroughly as possible by software updates, and keep consumers informed about potential security risks. If our CyberShoe designer pays heed to these recommendations, she will certainly reduce the potential for successful litigation against her for any cybersecurity flaw in her product.

---

[77] *Id.*