The CHIPS Act

Connected Home Information Privacy and Security Act

Alex Noakes, Craig Wesoly, Johnny Wong, Clark Wood

The CHIPS Act: Connected Home Information Privacy and Security Act
White Paper

Alex Noakes, Craig Wesoly, Johnny Wong, Clark Wood

Executive Summary

The devices in your home can hear you. They listen, record your conversations with always-on microphones, and watch your actions with HD video cameras. They know when you leave your home and when you go to bed, and sometimes they even talk with you. In January of this year, a stranger accessed a family's Foscam baby monitor, watching their child over the camera and speaking to the child at night while the parents were asleep.[1]

This kind of home privacy invasion is possible because of a growing and insecure Internet of Things (IoT) and the lack of comprehensive laws governing this area. Despite the privacy and security concerns, IoT has vast potential to improve our lives. Consumers stand to benefit enormously from smart devices, which use sensors to gather data about their environment and respond accordingly. Smart thermostats reduce energy bills, smart refrigerators keep track of the groceries and create shopping lists, and smart house locks do not need a physical key.

Our proposed federal legislation protects consumers' privacy by establishing baseline standards on notice and consent, security measures, and data breach responses. Under the proposal, manufacturers are required to provide layered notices and obtain the consumer's written consent in order to disclose their information to third parties. Manufacturers must also ensure the security of the connected home devices by implementing measures such as strong encryption. In case of a data breach, the consumers must be notified within 10 days.

To promote innovation, the proposed legislation provides the option for manufacturers to propose alternative standards that meet or exceed the protections offered by the baseline standards. Since the Federal Trade Commission (FTC) has extensive experience in protecting consumer privacy, the proposal grants the agency both rulemaking and enforcement authority. By taking a comprehensive yet flexible approach, the legislation resolves the privacy and security concerns associated with connected home devices, enabling the stakeholders to realize the technology's potential.

[1] Chante Owens, *Stranger Hacks Family's Baby Monitor and Talks to Child at Night*, THE SAN FRANCISCO GLOBE (Jan. 7, 2016), http://sfglobe.com/2016/01/06/stranger-hacks-familys-baby-monitor-and-talks-to-child-at-night/?src=srd_48350&t=syn.

Connected Devices in the Home Explained

The Internet of Things (IoT) is an ever-growing system of devices that interact with each other over wired or wireless connections. In much the same way that phones have become powerful computers with many sensors attached, more and more devices found in the home are becoming "smart" devices. These devices may collect information using various sensors, analyze the information they collect to make decisions, and transmit this information to any computer accessible over the Internet.

What information a device collects depends on what sensors the device has. The Nest Protect smoke alarm, for instance, lists seven sensors on its fact sheet, including a heat sensor, an ambient light sensor, and an occupancy sensor.[2] Connected devices also tend to use Wi-Fi or Bluetooth to connect to local networks and the Internet. They may work together or independently, and may export collected information to a remotely located "cloud" server for processing.

In-home IoT devices often lack large screens for interacting with the user. Since controlling these devices can be complicated, companies often include a mobile app to which devices connect. For example, the Amazon Echo features no screen, interacting with the user primarily through voice-activated commands. It is initially configured through a mobile app available for iOS and Android devices.[3]

Stakeholders

The proposed legislation affects four main stakeholders: (1) consumers, (2) manufacturers, (3) third parties to whom the consumers' information is disclosed, and (4) the Federal Trade Commission (FTC).

Consumers are the stakeholders who would benefit most from the legislation. The data collected by connected home devices can be vast and sensitive, and unauthorized access to such data poses serious privacy concerns.[4] For example, hackers have viewed baby monitors and video cameras, gained control of smart meters, and retrieved e-mail credentials from a smart refrigerator.[5] Security flaws in connected home devices can compromise consumers' physical

---

[2] Nest, *The Nest Store*, https://store.nest.com/product/smoke-co-alarm/ (last visited May 9, 2016).

[3] Amazon, *Set up Your Amazon Echo*, https://www.amazon.com/gp/help/customer/display.html?nodeId=201601770 (last visited May 9, 2016).

[4] TRUSTe, *2015 TRUSTe Privacy Index*, https://www.truste.com/resources/privacy-research/us-internet-of-things-index-2015/ (last visited May 9, 2016).

[5] Chante Owens, *Stranger Hacks Family's Baby Monitor and Talks to Child at Night*, THE SAN FRANCISCO GLOBE (Jan. 7, 2016), http://sfglobe.com/2016/01/06/stranger-hacks-familys-baby-monitor-

safety as well. The Kwikset Kevo door lock had a vulnerability that allowed hackers to unlock the door and share the key via a mobile app as soon as they stole the consumer's cell phone.[6] Our proposed legislation aims to protect consumers from such privacy and security breaches.

Manufacturers of connected home devices may be concerned that the legislation would stifle innovation or reduce profits, but establishing baseline privacy standards would actually bolster consumer confidence in the devices and facilitate the market's growth. The proposal also offers flexibility in how the manufacturers can meet the standards. Because the devices may collect large amounts of personal information, the legislation places the responsibility on the manufacturers to be the stewards and clearinghouse for the consumers' information.

Third parties such as data brokers, analytics firms, and cloud service providers often receive and process consumer data collected by the manufacturers. Although third-party use may benefit consumers, the legislation requires notice and consent before the information is disclosed. Third parties also have to meet certain baseline privacy standards, thus protecting the consumer's information even when it is shared multiple times.

The FTC, charged with policing unfair and deceptive business practices, is also a vital stakeholder. With its extensive experience in protecting consumer privacy, the FTC has the knowledge and expertise to devise and enforce the specific rules. By expanding the definition of unfair, deceptive, or abusive acts to include violations of the legislation's notice and consent, disclosure, security, and data breach response requirements, the proposal increases the FTC's effectiveness in regulating connected home devices.

Existing Laws

The privacy of the American home is currently underprotected. Existing federal and state law does provide some protection; however, this only exists in limited circumstances. Health information is generally protected through rules promulgated pursuant to the Health Insurance Portability and Accountability Act (HIPAA). HIPAA rules provide excellent protection to health information; however, only covered entities must comply with these rules. Covered entities

---

and-talks-to-child-at-night/?src=srd_48350&t=syn; J.M. Porup, *"Internet of Things" Security Is Hilariously Broken and Getting Worse*, ARS TECHNICA (Jan. 23, 2016), http://arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/; Pierluigi Paganini, *Smart Meters in Spain Can Be Hacked to Hit the National Power Network*, SECURITY AFFAIRS (Oct. 17, 2014), http://securityaffairs.co/wordpress/29353/security/smart-meters-hacking.html; John Leyden, *Samsung Smart Fridge Leaves Gmail Logins Open to Attack*, THE REGISTER (Aug. 24, 2015), http://www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar/.

[6] Nitesh Dhanjani, ABUSING THE INTERNET OF THINGS (2015).

include health plans, healthcare clearinghouses, and healthcare providers.[7] This means that the protection afforded to health information largely depends on who collects, stores, and uses it. Connected home devices are capable of collecting massive amounts of health information, but that information usually remains unprotected by HIPAA rules.

Currently no federal statute provides for general data-security measures.[8] Instead, data security is generally regulated through either FTC enforcement actions or state data-breach notification laws. Neither of these is capable of fully addressing data breaches stemming from IoT devices.[9]

The Federal Trade Commission Act authorizes the FTC to pursue actions against companies who engage in "unfair or deceptive acts or practices in or affecting commerce."[10] The FTC has relied on this authorization to bring enforcement actions against, as well as reach settlement agreements with, companies for alleged privacy violations and data security failures.[11] Under the "deception" prong, the FTC claims that a company has contradicted statements made to consumers.

The FTC has used this authority to enforce claims against connected home device manufacturers in two notable instances. In 2013, the FTC alleged that, despite TRENDnet's assertions that its SecurView cameras were secure, "the cameras had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet address."[12] In 2015, the FTC filed a complaint alleging that ASUS deceived its consumers by claiming that its routers could "protect computers from any unauthorized access, hacking, and virus attacks."

Through these enforcement actions, the FTC ultimately reached settlement agreements with both TRENDnet and ASUS. While such agreements are a step in the right direction, they fall short for three reasons. First, the actions are brought after the wrongdoing, and the ensuing harm to consumers has already occurred. Second, the agreements only bind the companies that were parties to them. Other companies typically look to these agreements and change their

---

[7] Centers for Medicare and Medicaid Studies, *Are You a Covered Entity (Apr. 2, 2013),* https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/AreYouaCoveredEntity.html.

[8] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 86, 136 (2013).

[9] *Id.*

[10] 15 U.S.C. § 45(a)(2) (2012).

[11] Federal Trade Commission, *FTC Approves Final Order Settling Charges Against TRENDnet, Inc.* (Feb. 7, 2014), https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against- trendnet-inc.

[12] *Id.*

practices as a result, but they are under no obligation to do so.[13] Finally, the FTC relied on company policies and statements in bringing previous actions. This is problematic because connected home device companies may not always issue privacy policies.[14]

The FTC can also bring enforcement actions to curtail unfair practices. To do so, the FTC must show that a company injured consumers in a manner that violated public policy. FTC action is strongest when addressing an area where a federal statute provides data security requirements. Outside of such circumstances, the FTC's authority is less clear.[15] Recently the FTC brought an unfair practices action against Wyndham Hotel Group alleging that since 2008 Wyndham's "repeated security failures exposed consumers' personal data to unauthorized access."[16] The FTC's authority to bring such an action was ultimately upheld, but only after a legal battle.[17] The FTC's ability to regulate IoT practices would be strengthened by enacting legislation on data-security requirements.[18]

State data-breach notification statutes are also inadequate to address IoT security violations. Currently, forty-seven states have data breach notification laws.[19] All of those cover "personal information." However, they typically limit personally identifiable information to an individual's first and last name, plus one or more of the individual's Social Security number, driver's license number, or bank or credit card account information. This means that a breach implicating only sensor data would not trigger such laws.[20] Absent some creative interpretation, no existing state legislation covers sensor data.[21]

---

[13] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 619 (2013).

[14] Sen.se, *Terms and Conditions*, https://sen.se/store/conditions/ (Sen.se has a privacy policy listed for its online store, but does not have one for its device named "Mother") (last visited May 9, 2016).

[15] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 86, 136 (2013).

[16] Federal Trade Commission, *FTC Files Complaint Against Wyndham Hotels for Failure to Protect Consumers' Personal Information* (June 26, 2012), https://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect.

[17] *See* FTC v. Wyndham Worldwide Co., No.13-1887(ES), 2014 WL 1349019, at *6–9 (D. N.J. Apr. 7, 2014).

[18] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 86, 137 (2013).

[19] National Conference of State Legislatures, *2016 Security Breach Legislation* (May 3, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/2016-security-breach-legislation.aspx.

[20] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 86, 137 (2013).

[21] *Id.* at 138-39.

At least twenty states have introduced or are considering security breach notification bills in 2016; however, none protect sensor data.[22] Absent comprehensive federal legislation, this piecemeal legislative framework will leave types of sensor data and consumers at risk.

Privacy Issues

Because there is currently no federal mandate for privacy policies, such statements in the space of connected home devices vary tremendously. Consider the privacy policy for Nest products. Nest is transparent and clear about what they collect, how they handle and use consumer data, and who can access it. For example, with regards to sharing data with third parties, Nest's privacy policy states, "Under no circumstance do we share personal information for any commercial or marketing purpose unrelated to the delivery of Nest Products and services without asking you first. Period. We do not rent or sell our customer lists."[23] Such a policy works well within the current structure of privacy law because Nest can properly be held accountable by the FTC for misusing consumer data. However, it is not perfect, as it leaves caveats for what Nest can share with partners that are also under the Alphabet holding company.

Many privacy policies from connected home devices have weak or vague language, such as the language of Philips Hue's privacy policy on sharing with third parties: "If we are required by law to obtain your consent, or otherwise believe that your consent is appropriate in the circumstances, we will obtain your consent before we share your personal data."[24] It is much harder for the FTC to hold Philips Hue accountable for whether or not it was "appropriate" to obtain consumer consent.

There are also examples of companies collecting data with no privacy policy at all. Consider Mother, a device produced by Sen.se, which works in concert with special sensors placed throughout the home. The tags can be placed on virtually anything, and Mother collects all of the data. There is no mention of security or privacy of data anywhere in the terms of service, even though Sens.se claims to be able to collect anything about the consumer's life. The only mention of the collected data on the website is: "All data generated by devices you buy is yours, only yours. Period. At any time, you can of course choose to delete all your recorded

---

[22] National Conference of State Legislatures, *2016 Security Breach Legislation* (May 3, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/2016-security-breach-legislation.aspx.

[23] Nest, *Privacy Statement for Nest Products and Services* (Mar. 10, 2016), https://nest.com/legal/privacy-statement-for-nest-products-and-services/.

[24] Philips Hue, *Privacy Notice for Hue* (Feb. 24, 2015), http://www2.meethue.com/en-us/privacy-policy/.

data."[25] This gives the FTC limited ability to hold this company accountable for any deceptive practices.

Because there are currently so many different levels of privacy policies in this space, it is difficult for the FTC to be able to consistently hold companies to the same level of accountability. There should be a baseline standard that all companies must meet or exceed so that companies can be held accountable for the misuse of consumer data.

Security Issues

The consensus among many cybersecurity professionals is that most connected home devices are not only insecure, but flagrantly disregard decades of computer security research.[26] Insteon, the maker of a now-discontinued home automation product, did not require authentication to access its products' Internet-facing control services. This allowed anyone to search the Internet for these connected devices and take direct control of consumer's homes, including house lights, televisions, and garage doors.[27]

Computer security is difficult, and best practices in security will continue to evolve, but many connected home device producers ignore well-known basics,[28] such as:

1. Using strong encryption wherever possible, when well-known cryptographic algorithms and libraries for implementing those algorithms are widespread. The Ubi smart speaker, for instance, sends all voice chats over an unencrypted connection, allowing an eavesdropper to easily listen.[29] However, open source encryption libraries, like OpenSSL, have been available since 1998.[30]

[25] Sen.se, *Mother*, https://sen.se/mother/ (last visited May 9, 2016).

[26] Bruce Schneier. *The Internet of Things is Wildly Insecure—And Often Unpatchable*, WIRED (Jan. 6, 2014), http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/.

[27] Kashmir Hill. *When "Smart Homes" Get Hacked: I Haunted a Complete Stranger's House via the Internet*, FORBES (July 26, 2013), http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/#3f469cf846a5.

[28] IoT Village, *IoT Village DEFCON 2015*, https://www.iotvillage.org/ (last visited May 9, 2016).

[29] Sarthak Grover & Nick Feamster, *The Internet of Unpatched Things – PrivacyCon 2016*, https://www.ftc.gov/system/files/documents/public_comments/2015/10/00071-98118.pdf (last visited May 9, 2016).

[30] OpenSSL Project, *OpenSSL Changelog*, https://www.openssl.org/news/cl098.txt (last visited on May 9, 2016).

2. Avoiding weak and generic default passwords, which attackers can easily guess, an insecurity known at least since the 1979 paper, "Password Security: A Case History".[31] However, just this February, ASUS settled in court over a router that was specifically marketed as a way to "safely secure and access your treasured data" via a personal cloud, but which they secured using the default username and password "admin."[32]

3. Exposing insecure, unauthenticated services to the Internet or local network, which attackers can easily find with existing tools. This is startlingly common with devices incorporating cameras, as mentioned above, even though the concept of disallowing some network connections has at least existed since 1993.[33]

4. Failing to make use of modern security mitigations, which standard tools often bake in for free,[34] and to apply updates, even though open source package managers like APT have allowed users to update system packages on Linux since at least 1999.[35]

Regulate *Use* of Data, Not Collection

Connected home devices are not only insecure, but are also privy to information gleaned from sensors distributed throughout the owner's home. Therefore, a firm understanding of what data devices collect, how they use it, and to whom they send it is crucial for owners.

From a technical and economic standpoint, however, data collection is difficult to regulate. Consumers are knowingly buying devices whose job is to sense the environment around them and installing these devices in their home. Whether or not consumers are aware of or comfortable with just how invasive connected home devices may be is both difficult to determine

---

[31] Robert Morris & Ken Thompson, *Password Security: A Case History*, 22 COMMUNICATIONS OF THE ACM 594 (1979).

[32] Federal Trade Commission, *ASUS Settles FTC Charges that Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk* (Feb. 23, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.

[33] Steven McCanne & Van Jacobson. *The BSD Packet Filter: A New Architecture for User-Level Packet Capture*, PROCEEDINGS OF THE USENIX WINTER 1993 CONFERENCE (1993).

[34] As an example, Address Space Layout Randomization (ASLR) was first described and implemented for Linux in 2001 (https://pax.grsecurity.net/docs/aslr.txt). ASLR is enabled in embedded Linux, an operating system used by many routers, by providing two additional flags when compiling the application (Cisco Application Developer Security Guide: https://developer.cisco.com/media/onepk_security_guide/GUID-527CB4BF-B5AC-41A3-92B1-883C09B8730D.html).

[35] Debian, *A Brief History of Debian*, https://www.debian.org/doc/manuals/project-history/ch-detailed.en.html#s4.1 (last visited on May 9, 2016).

and subject to change over time. After all, the entire point of many connected home devices is to leverage sensor data to create value for the customer, an activity we do not wish to curtail.

For these reasons we find it unlikely that limiting collection is the best way to protect user privacy. We will instead recommend that data collection remain unfettered, but that sharing collected data with other entities, which should leave some form of paper trail, be carefully regulated for abuses of privacy.

Proposed Policy Solution

The Connected Home Information Privacy & Security Act (CHIPS) aims to establish a federal privacy and data protection law for connected home devices while permitting covered entities to propose alternative standards. CHIPS proposes two regulatory pathways for covered entities. Covered entities can either comply with a baseline set of privacy standards, or they can propose alternative guidelines that meet or exceed CHIPS's baseline standards. CHIPS will grant the FTC both oversight and rulemaking authority. The FTC will also conduct periodic reviews of the baseline standards to ensure that privacy and data security concerns are addressed as technology continues to evolve.

Option One: Baseline Standards

To ensure transparency and meaningful user consent, covered entities must provide owners with a layered privacy policy that consists of (1) a brief notice summarizing the policy's scope, and (2) a full notice describing the collection, use, and disclosure of data in detail.

When the device is first activated, covered entities must provide notice to the owner regarding the data collected using the sensors in the device. The notice must state the sensors in the device, the types of data the sensors collect, the ways the data are used, and the purposes for which data are collected. Consent to collect personal sensor information can be obtained through layered notice. Absent informed, written consent from the owner, covered entities are prohibited from disclosing the data collected by the device to third parties. There are two exceptions: consent is not required (1) for inter-device communication, or (2) in response to a court order. Third parties that receive the information are called business associates. They may disclose personal sensor information only after obtaining the written consent of the covered entity.

The Act requires covered entities and business associates to secure personal sensor information. The Act provides covered entities with a non-exhaustive list of adequate security measures tailored to connected home devices. The list is drawn primarily from best practices in government and private industry, with the intent of maximizing security at minimal cost to covered entities. Both covered entities and business associates are required to strongly encrypt personal sensor information at all times, thus ensuring that such information receives adequate

protection regardless of who possesses it. Before receiving personal sensor information, business associates must enter into a written agreement with the covered entity regarding how they handle that information.

No list, however, will remain sufficient to ensure data security indefinitely. Consequently, covered entities and business associates shall look to standards developed and promulgated by the National Institute for Standards and Technology (NIST) for encryption and passwords, such as NIST Special Publications 800-57 Part 1 Revision 4 and 800-118. NIST guidance ensures that adequate security measures keep pace with technological development. NIST frequently refreshes best practices on cryptography and security practices, and opens up drafts to public comments. We recognize that software security is an evolving field and encourage covered entities to propose standards that meet or exceed these criteria.

Option Two: Alternative Standards

Given the wide array of devices available and the types of information they collect, CHIPS provides covered entities the opportunity to propose alternative standards to the FTC for approval. The FTC shall seek public comment and issue a written determination within 180 days of the filing of the application.

Criteria for Approval

Allowing covered entities to propose alternative privacy and data security standards promotes both flexibility and innovation. However, consumer privacy must not become a secondary consideration. As a result, those seeking to employ alternative standards must articulate rational reasons for not applying the baseline standards. In determining the validity of such reasons, the FTC may consider, among other factors, the nature of the device and the burden the baseline standards will place on that device. Additionally, the proposed standards must meet or exceed the baseline standards' protections for owners. Finally, the standards must provide annual review mechanisms to determine the sufficiency of privacy and data security practices, as well as enforcement mechanisms to rectify instances of noncompliance.

Enforcement

The FTC has oversight and rulemaking authority over the covered entities. A willful or negligent violation of the baseline privacy standards or regulations promulgated under this Act is considered an unfair, deceptive, or abusive act or practice as defined in the FTC Act. In case of a data breach, a covered entity is required to disclose the breach to the owners, and a business associate must disclose to the covered entity. The notice must be (1) written in plain language, (2) titled "Notice of Data Breach," and (3) issued within ten days of discovering the breach.

Advantages and Challenges

The proposed legislation offers strong baseline standards that protect consumers' privacy while allowing companies to innovate. The flexible approach of giving covered entities the option to develop alternative standards will incentivize them to improve security and privacy protections. Also, the legislation gives the FTC a proactive role in enforcement and requires covered entities to notify owners in case of a data breach.

By defining a willful or grossly negligent violation of the baseline standards as an unfair, deceptive, or abusive act or practice as defined in the FTC Act, the legislation draws on the FTC's existing regulatory and enforcement mechanisms. Also, forty-seven states have enacted similar data breach notification provisions to date.

Because the proposed legislation imposes significant requirements on the covered entities in an area that is currently largely unregulated, the companies will likely object to the baseline standards. They will cite to higher costs, technical limitations, and decreased competitiveness as reasons for opposing the legislation.

However, these objections do not outweigh the need for privacy and security protections. Adequate security standards are ubiquitous and cost-effective in today's computers, and most connected devices are computers in that they can be programmed to carry out different functions. Setting aside computing power and storage to implement security measures imposes only minimal costs. Development costs may be more significant, but the availability of open source packages can reduce or offset such expenditures.

In addition, privacy and security standards will spur innovation and expand the market by assuring consumers of the devices' safety. As consumers gain confidence in the devices' protection of their personal information, they are more likely to adopt the new technology, thus facilitating the market's growth. The option to propose alternative standards further incentivizes companies to devise ways to meet the standards more effectively than their competitors.

Conclusion

Connected home devices already promise substantial improvements to consumers' lives. Innovation in the space, and the benefits it brings, cannot be discounted, but neither can we ignore the dangers inherent in filling the home with Internet-connected devices, which generate and transmit rich datasets that may be used to infer private details about people's lives.

With little regulation on connected home devices, consumers currently rely on the privacy policy statements provided by the companies, which see clear value in their customers' data. The FTC, already possessing experience in pursuing privacy complaints, has recently begun to investigate unfair and deceptive security practices. Setting baseline privacy standards and requiring manufacturers and third parties to implement security measures provide much-

needed protections to consumers while leaving developers largely free to innovate and improve their devices.

The CHIPS Act

Connected Home Information Privacy and Security Act

What is the Internet of Things (IoT)?

IoT is the ever-growing network of connected devices designed to make our lives easier and more enjoyable.

Why the Excitement about IoT?

Connected home devices can improve:

1. Energy conservation
2. Automation and convenience
3. Health and safety
4. Consumer choice

Why the Worries about IoT?

Data privacy is not well-regulated.

1. No federal law protects sensor data.
2. The FTC's enforcement is limited.
3. State data breach laws do not cover sensor data.

Security is often weak.

Device vulnerabilities are routinely exploited, granting hackers control over the devices and the personal information collected.

How Does the CHIPS Act Protect Privacy?

Baseline Standards

1. Notice and Consent

Covered entities must:

- Provide layered notice to collect information.
- Obtain informed, written consent to disclose data.

Business associates must:

- Obtain written consent from covered entities to disclose information.

2. Security Standards

CHIPS mandates adequate measures including:

- Encrypting personal sensor information.
- Never using weak passwords.
- Never running an unauthenticated service.
- Timely security updates.

3. Data Breach Disclosure

Covered entities must notify owners in the event of a data breach.

Alternative Standards

Covered entities may propose alternative standards that meet or exceed CHIPS standards.

Proposals are subject to FTC approval.

Rulemaking & Enforcement

The FTC is granted rulemaking authority to implement the baseline standards.

Violations of CHIPS are treated as unfair or deceptive acts.

Alex Noakes, Craig Wesoly, Johnny Wong, Clark Wood

The CHIPS Act: Connected Home Information Privacy and Security Act
Section-by-Section Summary

Alex Noakes, Craig Wesoly, Johnny Wong, Clark Wood

Section 1: Short Title

Section 2: Definitions

- **Connected Home Device:** includes any computer that (1) collects, accesses, manipulates, or analyzes; and (2) stores or transmits any sensor data originating within a home. This definition is designed to encompass a wide range of devices that raise privacy concerns in the home. Its broad language ensures that the Act will remain relevant as technology evolves. Exceptions are made for networking equipment like modems and routers because they generally function as data channels. Exceptions are also made for electronic devices that are useful both inside and outside the home, which include cell phones, personal computers, tablets, and wearables. These exceptions are included to avoid placing an unreasonable burden on other industries.
- **Owner:** means the owner of the connected home device.
- **Covered Entity:** includes those companies that manufacture connected home devices or develop the software that runs on or accesses personal sensor information from connected home devices, as they have significant access to the devices and personal sensor information.
- **Business Associate:** means a person or entity that receives or accesses personal sensor information from a covered entity or another business associate. This definition is inspired by HIPAA and is intended to ensure that such information remains protected when disclosed to third parties.
- **Sensor:** means a device that detects or measures a physical property and records, indicates, or otherwise responds to it.
- **Sensor Data**: means any data collected by a sensor. This broad definition is meant to distinguish data collected by sensors and data collected in other ways, such as billing information provided by an owner.
- **Protected Health Information:** means any sensor data that are related to the health of an individual. This definition is modeled after the one used in HIPAA.
- **Personal Sensor Information:** means any sensor data that a connected home device collects about an individual. Personal sensor information is distinguished from sensor data that do not pertain to the individual, such as weather records. This distinction is made so that personal sensor information can be more strictly protected than other sensor data.
- **Inter-Device Communication:** means the transmission of data between any two or more connected home devices belonging to the same owner. The potential of a connected home depends on devices communicating with each other, so the Act exempts this type of communication from consent requirements. This exemption balances consumer control over their data with the convenience offered by interoperation between connected home devices. Because the owner bought the devices and enabled their interoperation, it is reasonable to assume that the owner intends for the devices to work in concert and communicate with each other.
- **Layered Notice:** means a two-tiered privacy notice containing (1) a summary of the policy's scope, as well as basic points concerning a covered entity's practices for the

collection, use, disclosure, and security of personal sensor information; and (2) a full notice containing all material information on a covered entity's practices for collection, use, disclosure, and security. This two-tiered structure aims to improve upon existing notices, which may be difficult to understand and are rarely read by consumers. The first layer should provide owners with the information necessary to make an informed decision, and the owners can refer to the second layer for more details.

- **Unauthenticated Service:** means any computer program that may be accessed or used without a user providing proof of his or her identity. Many unauthenticated services have a well-tested, low-cost, and secure alternative, such as configuring the File Transfer Protocol (FTP) to disallow anonymous logins.
- **Security Update:** means any change to computer software intended to remove any software vulnerability. Covered entities should send periodic updates to ensure the security of the device and to patch any vulnerabilities that have been found.

Title I: Baseline Privacy Standards

Section 101: Authority of the Federal Trade Commission (FTC)

- The Act grants the FTC rulemaking authority to promulgate regulations that achieve the standards set forth in Title I. Given its extensive experience in protecting consumers and regulating privacy, the FTC is best suited to implement the standards.
- The FTC shall conduct periodic reviews of these standards and update them as necessary.

Section 102: Notice and Consent

- Before collecting personal sensor information, a covered entity must provide the owner with a privacy notice.
- The privacy notice must explain what types of sensor data are collected, how the personal sensor information is used, how the personal sensor information is secured, and who has access to the personal sensor information.
- The privacy notice must be presented in the form of a layered notice, which provides owners with relevant information in a format that is easy to understand. If the device is designed to collect protected health information, privacy notices must conform with the HIPAA standards established in 45 C.F.R. §§ 164.501, 164.502, 164.504, 164.512, 164.532, 164.534.
- Consent for collection may be obtained by providing a layered notice to the owner, but disclosure requires the informed, written consent from the owner. The use of two different standards seeks to strike a balance between consumer privacy and market innovation.
- Business associates may disclose personal sensor information only after obtaining the written consent of the covered entity. This holds covered entities accountable for the subsequent use and disclosure of such information.
- Consent for disclosure is not required for the purposes of inter-device communication between devices belonging to the same owner, as such communication is enabled by the owner to realize the potential of a connected home.
- Consent to disclose is also not required in response to a court order issued pursuant to 18 U.S.C. § 2518. The higher requirements prescribed by the Wiretap Act for a court order

better protect privacy expectations surrounding connected home devices than mere probable cause required for a warrant.

Section 103: Security Measures

- The Act requires covered entities and business associates to secure personal sensor information. The Act provides covered entities with a non-exhaustive list of adequate security measures tailored to connected home devices. The list is drawn primarily from best practices in government and private industry, with the intent of maximizing security at minimal cost to covered entities.
- Covered entities and business associates shall look to standards developed and promulgated by the National Institute for Standards and Technology (NIST) for encryption and passwords, such as NIST Special Publications 800-57 Part 1 Revision 4 and 800-118. NIST guidance ensures that adequate security measures keep pace with technological development.
- Both covered entities and business associates are required to strongly encrypt personal sensor information at all times, thus ensuring that such information receives adequate protection regardless of who possesses it.
- Before receiving personal sensor information, business associates must enter into a written agreement with the covered entity regarding how they handle that information.

Section 104: Data Breach Responses

- Covered entities must notify owners of any security breach in which the owner's personal sensor information was or is reasonably believed to have been compromised. Business associates must notify the covered entity of any such breach.
- A security breach notice must be titled "Notice of Data Breach," written in plain language, and issued within 10 business days. These requirements are modeled after those in California's data breach law.

Title II: Alternative Privacy Standards

Section 201: Standards Proposed by Covered Entities

- To afford flexibility and incentivize innovation, covered entities may submit proposals of alternative standards to the FTC. The FTC must respond within 180 days.
- The proposed standards may only be approved if (1) the covered entity articulates rational reasons to not apply the baseline standards; (2) the proposed standards meet or exceed the baseline standards' protections; and (3) the proposed standards provide annual review and enforcement mechanisms. These requirements ensure that the alternative standards are necessary and robust.

Title III: Enforcement

Section 301: Federal Trade Commission

- Any willful or negligent violation of the Act will be treated as an unfair, deceptive, or abusive act or practice. Such violations are subject to FTC enforcement.
- The Act does not provide a private right of action.

Connected Home Information Privacy and Security Act

Alex Noakes, Craig Wesoly, Johnny Wong, Clark Wood

SECTION 1. SHORT TITLE.

This Act shall be known as the Connected Home Information Privacy and Security Act (CHIPS).

SECTION 2. DEFINITIONS.

(a) "Connected Home Device" includes—

(1) any computer (as defined by 18 U.S.C. § 1030(e)(1)) that

(A) collects, accesses, manipulates, or analyzes; and

(B) stores or transmits—

sensor data originating within a residence or domicile.

(2) Exceptions. Connected Home Device does not include—

(A) devices solely used as networking equipment, including but not limited to modems and routers; or

(B) devices whose predominant purpose is independent of the home, including but not limited to cell phones, personal computers, tablets, and wearables.

(b) "Owner" means the owner of the connected home device.

(c) "Covered Entity" includes—

(1) any manufacturer of connected home devices; and

(2) any developer of a software application that runs on or accesses personal sensor information from a connected home device.

(d) “Business Associate” means a person or entity that receives or accesses personal sensor information from a covered entity or another business associate.

(e) “Sensor” means a device that detects or measures a physical property and records, indicates, or otherwise responds to it.

(f) “Sensor Data” means any data collected by a sensor.

(g) “Protected Health Information” means any data that relate to the past, present, or future physical or mental health or condition of an individual; or the provision of health care to an individual.

(h) “Personal Sensor Information” means any sensor data that a connected home device collects about an individual.

(i) “Inter-Device Communication” means the transmission of data between any two or more connected home devices belonging to the same owner.

(j) “Layered Notice” means a two-tiered notice containing the following—

(1) Tier 1. A concise notice containing—

(A) A summary of the notice’s scope, as well as basic points concerning a covered entity’s practices for the collection, use, disclosure, and security of personal sensor information;

(B) An easy way to access the relevant portions of the full notice; and

(C) Contact information for personnel responsible for information privacy.

And—

(2) Tier 2. A full notice containing all material information on a covered entity's practices for the collection, use, disclosure, and security of personal sensor information.

(k) "Unauthenticated Service" means any computer program that may be accessed or used without a user providing proof of his or her identity.

(l) "Security Update" means any change to computer software (as defined by 48 C.F.R. § 2.101) intended to remove any software vulnerability.

TITLE I: BASELINE PRIVACY STANDARDS

SECTION 101: AUTHORITY OF THE FEDERAL TRADE COMMISSION (FTC)

(a) **In general.**

(1) No later than 1 year after the passage of this Act, the FTC shall prescribe rules that define with specificity the baseline privacy standards described in Title I.

(2) The FTC may prescribe interpretive rules and general statements of policy on the baseline privacy standards.

(3) The FTC shall conduct periodic reviews of the baseline privacy standards and update the rules as necessary.

(b) **Procedures applicable.** When prescribing a rule under this Act, the FTC shall proceed in accordance with 5 U.S.C. § 553.

SECTION 102: NOTICE AND CONSENT

(a) **In general.**

(1) Before collecting personal sensor information, a covered entity shall provide the owner with a conspicuous notice of the terms and conditions concerning the collection, use, disclosure, and security of the personal sensor information.

(2) If a connected home device is designed to collect protected health information, notice must conform with the standards prescribed in 45 C.F.R. §§ 164.501, 164.502, 164.504, 164.512, 164.532, 164.534.

(b) **Notice requirements.** The notice required under subsection 102(a) shall include—

(1) a layered notice; and

(2) all material information on the following—

(A) The sensors that the connected home device contains;

(B) The types of sensor data collected;

(C) How personal sensor information is used;

(D) The purposes for which personal sensor information may be disclosed;

(E) The third parties to which personal sensor information may be disclosed; and

(F) Compliance with adequate security measures described in § 103 of this Act.

(c) **Consent.**

(1) **Collection.** Consent to collect personal sensor information can be obtained by providing a layered notice to the owner.

(2) **Disclosure.**

(A) **In general.** Personal sensor information may not be disclosed before obtaining the informed, written consent of the owner. Such consent may be obtained at the same time the layered notice is provided.

(B) **Exceptions.**

(i) Consent is not required in the following circumstances—

(I) For the purposes of inter-device communication; or

(II) In response to a court order issued pursuant to 18 U.S.C. § 2518.

(ii) Business associates may disclose personal sensor information only after obtaining the written consent of the covered entity, provided that the covered entity has complied with subsection 102(c)(2)(A).

SECTION 103: SECURITY MEASURES

(a) **In general.** Covered entities shall take adequate measures to ensure the security of connected home devices and personal sensor information.

(b) **Adequate measures.** Adequate measures include, but are not limited to—

(1) Strongly encrypting personal sensor information at all times in transit or at rest;

(2) Strongly encrypting all data transmitted over the network, unless to do so would result in an unreasonable burden on the covered entity or connected home device;

(3) Eschewing the use of weak default passwords or suggesting the use of weak passwords to owners;

(4) Never running an unauthenticated service that provides any means of access to the connected home device; and

(5) Providing a secure way to receive and apply security updates in a timely fashion.

(c) Business associates shall comply with subsection 103(b)(1).

(d) Before receiving personal sensor information, a business associate must enter into a written agreement with the covered entity, affirming the business associate's responsibility to—

(1) Comply with subsection 103(b)(1);

(2) Prevent the use or disclosure of the personal sensor information other than as provided for by its contract; and

(3) Report to the covered entity any use or disclosure of the personal sensor information not provided for by its contract of which it is aware.

(e) Covered entities and business associates shall look to standards developed and promulgated by the National Institute for Standards and Technology when implementing strong encryption and passwords.

SECTION 104: DATA BREACH RESPONSES

(a) **In general.** A covered entity shall disclose a breach of the security of personal sensor information or a connected home device following discovery or notification of the breach to an owner whose personal sensor information was, or is reasonably believed to have been, acquired by an unauthorized person.

(b) A business associate shall disclose a breach of the security of personal sensor information following discovery or notification of the breach to the covered entity with which it has entered into an agreement.

(c) **Notice requirements.** A security breach notification issued pursuant to this section shall be—

(1) Titled "Notice of Data Breach";

(2) Written in plain language; and

(3) Issued within 10 business days of discovery or notification of the breach.

(d) If a connected home device is designed to collect protected health information, a data breach response must be conducted in accordance with the requirements prescribed in 45 C.F.R. §§ 164.400, 164.402, 164.404, 164.406, 164.408, 164.410, 164.412, 164.414.

TITLE II: ALTERNATIVE PRIVACY STANDARDS

SECTION 201: STANDARDS PROPOSED BY COVERED ENTITIES

(a) **In general.** In place of the standards set forth in Title I of this Act, covered entities may propose alternative standards to the FTC for approval.

(b) **FTC review.** Upon receipt of the application, the Commission shall seek public comment and issue a written determination no later than 180 days after the filing. In order for an application to be approved, the following conditions must be met—

(1) A covered entity's application must articulate rational reasons to not apply the baseline standards;

(A) In determining the validity of such reasons, the FTC may consider, among other factors—

(i) The nature of the connected home device; and

(ii) The burden the baseline standards place on that connected home device.

(2) The proposed standards must meet or exceed the baseline standards' protections for owners;

And—

(3) The proposed standards must provide—

(A) Annual review mechanisms to determine the sufficiency of privacy and data security measures; and

(B) Enforcement mechanisms to rectify instances of noncompliance.

TITLE III: ENFORCEMENT

SECTION 301: FEDERAL TRADE COMMISSION

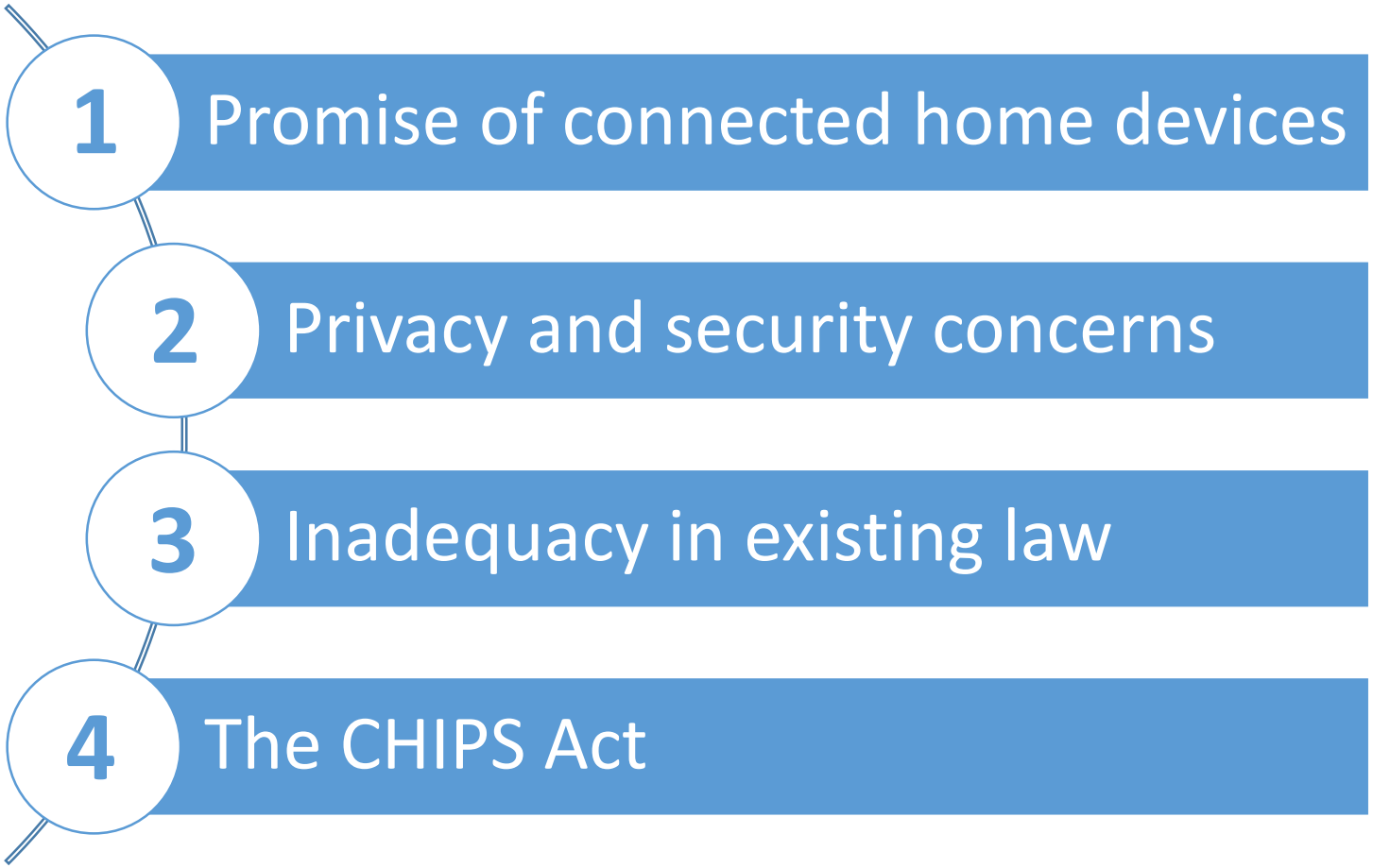
(a) A willful or negligent violation of Title I of this Act, or a regulation promulgated under this Act, shall be treated as a violation of the rules defining unfair, deceptive, or abusive acts or practices prescribed under § 18(a)(1)(B) of the FTC Act (15 U.S.C. § 57a(a)(1)(B)).

(b) Nothing in this Act shall be construed as providing a private right of action.

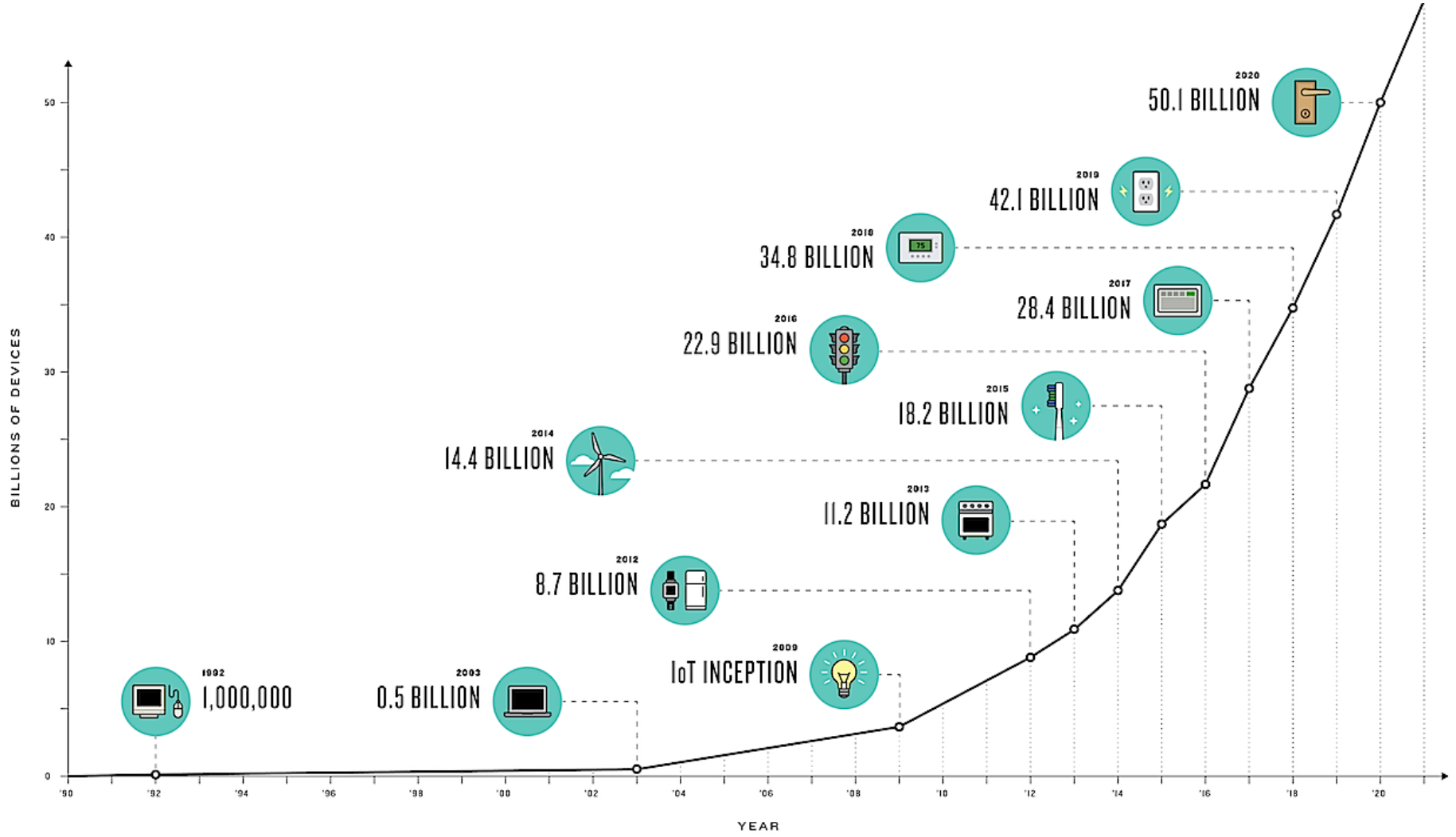
The CHIPS Act:

Connected Home Information Privacy and Security

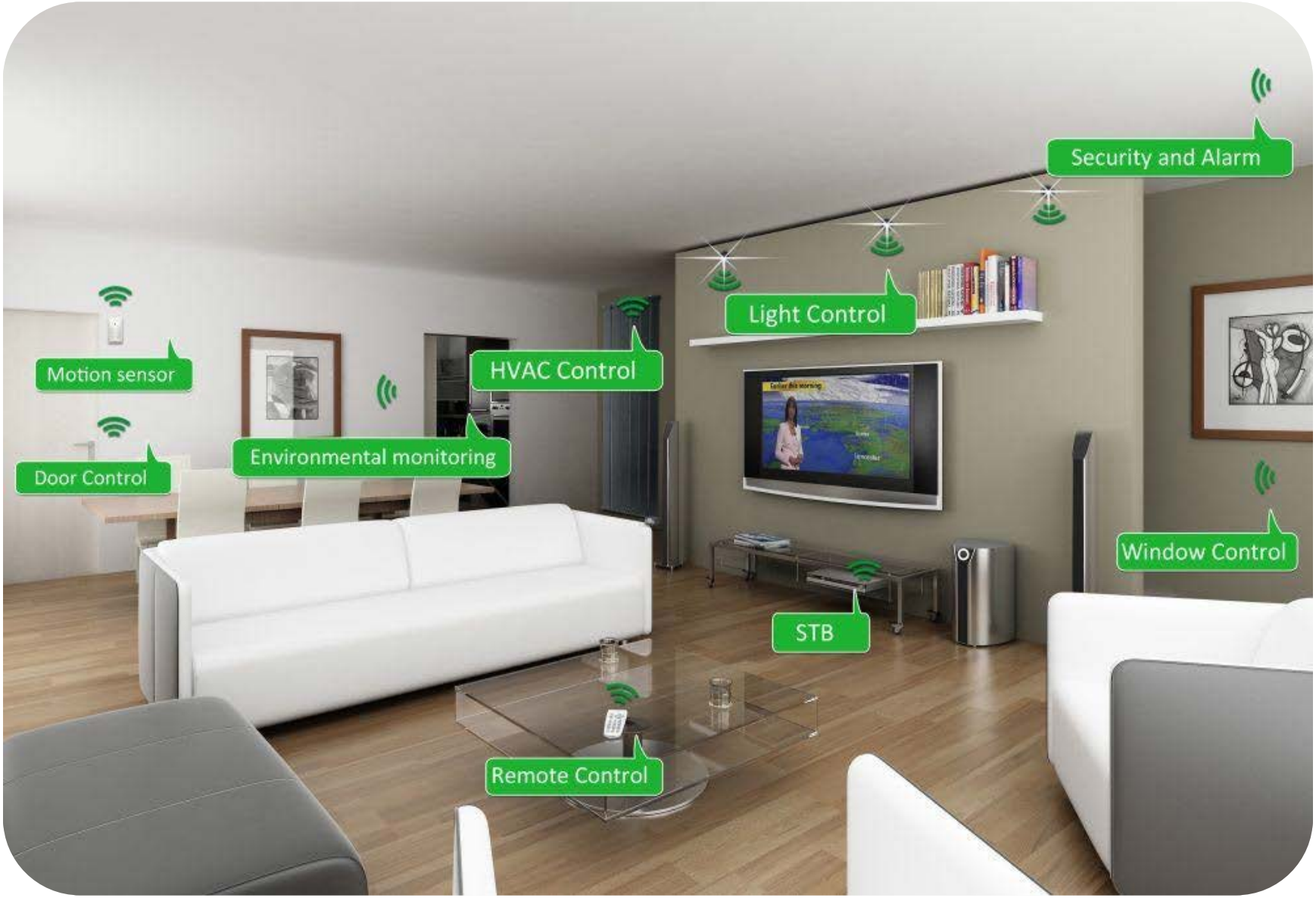
Alex Noakes, Craig Wesoly, Johnny Wong, Clark Wood


1
Promise of connected home devices
2
Privacy and security concerns
3
Inadequacy in existing law
4
The CHIPS Act

Internet of Things (IoT)



The Connected Home



Risks of the Connected Home

Case Study: Smart Baby Monitors

- Connected to Internet, live video, mobile apps
- Vulnerabilities
  - Backdoor credentials
  - Authentication bypass
  - Default credentials like “admin”/”admin”

Our Investigation

Other Vulnerable Devices

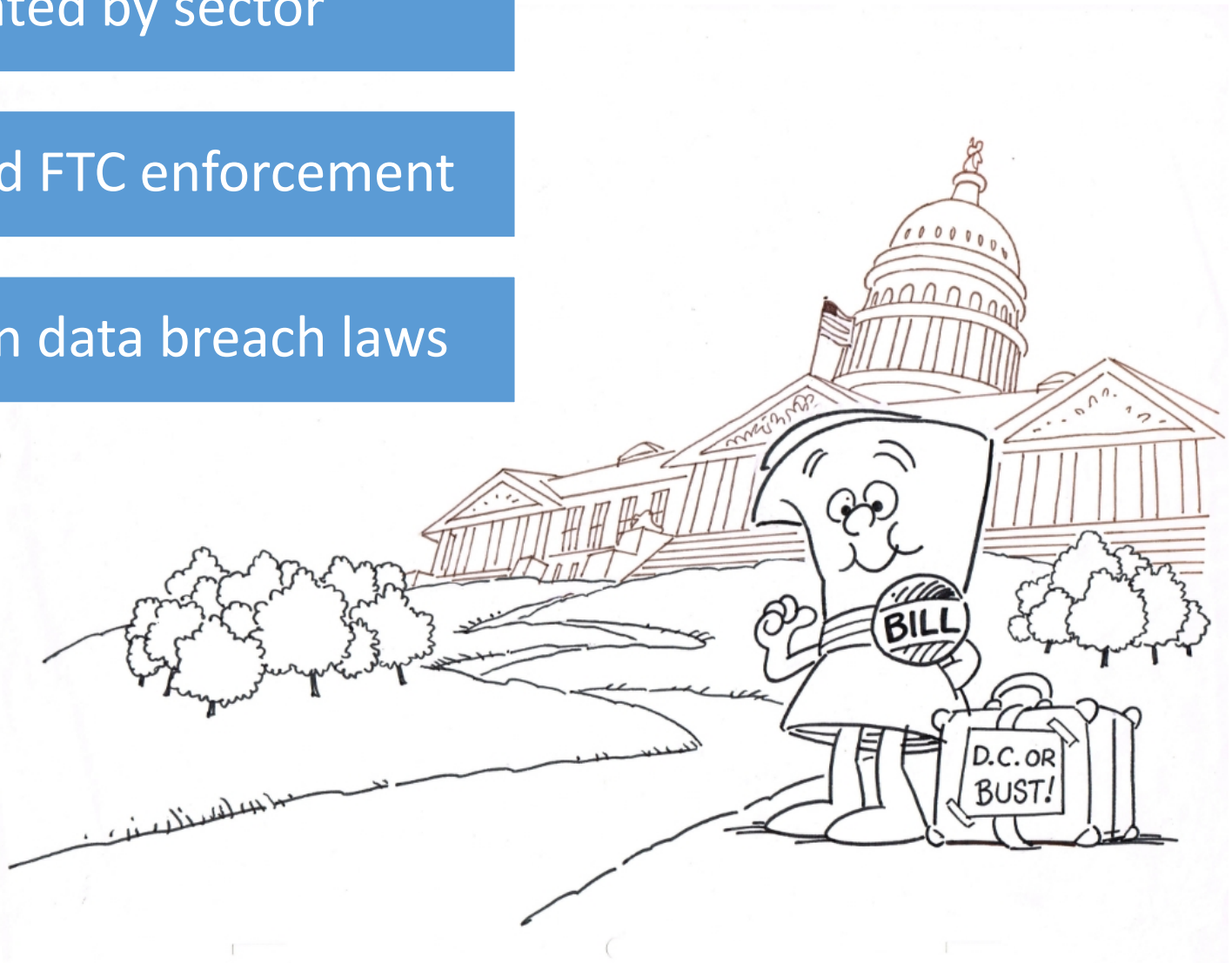
What Your Home Knows

Existing Law is Lacking

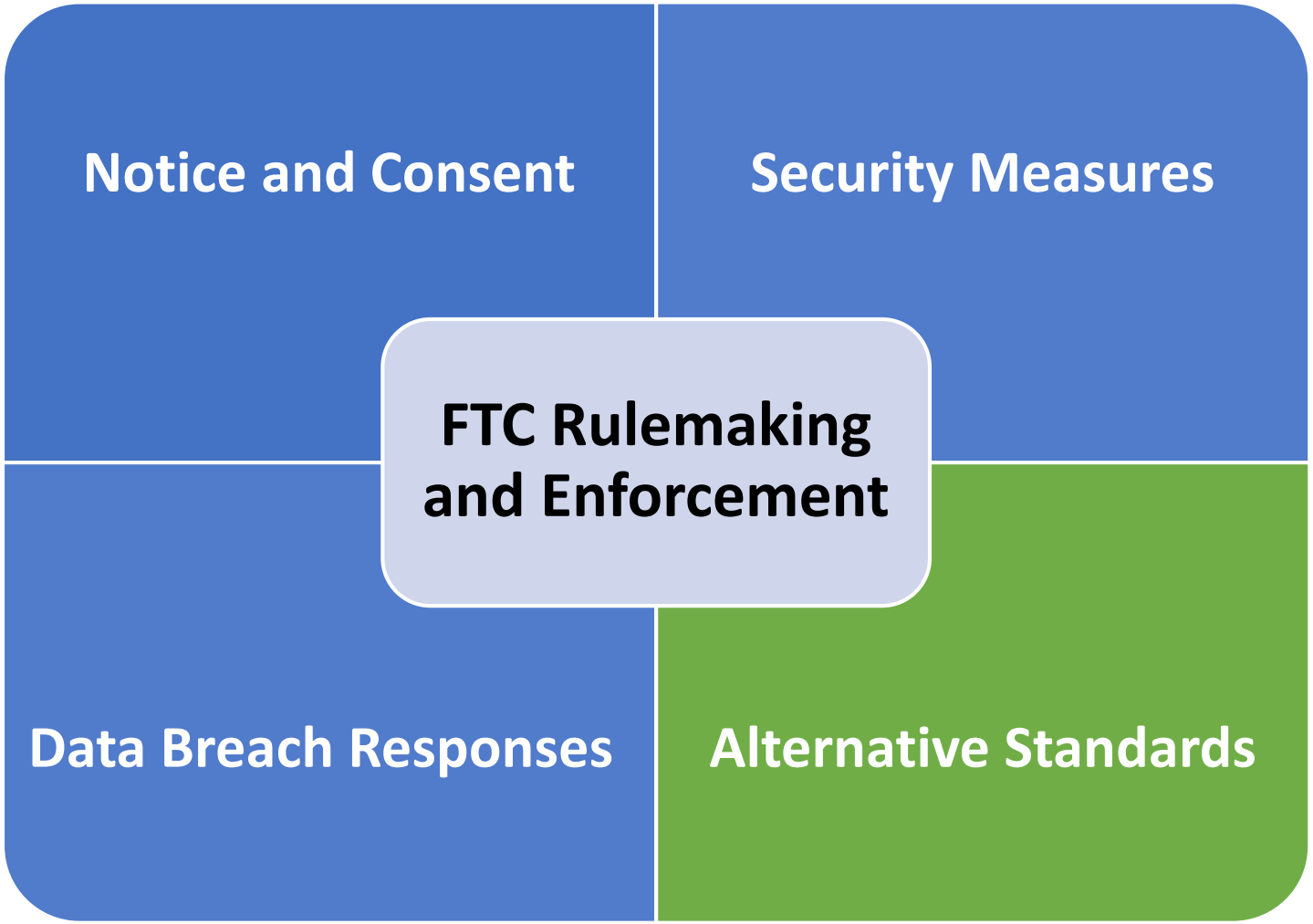
Regulated by sector

Limited FTC enforcement

Gaps in data breach laws

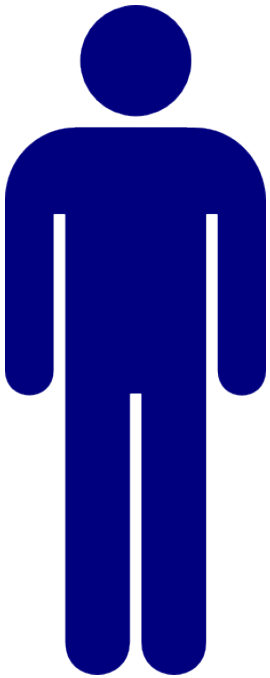


Solution: The CHIPS Act



Who is Affected

Owner



Covered Entities

nest

hue PHILIPS

amazon echo

Business Associates

datalogix

acxiom

Google Cloud Platform

amazon web services

Layered Notice

Information P&G Collects

Click here for more information

- P&G collects information about you from a variety of sources, including:
  - Information we collect from you directly.
  - Information w… obile applications or services, or vi…
  - Information w… available sources.
- All the information P&G … cations with you, and to develop world-class pr…

dev…

Uses

- P&C…
- We…
- We…
- If yo… serv…

…rmation …ss …y if we …send …nd

Your …

- You… thos… uns…
- Clic…

…rmation …s in

Information P&G Collects

We may collect information about you from a variety of sources. This includes information we collect directly from you; information we collect when you visit our sites, view our online content or use our mobile applications or other services; and information we collect about you from other sources.

Information we collect directly from you

We collect information directly from you when you choose to participate in our offers and programs, create an account on our websites or in our mobile applications, call or email us, or otherwise provide information directly to us. The following are examples of information we may collect directly from you:

- Name.
- Email address.
- Postal address.
- Username and password.
- Telephone and/or fax number.
- Date of birth.
- Other household information about you and your family such as gender or product use preferences and/or behaviors.
- Health information, such as health information related to product usage and medical history.
- Biometrics collected during volunteer consumer research studies (such as facial expression recognition, heart rate, and skin condition).
- Demographic information.
- Payment information (such as a credit card).
- Future communication preferences.
- Contact information for friends you may wish us to contact.
- Telephone number and recordings when you call our consumer line.

Information we collect when you visit our sites, view our online ads or promotions, or use our mobile applications or other services

We use cookies and other technologies to collect information when you visit our sites, view our online advertisements or promotions, or use our mobile applications or other services. The following are examples of information we may collect with these technologies:

- Information about your device browser and operating system.
- IP address.
- Web pages you view.
- Links you click.
- P&G emails you open.

Information collected through Mobile Applications

When you download our mobile applications to your mobile device we may also collect information that you provide. We also automatically collect information through our applications.

The following are examples of the types of information we may automatically collect through our applications:

- Advertising ID or similar identifier.
- Information about your device's operating system.
- Information about the way you use the application.

Consent for Collection and Disclosure

Covered Entities

Collection: Provide layered notice to owner
Disclosure: Obtain informed, written consent from owner

Business Associates

Disclosure: Obtain written consent from covered entity

Exceptions


Inter-device communication


Wiretap Act warrants


Protected health information

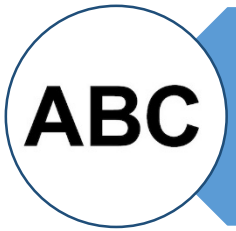
Security Measures

Security Measures	Covered Entities	Business Associates
NIST security standards	✓	✓
Strong encryption at all times	✓	✓
Written agreement to protect info	✓	✓

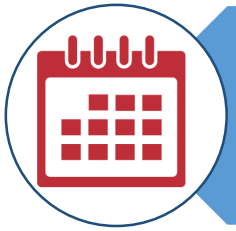
Data Breach Response

Notices Must Be:

Titled “Notice of Data Breach”



Written in plain language



Issued within 10 days of discovery

Alternative Standards

Covered Entities Must Propose:

- A reason why baseline should not apply
- Standards that meet or exceed the baseline
- Enforcement mechanisms
- Annual review mechanisms

FTC Rulemaking and Enforcement

Questions?