THE TROJAN HOUSE

EVAN ENZER
ARJUN RAVI
JULIAN MELENDI
SOHINI UPADHYAY
ELENI MANIS, PHD, MPA

DEC 15, 2022

Supported in part by a grant from the John D. and Catherine T. MacArthur Foundation
EXECUTIVE SUMMARY

• “Smart home” devices record audio and video in the home—and even collect daily schedules and health details.

• Once collected, this data is less than a warrant or data breach away from police and hacker access.

• Across the board, smart home devices have superior, privacy-protecting alternatives that perform the same key functions.

• The law doesn’t protect smart home users. “Do not buy” is the best advice until it does.
I. INTRODUCTION

While the marketing will feature cozy holiday cheer, gifting so-called “smart” home devices—internet-connected speakers, thermostats, beds, vacuums, and other home appliances—is a bad idea. Smart devices are a popular holiday purchase, but bringing this technology into a home enables detailed government and corporate surveillance. A smart vacuum like Roomba will clean your floors, but it wants to case the joint it cleans, demanding a detailed floorplan for optimal performance. For smart speakers, full functionality comes at the cost of bugging your home: Apple demands transcripts of user interactions with its speakers, while Google demands complete audio recordings. Once collected, user data is less than a warrant or data breach away from police, hackers, and other actors who don’t have users’ interests in mind.

This home surveillance is needless and avoidable. Every smart home device reviewed below has a superior, privacy-protecting alternative that performs the same key functions. This guide makes the case for getting smart by embracing “dumb” and opting for superior, privacy-preserving gifts for the home.

II. AVOIDING PREDATORY DATA COLLECTION IN THE HOME

A. Smart Speakers

A smart speaker activates when it hears its wake word (“Alexa,” “Hey Google”) and responds to user commands, often recording them. Smart speakers’ abilities vary, but they share common functions: playing music, looking up information and making recommendations, placing phone calls, and controlling compatible household devices, like the lights or TV. Beyond these basic functions, users can install apps onto their smart speakers, enabling actions like shopping by voice.

3 Ask Siri, Dictation & Privacy. Copied from a MacBook Pro’s Siri settings.
But data suggests that most people don’t use most of smart speakers’ bells and whistles. The most common use of smart speakers is…drumroll…playing music. Other popular uses include checking the weather, searching silly questions on the internet, and controlling other household devices.

Of course, you don’t need a smart speaker to do any of these things, and for each use case there is a better alternative. For the person who likes music, consider a Bluetooth-enabled speaker. It can stream music from a phone, laptop, or online service. Consumer Reports describes its top-rated Bluetooth speaker as “among the very best speakers we’ve ever tested,” with “real magic” in its midrange. By contrast, its top-rated smart speaker has “boomy” bass, “smeared” treble, and a “hazy” and “nasal” midrange. Why bother?

Likewise, for someone who wants to turn their lights on and off on a schedule, plug-in timers are more user friendly than smart speakers. Plug a timer into the wall, plug a lamp or other device into the timer, and set the desired on/off times. The task is complete without any of the hassle, added expense, or compatibility issues of smart speakers. Many tabletop appliances that people use on a regular schedule, like coffee machines, make automated scheduling even easier with a built-in timer. And for the person who would ask a smart speaker a silly question: a Magic 8 ball?

Just not a smart speaker. Smart speakers bug homes by using voice assistant software to “hear” commands and respond appropriately. Once a voice assistant hears or thinks it hears its wake word, it begins analyzing—and often recording—everything. By default, Apple collects up to six months of transcripts from a user’s conversations with Siri; a map of each user’s relationships constructed from contacts, household members, and people named in photos; and a catalog of users’ interests as conveyed by their apps, podcasts, and music. Some voice assistants let users opt out of transcripts.

---


or audio recordings, but at a loss of functionality.\textsuperscript{14} For example, users can override Amazon’s default setting and refuse to upload their exchanges with Alexa to the cloud, but then Alexa won’t tailor its responses to users—so much for being helpful.\textsuperscript{15}

People who use smart speakers to control lights, thermostats, or other devices according to preprogrammed routines are also effectively sharing their daily schedules with anyone listening or reviewing their usage data. “Siri, turn the lights on at 7:00 AM and turn the heat on at 5:00 PM” implies that you get up at seven and don’t return home until after five. “Hey Google, cancel my scheduled actions and turn down the heat” translates to “it’s vacation time.”\textsuperscript{16}

You may wonder who is monitoring this data—is anyone listening? It turns out companies can and do share users’ data with government agencies and other private entities. Voice assistant makers like Apple, Google, and Amazon field thousands of requests from federal and state and local authorities for user data. Google received over 47,000 government requests for U.S. user information over its most recent half-year reporting period and granted 84% of these requests.\textsuperscript{17} Apple granted 90% of 7,000 law enforcement requests for user account data in the U.S. over the same period, plus thousands of government requests for other information.\textsuperscript{18} Amazon received over 3,500 subpoenas, search warrants, and court orders for U.S. user data over the last 6 month period, not including national security requests, which it omits from reporting.\textsuperscript{19}

Apple,\textsuperscript{20} Google,\textsuperscript{21} and Amazon\textsuperscript{22} have also shared their voice assistants’ audio recordings with private contractors, giving them access to excruciatingly sensitive personal, financial, and health details revealed in voice assistant recordings. An Amazon team in Bucharest, Romania monitors

\textsuperscript{14} Kari Paul, “Workers Listen to AI Home Devices.”
\textsuperscript{15} “Amazon.com: Data Use,” Amazon, accessed March 3, 2022, \url{https://www.amazon.com/b/?node=23608617011}.\textsuperscript{14}
\textsuperscript{16} “Scheduling Smart Home Actions, Actions on Google Smart Home, Google Developers,” Google, November 7, 2022, \url{https://developers.google.com/assistant/smarthome/develop/scheduling}.\textsuperscript{16}
\textsuperscript{17} “Requests for User Information – Google Transparency Report,” Google, accessed November 29 2022, \url{https://transparencyreport.google.com/user-data/overview?user_requests_report_period=authority:US}.\textsuperscript{17}
\textsuperscript{22} Jack Morse, “Reminder: Your ‘Smart AI’ Often Involves a Low-Paid Contractor Surveilling You,” \textit{Mashable}, April 11, 2019, \url{https://mashable.com/article/amazon-echo-humans-listening-recordings-smart-tech}.\textsuperscript{22}
Alexa recordings and has eavesdropped on family rows, financial and health discussions, kids and guests speaking, and even couples having sex. Users regularly trigger Apple’s Siri by accident, allowing Apple contractors to overhear confidential medical and legal conversations. Smart speakers are also entry points that can give hackers control over households and access to personal information. As one cybersecurity specialist put it, “hacking a virtual assistant in millions of people’s homes is what malicious actors dream of doing.” Hackers can configure smart speakers to eavesdrop on household activity. In one high-profile case, a hacker accessed a smart baby monitor and broadcast threats to kidnap the child. This was not an isolated case: there are other accounts of hackers accessing smart monitors.

By contrast, Bluetooth speakers, plug-in timers, and other non-smart devices don’t double as wiretaps and introduce none of these risks. They can’t be hacked from a distance and don’t collect data for malicious actors to abuse.

**B. Smart Thermostats and Smart Meters**

Smart thermostats and meters operate hand in hand with smart speakers. Due to interoperability constraints, smart speakers can only control a home’s heat and air conditioning from a distance with compatible smart thermostats. Smart thermostats collect a record of utility usage including useful heating and cooling patterns and other sensitive information. This data poses a serious risk: it can be hacked from a very close distance (e.g., by someone inside one’s home), and using a streaming service with a speaker almost certainly involves data collection by the streaming service.
captures home and away routines with great accuracy.\(^{31}\) Indeed, Immigration and Customs
Enforcement (ICE) has pursued undocumented people by identifying their home address through
their utility records.\(^{32}\) In 2020, for example, ICE used utility records to locate a man who had done
nothing other than overstay his legal vacation.\(^{33}\) The data available to ICE through smart meters also
enables it to pursue individuals by identifying when they are likely to be home.\(^{34}\)

Some smart thermostats even offer smartphone applications with a “geofencing mode” to track a
user’s location and adjust their heat or air conditioning as they enter and leave their home.\(^{35}\) This is
the same tool that allows police, prosecutors and private parties to identify protestors and people
seeking abortions based on the location of their mobile devices.\(^{36}\) In one case, police used
geofencing to gather device-identifying information for every person that attended a Black Lives
Matter protest.\(^{37}\) In another, anti-abortion activists used geofence technology to harass visitors to a
reproductive health clinic.\(^{38}\) With “geofencing mode,” home residents voluntarily subject themselves
to this policing technology.

There is a simple, equally useful alternative to smart thermostats. Programmable thermostats can
adjust heating or cooling according to users’ preprogrammed demands, helping them save energy
and money without broadcasting their daily schedules over the internet.\(^{39}\) A person can’t use a
programmable thermostat to monitor their home from afar, but that’s the point: it’s not a
surveillance device, and police can’t coopt it for spying.

---

\(^{31}\) *Naperville Smart Meter Awareness v. City of Naperville*, No. 16-3766, 6 (7th Cir. 2018).


\(^{33}\) Georgia DDS, Email to Georgia DDS; B1/2 Visa Overstay by Immigrant, June 2, 2020, [GADMV_001230](#).

\(^{34}\) *See Naperville*, No. 16-3766 at 6 (7th Cir. 2018).


Though consumers can and should avoid purchasing smart thermostats, it’s important to know that malicious actors can still access data about their household routines through smart meters. As of 2018, more than 50% of U.S. homes used smart meters to monitor electricity usage and convey that data to utility companies.\footnote{Daniel Shea and Kate Bell, “Smart Meter Opt-Out Policies,” National Conference of State Legislatures, August 20, 2018, \url{https://www.ncsl.org/research/energy/smart-meter-opt-out-policies.aspx}.} Cities like NYC also monitor water usage using smart meters.\footnote{Albert Fox Cahn and Zartosht Ahlers, “Is Your Faucet Spying on You?,” \textit{New York Daily News}, June 26, 2022, \url{https://www.nydailynews.com/opinion/ny-oped-20220627-qu65yn4f6ide5odlaax2274sg6v-story.html}.} Like smart speakers and smart thermostats, these meters reveal home/away patterns and household routines. These patterns can be incredibly granular, ranging from whether someone likes to shower at night\footnote{Alexandria Franklin, “The Fourth Amendment in Your Shower: Naperville, Reasonable Expectations of Privacy, and the Intimate Nature of Electric Smart Expectations of Privacy, and the Intimate Nature of Electric Smart Meter Data,” \textit{North Carolina Law Review} 99, no. 4 (2021), \url{https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=6848&context=nclr}.} to whether guests are staying in the home.\footnote{Surya Mattu and Kashmir Hill, “The House That Spied on Me,” \textit{Gizmodo}, February 7, 2018, \url{https://gizmodo.com/the-house-that-spied-on-me-1822429852}.} In New York, individual water consumption data will soon be made public by law, making it even easier for police and others to track households’ daily patterns.\footnote{Albert Fox Cahn, “Is Your Faucet Spying?”} 

C. Smart Vacuums and Mops

Smart vacuums (and mops) are among the worst offenders in the home surveillance arena: they routinely case the joint that they clean. Smart vacuums operate by mapping a user’s home and using that map to navigate around obstacles while vacuuming.\footnote{“Privacy Policy,” iRobot.} iRobot’s Roomba vacuum stores a comprehensive digital floorplan of the house it cleans so detailed that it knows where the furniture is.\footnote{“How Does My Robot Navigate?,” iRobot, November 19, 2021, \url{https://homesupport.irobot.com/s/article/31056}.} iRobot additionally collects a range of sensitive personal data of seemingly no use to a vacuum company, including user demographics, age, whether a household includes children, and what apps users keep on their other smart devices.\footnote{“Privacy Policy,” iRobot.} Amazon recently acquired iRobot, adding home mapping to its already Orwellian tracking of individual Americans’ consumption patterns and daily lives.\footnote{Katherine Tangalakis-Lippert, “Amazon's Empire of Surveillance: Through Recent Billion-Dollar Acquisitions of Health Care Services and Smart Home Devices, the Tech Giant Is Leveraging Its Monopoly Power to Track 'Every Aspect' of Our Lives,” \textit{Business Insider}, April 28, 2022, \url{https://www.businessinsider.com/amazon-empire-of-surveillance-leveraging-monopoly-power-tracking-purchases-2022-8}.}

There are at least two good alternatives to handing one’s floorplan over to vacuum companies. For less than one-fifth of the price of the top competitor, one can buy a robot vacuum that doesn’t
collect data, couldn't share it with manufacturers if it did, and is one of Consumer Reports’ top-rated robot vacuums.\textsuperscript{49} Or, for the price of a robot vacuum, one can buy two or more top-rated traditional vacuums and give a friend the gift of vacuuming in privacy.\textsuperscript{50} Households that already have Roombas should configure them to operate offline to avoid sharing home maps with Amazon, a major source of data for law enforcement.\textsuperscript{51}

D. Smart Beds

Smart beds collect a surprising amount of health data. Ordinary adjustable beds allow users to control their mattress’s firmness and positioning. A smart bed like Sleep Number will perform these adjustments automatically and provide reports on supposed sleep quality if, in addition to providing one’s age, height, weight, and gender,\textsuperscript{52} one allows the company to collect biometric, respiration, and heart rate data.\textsuperscript{53} The company shares user data with third party companies,\textsuperscript{54} increasing the risk of a data breach that makes confidential health information publicly available.\textsuperscript{55}

And reviewers don’t even give high marks to smart beds. They suggest that a well-chosen traditional mattress can better meet a sleeper’s needs at a lower price.\textsuperscript{56} Consumer Reports doesn’t recommend any smart mattresses at all for users not specifically looking for an adjustable bed.\textsuperscript{57} Sleepers who want smart beds’ key features—the ability to adjust a bed’s firmness, incline, or temperature—can find the same features in an internet-free bed that doesn’t collect, much less share, data that would


\textsuperscript{50} Based on $800+ price tag of the iRobot iRoomba S9+ at the time of publication and the price of most of Consumer Reports’ top picks for canister vacuum cleaners. “Vacuum Cleaner Ratings & Reviews,” Consumer Reports, accessed December 1, 2022, \url{https://www.consumerreports.org/products/vacuum-cleaners-28984/canister-vacuum-28670/view2/}.

\textsuperscript{51} “iRobot Privacy and Data Sharing Common Questions,” iRobot, November 19, 2021, \url{https://homesupport.irobot.com/s/article/964}.

\textsuperscript{52} Based on Sleep Number smart bed. “Legal Privacy Policy,” Sleep Number, October 20, 2022, \url{https://www.sleepnumber.com/pages/legal-privacy-policy}.

\textsuperscript{53} “Legal Privacy Policy,” Sleep Number.

\textsuperscript{54} “Personal Sleep IQ Information,” Sleep Number.

\textsuperscript{55} Sharyl J. Nass et al., \textit{The Value and Importance of Health Information Privacy, Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research} (National Academies Press (US), 2009), \url{https://www.ncbi.nlm.nih.gov/books/NBK9579/}.


\textsuperscript{57} “Mattress Ratings & Reliability,” Consumer Reports, accessed December 1, 2022, \url{https://www.consumerreports.org/products/mattresses-28948/mattress-28705/recommended/}.
be protected by law in any proper medical context. The bottom line: choose a good mattress, not one that collects health information.

Home surveillance companies appear to be lining up to collect and monetize sleep data. Amazon recently introduced a health and sleep tracking alarm clock, just in time for the holiday shopping season. An early reviewer described their disappointment with the product, saying its data quality was questionable, its reports were unhelpful, and a lightbulb on a timer could have woken them up just as well. Again: smart devices have equally effective, non-spying counterparts.

E. Other Home Goods

Vendors present their “smart” offerings as prestige goods, but in truth, internet-connected devices really feature more breakable parts, invasive data collection, and openings for hackers to cause mayhem. Hackers have spammed email accounts from refrigerators, launched cyberattacks from household devices, and stolen email credentials from smart technology. In 2016, a compromised network that included household devices carried out the largest distributed denial of service attack (a type of cyberattack that disrupts internet service) to that point in history. According to IBM, smart tech attacks rose 500% in 2020, and there were over 900 million cyberattacks involving smart devices in 2021. These incidents are expected to double by 2025.

Many low-tech devices clearly outperform their spying and unsecured counterparts. A classic water filter beats a Wi-Fi-connected version: half the price, none of the breakable electronic circuitry.

---

58 Chen, “Sleep Number Mattresses.”
60 Brian X. Chen, “Amazon Wants to Review Your Sleep.”
62 Thorin Kloskowsi, “Keep Connected Devices Secure.”
64 Eric Limer, “How Hackers Wrecked the Internet.”
Common drip coffee makers will brew a cup on schedule—just like their “smart” counterparts.\(^{67}\) One connoisseur’s guide to coffee makers extolls the virtues of drip coffee makers, French presses, pour-over cones, espresso machines…everything, it seems, except smart coffee makers, which receive no mention.\(^{68}\) It seems to go without saying, but refrigerators don’t need internet connections or voice assistants: they will keep groceries fresh just the same, without the bother of technical difficulties or the cost of extra repairs.\(^{69}\) One reviewer recommended a washing machine despite its smartness—the machine worked well without features knocked out by its spotty internet connection.\(^{70}\) Ratings for household gadgets, like countertop ovens,\(^{71}\) suggest that an internet connection adds “smart” branding and nothing else. Dumb outperforms “smart” any day.

### F. Smart Security Cameras

S.T.O.P. condemns the widespread, growing use of residential surveillance cameras, which are frequently coopted by police to harass Black and Latinx residents.\(^{72}\) We don’t have a lower-tech recommendation for these surveillance devices, but internet-connected surveillance cameras and video doorbells are the worst of the lot, making police use of civilians’ camera footage especially quick and easy.

Home security cameras generate an unprecedented amount of information of clear interest to law enforcement. A doorbell camera pointed at a household’s door generates a record of every visitor to the home. An indoor security camera can generate the same record, plus a record of what household members or visitors talked about—even when guests have not consented to be recorded. As is the case with voice assistant data, company employees have accessed these recordings without

---


\(^{70}\) Thorin Kloskowski, “Keep Connected Devices Secure.”


permission, and some companies routinely share recordings with law enforcement. As of 2021, it is estimated that one in ten U.S. police departments have partnerships with Amazon-owned Ring, a group that will soon include the New York City Police Department. Ring’s Neighbors app, which enables users to supply Ring footage to law enforcement, perpetuates unsubstantiated fears of neighborhood crime, at the expense—and safety—of innocent BIPOC people.

Despite advertising and police claims to the contrary, video doorbells open households and BIPOC community members to new forms of harassment. In 2020, 30 people sued Ring after hackers gained control of their doorbells and “screamed obscenities, demanded ransoms, and threatened murder and sexual assault.” In another case, the Los Angeles Police Department asked doorbell camera owners for their footage to identify Black Lives Matter protesters. One news outlet surveyed photos of individuals reported as “suspicious” by video doorbell users and found that most of those individuals were Black. Doorbell footage even invites dangerous vigilantism. In 2022, when a good Samaritan tried to bring a misdelivered box to the right house, the home’s occupant received an alert from his video doorbell, assumed there was an intruder, and grabbed his gun. He opened fire on a bystander sitting in a nearby car, blowing seven shots through the child seat. Everyone survived, by luck, but the danger invited by residential surveillance cameras can’t be overstated.

---

83 Evan Greer, “The Dark Side.”
G. VPN Routers: Keeping Hackers Out of Smart Homes

For many households, the horse has already left the barn: an estimated 25% of Americans bought “smart home” devices like smart speakers in recent years. For these households, a virtual private network (VPN)-enabled router could be a worthwhile gift. VPNs do two things to make internet activity more private and secure from hackers. First, they mask users’ locations by rerouting internet traffic through a dispersed network. Second, VPNs encrypt internet traffic. Together, these processes make it harder for hackers and other third parties to intercept personal information as it travels across the web.

Many so-called “smart” household devices can’t shield themselves from hackers—but you can defend them from attack by connecting to the internet through a VPN-protected Wi-Fi router. The same VPN router that connects a person’s computer or phone to the internet can protect every device reaching the internet through that router. Protecting your voice assistant-guided visit to BlackLivesMatter.com, the Gay and Lesbian Alliance Against Defamation’s website, or your local temple’s Zoom session can be as simple as using a VPN-secured router.

Using a VPN will mitigate hacking-related risks, but it’s not a complete privacy shield. Some VPNs compile personal and account information and can share them with third parties like government agencies. VPNs also won’t prevent the intended recipient of data from collecting or retransmitting it. Even with a VPN, Roomba can map a home; Sleep Number can compile health information; smart speakers can record audio and information about device use; utility meters can track daily

---

87 Michael Grothaus, “How to Protect Your Privacy.”
88 Michael Grothaus, “How to Protect Your Privacy.”
90 Katie Rees, “Can Governments See Who’s Using a VPN?,” Make Use Of, April 21, 2022, https://www.makeuseof.com/can-governments-see-vpn-use/.
schedules. That’s why we don’t recommend buying or gifting smart devices, even with VPN protection.92

III. LEGAL LIMITS ON HOUSEHOLD SURVEILLANCE

U.S. law allows police and prosecutors to access smart device users’ personal data, often with much less than a warrant.

A. Locally Stored Data is Constitutionally Protected

Under the Fourth Amendment, police and prosecutors usually need a warrant to search a home or a device inside a home.93 Storing data locally within one’s home rather than on company servers is the safest option for home devices—but that excludes smart products, which by definition broadcast their data over the internet.

B. The Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA) protects some information that home devices transmit to another person or company. This federal law regulates government access to electronic communications within the U.S.94 ECPA is divided into three sections, the Wiretap Act, Pen Register Act, and Stored Communications Act.95 Legislators did not draft any of these sections with smart home devices in mind, but they are flexible enough to apply to them in many circumstances, as described below.

The Wiretap Act protects the privacy of real-time communications, like calls placed using a smart speaker.96 The law requires law enforcement to demonstrate a reasonable need and probable cause before listening to conversations as they take place.97 The Pen Register Act guards communications’ secondary data like telephone numbers, IP addresses, or website URLs.98 Instead of requiring

93 U.S. Const. amend. IV.
98 18 U.S.C § 2312.
probable cause, this Act lets government agencies compel secondary information by meeting a low standard of showing that the data is relevant to an investigation.99 Problematically, ECPA allows companies to voluntarily share some information, like the data points protected by the Pen Register Act, with non-government third parties.100 But this information is all that’s needed to identify a person’s social connections, their interests, and location.101 Third parties receiving this data can (and in some cases, do) resell it to government agencies and others.102

As the name suggests, the Stored Communications Act applies to stored communications, like an email sent from a smart speaker and uploaded to cloud storage.103 Under the Act, government agencies only need to meet a low bar to (1) compel electronic communications services to produce communications stored over 180 days or (2) compel remote storage providers to produce communications with notice to the user.104 Courts have made it a bit harder for government agencies to get this data. The Sixth Circuit Court of Appeals requires that government agencies obtain a warrant before compelling emails, and law enforcement agencies typically comply with this rule.105 Of course, devices can store data other than emails, like the pattern of usage data collected by smart meters or speakers, and this is not clearly protected by the Sixth Circuit’s warrant requirement. Courts should extend full warrant protection to this data, but as it stands, they do not grant it the same protection as emails.106

---

99 18 U.S.C § 2312 (a)-(b).
102 Bradford-Franklin, “Legal Loopholes.”
103 18 U.S.C § 2703.
104 18 U.S.C § 2703.
106 The Seventh Circuit has ruled the Fourth Amendment applies to smart meters. However, it also ruled that a local government utility did not need a warrant to view smart meter data. Jamie Williams, “Win! Landmark Seventh Circuit Decision Says Fourth Amendment Applies to Smart Meter Data,” Electronic Frontier Foundation, August 21, 2018, https://www.eff.org/deeplinks/2018/08/win-landmark-seventh-circuit-decision-says-fourth-amendment-applies-smart-meter.
C. State Laws

States including Illinois, California, Texas, and Michigan have gone beyond ECPA to require government agencies to obtain a warrant in more situations than required by federal statute.\(^{107}\) Illinois’ recently enacted Protecting Household Privacy Act (PHPA) prohibits state and local law enforcement agencies from compelling stored household data without a warrant.\(^{108}\) PHPA applies to “any information or input provided by a person to a household electronic device,”\(^{109}\) but excludes personal computers, phones, tablets, and internet infrastructure like routers.\(^{110}\) That means Illinois police cannot access any information provided to household cameras, smart speakers, appliances, and other home goods without a warrant (with few exceptions\(^{111}\)) unless a user consents.\(^{112}\) It is not clear how courts will treat the data that users input into a household device but store on an excluded item, like a smartphone, but the law’s language extending its application to “any information or input” appears broad enough to apply to data regardless of input method or storage location.\(^{113}\) That means the PHPA protects a smart bed or any home device controlled through a phone or computer and any smart home device connected to the internet through a router, even if the device stores data on remote servers.

Almost every state has also considered comprehensive consumer privacy legislation that would give home surveillance device users greater control of their data, but only a handful have adopted it.\(^{114}\) Comprehensive statutes typically give consumers the right to opt out of data-sharing and the right to delete information.\(^{115}\) These rights do not apply against government agencies and do not prevent companies from sharing information in response to a law enforcement inquiry or legal

---


\(^{108}\) 5 I.C.L.S. 855/10, /45.

\(^{109}\) 5 I.C.L.S. 855/5.

\(^{110}\) 5 I.C.L.S. 855/5.

\(^{111}\) 5 I.C.L.S. 855/15.

\(^{112}\) 5 I.C.L.S. 855/5.

\(^{113}\) 5 I.C.L.S. 855/5.


\(^{115}\) IAPP, U.S. State Privacy Legislation Tracker.
process. Additionally, it is burdensome for households to exercise their rights under these laws. Despite these considerations, determined households can use these laws to delete their data and reduce the amount of personal information they make available to law enforcement agencies and private parties.

**D. The Federal Trade Commission (“FTC”)**

The Federal Trade Commission regulates home surveillance companies that engage in unfair and deceptive business practices. A company might draw FTC enforcement if it does not tell consumers that it will collect their data or if it contradicts its internal privacy policy. The FTC also recently announced that it is considering issuing new regulations that would act similarly to comprehensive privacy legislation. If it does, users of household surveillance technology across the U.S. may be given the right to opt out and delete data.

**IV. CONCLUSION**

Technology has made home life easier than ever, but don’t fall for the “smart” line. This holiday season, keep your loved ones’ rights, security, and privacy in mind while you’re shopping for them. Instead of buying “smart” tech, imagine how your friends and family will use their gifts. Will they listen to music? Would they like to time their lights or schedule their morning coffee? There’s a perfect gift out there that fits the bill without compromising rights, safety, and privacy. This season, shop smart by choosing “dumb.”

---

116 IAPP, U.S. State Privacy Legislation Tracker.