Arizona Law Journal of Emerging Technologies

Volume 5 *Article 4*

02-2022

CONSUMER IN A COALMINE: LAX SECURITY OF IOT VIDEO DEVICES PUTS CORPORATIONS BEFORE USERS

Georgia Johnson
Loyola Law School, Los Angeles

2021-2022 **https://azlawjet.com** **Vol. 5, Art. 4**

Arizona Law Journal of Emerging Technologies

CONSUMER IN A COALMINE: LAX SECURITY OF IOT VIDEO DEVICES PUTS CORPORATIONS BEFORE USERS

Georgia Johnson, JD Candidate

Table of Contents

CONSUMER IN A COALMINE: LAX SECURITY OF IOT VIDEO DEVICES PUTS CORPORATIONS BEFORE USERS

Georgia Johnson[*]

I. Introduction

The belief that a man's home is his castle is one of the oldest principles of both American law and society.[1] Rooted in 17th century England, this theory protects a man's right to do as he pleases in his home and regards the home as a sacred place away from prying eyes. For centuries, the home has been subject to the utmost ethical, legal, and societal protections that predate the U.S. Constitution.[2] Today, such regard for privacy is reflected in the Fourth Amendment.[3] Yet, because of rapid advancements in technology, a man's "castle" is increasingly vulnerable to unwanted intrusions.[4]

Today, hackers around the world attempt to penetrate man's proverbial castle, and many of them succeed. The rise of in-home, internet-connected devices presents a unique opportunity for hackers to view the inner workings of the home from anywhere in the world.[5] The general lack of security around such technologies has jeopardized the sanctity of the home—particularly with video camera devices that literally "see" into the home itself. There is a massive underground cybermarket (particularly in China) for hacked

[*] Georgia Johnson is a candidate for Juris Doctor at Loyola Law School, Los Angeles. The author would like to thank Cole Varner for his insight and input throughout the many stages of this piece. She is also grateful for Professor John Nockleby of Loyola Law School, Los Angeles for his guidance. Lastly, the author would also like to mention the staff and editorial board of the Arizona Law Journal of Emerging Technologies for their meticulous edits and invaluable input.

[1] Jonathan L. Hafetz, *"A Man's Home is His Castle?": Reflections on the Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries*, 8 WM. & MARY J. WOMEN & L. 175, 175-76 (2002).

[2] *Entick v. Carrington* (1765), 95 Eng. Rep. 807, 817; *Collins v. Virginia*, 138 S. Ct. 1663, 1670 (2018); U.S. CONST. amend. IV, § 2.

[3] *See generally United States v. Jones*, 565 U.S. 460 (2012) and *Kyllo v. United States*, 533 U.S. 27 (2001). The Fourth Amendment considers a man's home as a "first among equals" and protects his right to retreat into the private space of his home. The U.S. Supreme Court has recognized non-physical government monitoring, namely infrared surveillance and GPS tracking, as invasions of personal privacy. *Florida v. Jardines*, 569 U.S. 1, 6 (2013).

[4] Such access has a special impact when compared to the scope of Fourth Amendment protections, particularly since many IoT companies cooperate with law enforcement agencies and turn over home video footage without the permission of the user. For example, Ring has partnered with hundreds of police departments under a "neighborhood watch" system where officials can request footage unless the user specifies otherwise, though officers do not receive live footage access. Drew Harwell, *Doorbell-camera Firm Ring has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019, 3:53 PM), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach.

[5] *See infra* part III.A, at 7-8 (defining IoT and its impact on in-home video surveillance).

home video footage.[6] As a result, hackers have targeted and infiltrated video streams around the world and even gone so far as to use the compromised devices to harass families for their own entertainment.[7]

Many of the home video surveillance cameras of today are reliant on the "Internet of Things" (IoT).[8] The IoT is a system of interconnected devices that are linked to the cloud.[9] Examples of well-known IoT devices of today include voice assistants like the Amazon Alexa, robot vacuums, and smart thermostats.[10] As the technology of IoT video devices has rapidly developed, sufficient security measures have lagged. Security standards for such devices have gone unregulated and unchecked, since there is no government oversight to mandate foundational security measures for consumer devices.[11] The intersection of high demand for these videos and unregulated security measures is a perfect storm, and Ring is the best example. Ring is facing a class action lawsuit for allegedly failing to properly protect its users' information when hackers compromised home video streams and threatened families across the U.S.[12] Ring has responded to such incidents by shifting the blame to its consumers while quietly implementing increased security measures.[13]

Ring's example sets the precedent that the consumers are a canary in a coal mine—if there are security breaches, the consumer will ultimately suffer the consequences. This is unacceptable, particularly for sensitive devices like home video systems. This paper discusses several recent incidents of video device hacking and the harms that result from the security vulnerabilities of such devices. It begins by examining the origins of in-home video surveillance, the home-video surveillance device options today, and the advantages of modern home video devices. It then turns to the hackability and harms that may result when device security systems are easily breached and what can be done to secure these particularly sensitive devices to prevent future harms.

II. A Brief History of Video Surveillance Technology

Because of their high resolution, today's video cameras are nearly all Internet Protocol ("IP") cameras that send and receive images via the internet.[14] But video surveillance and security systems do not necessarily require an internet connection to function.[15] Indeed,

[6] Mandy Zuo, *Hackers are stealing videos from private security cameras and selling them as home video tapes*, SOUTH CHINA MORNING POST (March 31, 2021), https://www.scmp.com/news/people-culture/article/3127659/hackers-are-stealing-videos-private-security-cameras-and.

[7] *See infra* Part IV.A.

[8] Peter Chiang, *How the Internet of Things is reshaping video surveillance,* SECURITY EMAGAZINE (Sept. 28, 2021), https://www.securitymagazine.com/articles/96164-how-the-internet-of-things-is-reshaping-video-surveillance.

[9] Erika Rawes, *What exactly is the Internet of Things?*, DIGITALTRENDS (Jan. 28, 2020), https://www.digitaltrends.com/home/what-is-the-internet-of-things.

[10] *Id.*

[11] Charlotte A. Tschider, *Regulating the Internet of Things; Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age,* 96 DENV. U. L. REV. 87, 142 (2018).

[12] *See Orange v. Ring LLC,* No. 2:19-cv-10899 (C.D. Cal. Dec. 26, 2019).

[13] *See infra* Part IV.C.

[14] *See generally* U.S. Dep't of Homeland Sec., *CCTV Technology Handbook* (July 2013), https://www.dhs.gov/sites/default/files/publications/CCTV-Tech-HBK_0713-508.pdf (explaining IP camera connectivity, remote access, and installation).

[15] *Id.* at 5.

the first video surveillance system was invented during World War II to observe the launch of long-range ballistic missiles—long before the internet was around.[16]

a. The Rise of CCTV Analog Video Cameras

Shortly after World War II, CCTV became available on the public market. Some of the first video surveillance technology publicly available was closed-circuit television ("CCTV")—low-resolution, analog devices that operated on a limited network and recorded footage onto tapes.[17] The first CCTV cameras did not use the internet and instead relied on either a direct hardwire from camera to computer or a link between the camera and phone provider (initially landlines, though some CCTVs now operate on mobile networks).[18] CCTV cameras were initially used to broadcast professional sports, but once cable eclipsed CCTV sports broadcasts, CCTV became almost exclusively used for used for surveillance in high security areas, like banks, police departments, and prisons.[19]

The first CCTV home security system was patented in 1966, but at the time, CCTV systems were neither affordable nor practical for the average home owner.[20] Video surveillance technology relied on local VCR tape storage which could only store about 8 hours of video at a time.[21] This resulted in stockpiles of such tapes that the average person did not have the space to collect.[22] Further, analog CCTV cameras had poor resolution and low frame rates, making much of the image quality blurry for the high cost of installation and record keeping.[23] Eventually, Digital Video Recording (DVR) made it possible to store video recordings digitally. Still, such systems were often prohibitively expensive to maintain such that it was unrealistic for the average family to install such systems—they were mostly used for law enforcement purposes.[24] It was not until the invention of the IP camera in the 1990s that home video surveillance became more widely available and financially accessible.[25]

[16] *A Brief History of The Security System*, CONDOR TECH (Jan. 12, 2017), https://www.condortech.com/security-camera-systems-washington-dc/a-brief-history-of-the-security-camera-system/#:~:text=The%20first%20video%20surveillance%20system,an%20eye%20on%20their%20business.

[17] Michael Kwet, *The Rise of Smart Camera Networks, and Why We Should Ban Them*, THE INTERCEPT (Jan. 27, 2020 9:53 AM), https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks.

[18] *See* U.S. Dep't of Homeland Sec., *supra* note 14.

[19] *Id.*

[20] U.S. Patent No. 3,482,037 (issued Dec. 2, 1969).

[21] *Evolution of Video Surveillance Systems*, NCAVF (Apr. 14, 2016), https://ncavf.com/blog/evolution-of-video-surveillance-systems/

[22] *Id;* Daniel Bortz, *Home-security systems aren't just for the wealthy. Here's how to choose one.,* WASH. POST (Jul. 24, 2018, 4:00 AM), https://www.washingtonpost.com/lifestyle/home/home-security-systems-arent-just-for-the-wealthy-heres-how-to-choose-one/2018/07/23/54985bea-8a8f-11e8-85ae-511bc1146b0b_story.html.

[23] Sarah Ludwig, *Pros and Cons for IP vs Analog Video Surveillance*, SECURITY EMAGAZINE (Apr. 12, 2018), https://www.securitymagazine.com/articles/88854-pros-and-cons-for-ip-vs-analog-video-surveillance.

[24] *See Evolution of Video Surveillance Systems*, *supra* note 21.

[25] *Id.*

b. The Invention of Internet-Reliant Video Devices

In 1996, the palm-sized Axis Neteye 200 internet video camera became the publicly-available camera that was part of the IoT.[26] The camera functioned as a time-lapse recorder that captured 1 frame every 17 seconds and cost $1,299.[27] In 2002, the XCam2 mini wireless camera debuted on the market as one of the first affordable home surveillance cameras, costing around $80 at the time.[28] Manufactured by X10 Wireless Technology, the XCam2 sent a wireless video signal to its nearby base station, where it could be viewed on a computer or television set.[29] Because of its affordability, the Xcam2 was attractive to families who wanted a "nanny cam" device that allowed them to check on children and pets while they were away from home.[30] Yet, the security protocols for these nanny cams were virtually non-existent; the signal could be easily intercepted with a cheap electronic receiver from a quarter-mile away.[31] Indeed, a 2002 New York Times article reported that two security experts drove around a New Jersey suburb intercepting video signals from wireless nanny cams around the neighborhood.[32] At the time, wiretapping laws applied to intercepting sound, not video, so what they were doing was legal.[33]

Today, there is more legal liability for such snoopers; video surveillance technologies now fall under federal and state wiretapping laws.[34] Yet even in 2000, security risk managers knew that first version products on the consumer market "rarely include strong security," and that it is often better for manufacturers to design and implement security features *before* products are launched, since adding them after the fact is more difficult.[35] Unfortunately, many companies today launch video devices that are vulnerable to security breaches and are making the same mistakes that X10 did more than 20 years ago.

III. <u>Modern Home Monitoring: Ring & Other IoT Devices</u>

The demand for home security is nothing new. Companies like ADT, Comcast, and Honeywell have offered home security services for decades, and the first security camera was invented over 50 years ago.[36] The main difference is that, today, homes are increasingly inhabited by more smart things than smart people. The rise of the IoT promises affordable, convenient, and integrated devices; all people must do is click "buy" and connect the device to the internet—no wires or service plans needed.

[26] *Axis NetEye 200 (1996)*, DIGITALKAMERA MUSEUM, https://www.digitalkameramuseum.de/en/cameras/item/axis-neteye-200 (last visited Mar. 5, 2021).
[27] *Id.*
[28] John Schwartz, *Nanny-Cam May Leave a Home Exposed*, N.Y. Times (Apr. 14, 2002), https://www.nytimes.com/2002/04/14/business/nanny-cam-may-leave-a-home-exposed.html.
[29] *Id.*
[30] *See Id.*
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] Grant Clauser, *Security Cameras, Ethics, and the Law*, N.Y TIMES (Sept. 23, 2016), https://www.nytimes.com/wirecutter/blog/security-cameras-ethics-and-the-law.
[35] Schwartz, *supra* note 28.
[36] *See supra* Part II.

a. IoT & Today's Video Security Technology

The IoT refers to the "dynamic global network infrastructure" of computing devices embedded in everyday objects enabling them to send and receive data.[37] The IoT is an all-encompassing category made up of billions of interconnected devices such as smart thermostats, shopping agents, smart locks, water filters, and more that each promise integrated, functional connectivity and thus, ease of use.[38] It would be unreasonable to outline the billions of systems incorporated in the IoT—they are too vast and complex.[39] Instead, this Article will focus on a considerably smaller category of IoT: smart video surveillance systems.

Many have come to associate the IoT with Amazon's Alexa and Google Home products—virtual home assistants that utilize artificial intelligence technology and integrate collections of IoT products into the home to create a "smart" home.[40] This smart home can play music, make phone calls, turn on a coffee machine, and lock the front door.[41] In the interest of home security, millions have invested in a smart security camera that conveniently pairs with other IoT devices.[42] Dozens of device options are available on the market, from the most popular Big Tech cameras like Google Nest and Amazon Ring to lesser-known companies like Arlo, Blink, Wyze, SimpliCam, Lorex, Swamm, Eufy and Zmodo. Each device promises seamless integration, affordability, and convenience.

To date, millions of Americans have purchased an IoT video device, be it Ring, Nest, or another type of IoT video surveillance system.[43] The sales for Amazon's Ring doorbell camera nearly tripled in December 2019 alone despite unfavorable news of compromised Ring devices.[44] The recent surge in popularity of such devices is not necessarily in response to an increase in residential crime; the number of residential burglaries in major U.S. cities fell 24% during the first year of the COVID-19 pandemic compared to a year prior.[45] Indeed, people are on average spending more time at home than ever, so why

[37] *Internet of Things*, LEXICO, https://www.lexico.com/en/definition/internet_of_things (last visited Apr. 9, 2021); European Research Cluster on the Internet of Things, *Internet of Things*, IERC (2014), www.internet-of-things-research.eu/about_iot.htm.

[38] Tschider, *supra* note 11, at 91; Stacy-Ann Elvy, *Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond*, 44 HOFSTRA L. REV. 839, 839-41 (2015-2016).

[39] Guido Noto La Diega & Ian Walden, *Contracting for the 'Internet of Things': Looking into the Nest*, QUEEN MARY UNIV. OF LONDON SCHOOL OF L. RESEARCH PAPER NO. 219/2016, 5-6 (2016).

[40] Donna L. Hoffman & Thomas P. Novak, *Emergent Experience and the Connected Consumer in the Smart Home Assemblage and the Internet of Things*, GEORGE WASHINGTON UNIV. SCHOOL OF BUS., Aug. 20, 2015, at 1, 7-8.

[41] *Id.* at 6.

[42] *Id.*

[43] Letter from Brian Huseman, Vice President of Public Policy, Amazon, to U.S. Senators (Jan. 6, 2020) (on file with author).

[44] Rani Molla, *Amazon Ring sales Nearly Tripled in December despite hacks*, VOX NEWS (Jan. 21, 2020), https://www.vox.com/recode/2020/1/21/21070402/amazon-ring-sales-jumpshot-data; *see infra* part IV.A, at 13.

[45] Richard Rosenfeld & Ernesto Lopez, *Pandemic, Social Unrest, and Crime in U.S. Cities*, NATIONAL COMMISSION ON COVID-19 AND CRIMINAL JUSTICE 3 (Nov. 2020), https://build.neoninspire.com/counciloncj/wp-content/uploads/sites/96/2021/07/Crime-in-US-Cities-October-Update.pdf; David S. Abrams, *Opinion: Most crime rates fell sharply during COVID lockdowns and stayed down*, MARKET WATCH (Mar. 30, 2021, 4:18 PM), https://www.marketwatch.com/story/most-crime-rates-fell-sharply-during-covid-lockdowns-and-stayed-down-11617135487.

worry about home security now? The answer is likely based on both cost and convenience.

b. Consumer Advantages of IoT Video Devices

In 2020, the home security business was worth an estimated $53.6 billion and, by 2025, is expected to reach $78.9 billion.[46] In the past, ADT and Honeywell charged hundreds of dollars for professional keypad-at-the-door security packages, which include equipment, installation, and monthly monitoring fees; the bare-bones ADT package starts at $599 plus $50/month monitoring.[47] While most do-it-yourself ("DIY") home video systems like Arlo, Ring, Nest, and Blink require an internet connection to function, ADT currently offers security packages that rely on a landline phone connection; yet many home surveillance cameras do not require an internet connection.[48] Since they are not connected to the internet, such cameras are comparably far less susceptible to hacking.[49] Unfortunately, these systems are more complex and invasive to set up because they require tapping into a mobile or landline phone connection.[50] Further, because these systems are not connected to the internet, users cannot access them remotely; in other words, users cannot access live footage from their cameras when they are not in their homes.[51]

But the business' most prominent and longest running players, like ADT, Xfinity, and Honeywell, may be soon taking a back seat to the DIY internet protocol camera systems, largely funded by Big Tech, that promise convenience and security without the hefty price tag. While ADT has dipped a toe into the DIY security systems in the past, its experimentation was ultimately eclipsed by its partnership with Google, which invested $450 million and took a 6.6% stake in ADT in 2020.[52] Google also purchased Nest in 2014 for over $3 billion, and Amazon purchased Ring in 2018 for more than $1 billion—one of Amazon's largest acquisitions ever, second only to its acquisition of Whole Foods.[53] Such acquisitions signal that Big Tech is very much the future of home security.

[46] *Home Security Systems Market by Home Type, Security, Systems, Services, Region-Global Forecast 2025*, REPORTLINKER (July 2020), https://www.reportlinker.com/p05495954/Home-Security-System-Market-by-Home-Type-System-Type-Offering-And-Geography-Global-Forecast-to.html?utm_source=GNW.

[47] *How Much Will a Home Security System Cost per Month?*, ADT, https://www.adt.com/resources/home-security-cost-per-month (last visited March 5, 2021).

[48] *Security Services & Features FAQs*, ADT, https://www.adt.com/help/faq/security-services-features/does-adt-system-need-landline (last visited March 6, 2021).

[49] Krista Bruton, *Security Cameras Without WiFi: What Are Your Options?*, BRINKS HOME (Aug. 19, 2020)**,** https://brinkshome.com/smartcenter/security-cameras-without-wifi-what-are-your-options.

[50] *Id.*

[51] *CCTV vs. IP Cameras: Which is best suited for your business?*, TAYLORED BLOG, https://www.taylored.com/blog/cctv-vs-ip-cameras-which-is-best-suited-for-your-business (last visited April 5, 2021).

[52] Sara Morrison, *Contracts, hacks, and Google: What to consider before you get a home security system,* VOX (Aug. 24, 2020), https://www.vox.com/recode/2020/8/24/21354628/home-security-adt-google-ring.

[53] Theodore Schleifer & Jason Del Rey, *Amazon is making its second-biggest acquisition ever – the doorbell Company Ring*, VOX (Feb. 27, 2018), vox.com/2018/2/27/17059768/amazon-ring-acquisition-doorbell; Aliza Vigderman, *Nest Secure vs Ring Alarm*, SECURITY.ORG (Nov. 25, 2020), https://www.security.org/home-security-systems/nest-secure-vs-ring-alarm/; Ramzeen A V, *Top Companies Acquired by Amazon*, TECHWYSE (May 5, 2020), https://www.techwyse.com/blog/infographics/amazon-acquisitions.

Amazon and Google's DIY home surveillance devices promise more affordability and accessibility than security packages touted by longstanding private security companies like ADT and without the long-term contract commitment. For example, Amazon's most basic Ring camera starts at $99.99 with a monthly service fee of $3 to $10.[54] Rather than the system alerting a private security company first, DIY IoT home security systems often alert the user directly when the system detects suspicious activity.[55] Likewise, many smart video devices link up to other home IoT devices (like Alexa), making IoT home security systems more attractive for those who already own linkable smart home gadgets.[56] The convenience of installation and access of internet-connected cameras like Ring attracts consumers, particularly because the system is cheaper and accessible on demand.[57] Together, these IoT devices are marketed as promoting convenience, security, and comfort; yet, many users report experiences have are anything but comfortable.[58]

IV. Hackability & Harms of Modern Home Video Monitoring

Since releasing its first video device in 2015, Ring has faced a swath of privacy lawsuits alleging device hacking, spying, and harassment.[59] The Ring mobile app shows the address of the user, live footage of the home, and archived footage—all attractive pieces of information for cybercriminals.[60] Once a hacker has broken into a Ring account, they can not only access past and present footage, but they can also digitally "reach" into the home and speak directly through the microphone to the occupants.[61] In some cases, hackers verbally assault and threaten families, and there are growing fears that once one smart device is compromised, other connected devices are also susceptible.[62]

a. Recent Incidents of Video Device Hacking

Perhaps the most unnerving part of in-home video hacking is that users do not necessarily know when infiltrations happen; it is only when the hackers make themselves known that the users know their device has been compromised.[63] The most recent lawsuit against Ring is an amalgamation of several such instances. A widely publicized class action lawsuit, *Orange v. Ring*, alleges that Ring's lax security standards and protocols render the camera systems particularly vulnerable to cyberattacks.[64] The case is currently pending, and the complaint relies on seven instances from across the U.S. in which

[54] *Id.; Protect Plans*, RING, https://ring.com/protect-plans (last visited March 5, 2021).
[55] *CCTV vs. IP Cameras, supra* note 51.
[56] *Id.*
[57] David Priest & Taylor Martin, *Are your home security cameras vulnerable to hacking?*, CNET (Dec. 13, 2021, 3:00 AM), https://www.cnet.com/home/security/stop-home-security-camera-hacking/.
[58] *Six Easy Ways to Get Started With Smart Home*, AMAZON, https://www.amazon.com/b?ie=UTF8&node=17165932011 (last visited Mar. 7, 2021).
[59] Kari Paul, *Dozens Sue Amazon's Ring after camera hack leads to threats and racial slurs*, THE GUARDIAN (Dec. 23, 2020, 4:40 PM), https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats.
[60] Joseph Cox, *We Tested Ring's Security. It's Awful*, VICE (Dec. 17, 2019, 12:41 PM), https://www.vice.com/en/article/epg4xm/amazon-ring-camera-security.
[61] *Id.*
[62] *See infra* Section IV.E.
[63] Neil Vigdor, *Somebody's Watching: Hackers Breach Ring Home Security Cameras*, N.Y. TIMES (Nov. 11, 2020), https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html.
[64] Complaint at 25, *Orange v. Ring LLC*, No. 2:19-cv-10899 (C.D. Cal. Dec. 26, 2019), 2019 WL 7373613 [hereinafter Orange Complaint].

hackers have spied on and harassed families.[65] The incidents include: a hacker proclaimed that he was Santa Claus to an eight-year-old via the microphone on the Ring device in her room; a Texas family was blackmailed by a hacker who claimed the couple's Ring account was terminated and that "they themselves would be terminated" if they didn't pay 50 bitcoin to the hackers; a family was harassed by a hacker who shouted profanities, racial slurs, and threats to the young children.[66]

While Ring may be the most recent target of these attacks in the U.S., it is by no means the only video security company to face them. In 2019, a hacker targeted a Northern California family's Google Nest device and broadcasted a fake emergency warning that three ballistic missiles were headed from North Korea to the U.S.[67] In 2018, a hacker broke into a Texas family's Nest and announced, "I am going to kidnap your baby. I'm in your baby's room."[68] Just months before, a Pennsylvania family was shocked to hear that their daughter had been having conversations with "the man in the video[.]"[69] Around the same time, a Wisconsin woman was shocked to find that a hacker had infiltrated both her Nest security camera and smart thermostat when they set the thermostat at 90 degrees and would not allow her to turn it down.[70] The issue persisted despite the fact that she changed her device password.[71]

Outside of Ring and Google, smaller companies are also susceptible to breaches. Just last month, Verkada, a Silicon Valley security startup worth $1.6 billion that provides private and commercial cloud-based IP security camera services, was targeted by a hacking group.[72] The hackers gained access to more than 150,000 Verkada cameras, including devices in Tesla factories, Equinox gyms, hospitals, jails, schools, police stations, home offices, and Verkada's offices themselves.[73] In one instance, the hackers gained access to footage that showed eight hospital staffers tackling a man and pinning him to a bed.[74]

However, Verkada's breach was particularly unique—it was not exactly malicious. Verkada systems were hacked by an international "hacker collective", which hacked the system to show the susceptibility of such video devices to hacking.[75] They did not seek

[65] *Id.* at 28.
[66] *Id.*
[67] Matthias Gafni, *"5 minutes of sheer terror": Hackers infiltrate East Bay family's Nest surveillance camera, send warning of incoming North Korea missile attack*, THE MERCURY NEWS (Jan. 23, 2019, 4:53 AM), https://www.mercurynews.com/2019/01/21/it-was-five-minutes-of-sheer-terror-hackers-infiltrate-east-bay-familys-nest-surveillance-camera-send-warning-of-incoming-north-korea-missile-attack/#link=%7B%22role%22:%22standard%22,%22href%22:%2.
[68] Elizabeth Chuck & Jason Abbruzzese, *"I'm in your baby's room": Nest cam hacks show risk of internet-connected devices*, NBC NEWS (Dec. 21, 2018, 11:32 AM), https://www.nbcnews.com/tech/tech-news/i-m-your-baby-s-room-nest-cam-hacks-show-n950876.
[69] *Id.*
[70] Steve Karantzoulidis, *Hacker Turns Up Nest Thermostat, Plays Vulgar Music Through Family's Camera*, SECURITY SALES & INTEGRATION (Sept. 25, 2019), https://www.securitysales.com/news/hacker-thermostat-vulgar-music.
[71] *Id.*

[72] William Turton, *Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals*, BLOOMBERG , https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams (Mar. 10, 2021, 9:35 AM).
[73] *Id.*
[74] *Id.*
[75] *Id.*

to steal information or sell the video footage.[76] The hackers were able to get admin login information that was available for free on the dark web. From there the hackers gained access to the "root" code system of the cameras, meaning that they could use the cameras to access other devices across the Verkada network.[77] The hackers said that though one of the reasons for the hack was to show how weak video camera security is; they ultimately said it was spurred by pure curiosity and because "it's also just too much fun not to do it."[78]

These hacking incidents aren't going anywhere soon—demand for hacked video footage is higher than ever and, as seen with Verkada, hacking such systems is a relatively new and exciting frontier for many cyber-hackers given the rise of IoT devices. Indeed, there are dark web podcasts and online forums where hackers discuss how to break into Ring accounts to access the cameras and "terrorize occupants for entertainment."[79] Moreover, the demand for compromised video footage and login information has skyrocketed in the last few years.[80] In China, hackers have stolen tens of thousands of clips from in-home security cameras.[81] The videos are sold on the dark web and are largely priced based on how "exciting" they are; some videos start at just $3 and the most expensive ones are sexually explicit or contain hours of footage.[82] Further, some hackers target medical offices, jails, and other particularly sensitive locations because such security systems are historically more difficult to hack. The video footage then gets resold and circulated, sometimes hundreds of times, around dark web forums and websites—all the while the user may not even know that the device was compromised.[83]

b. How Many Hacks Happen: Credential Stuffing Campaigns

At the heart of many video camera hacking defenses is a cyberattack method known as "credential stuffing."[84] Credential stuffing is a method in which attackers use massive lists of compromised user login credentials to breach a system; it is likely how the Ring breach of 2019 occurred and how the recent Verkada breach occurred.[85] When these data breaches happen, collections of stolen user data become available on the black market, and purchasers use the information for credential stuffing campaigns to gain access to private accounts.[86] The attacks rely on software to run through, or "stuff," such aggregated credential collections often from large-scale corporate data breaches—like the 2017 Equifax data breach that exposed the private information of around 147 million Americans or the Yahoo four-year breach that exposed information of 3 billion email accounts.[87] This works because many people tend to use and reuse the same passwords for

[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] Orange Complaint, *supra* note 64, at 35.
[80] *See* Zuo, *supra* note 6.
[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] *See* Lily Hay Newman, *Hacker Lexicon: What Is Credential Stuffing?*, WIRED (Feb. 27, 2019, 7:00 AM), https://www.wired.com/story/what-is-credential-stuffing.
[85] *Id.*
[86] *Id.*
[87] *Id.*; *In re Equifax Customer Data Sec. Breach Litig.*, No. 1:17-md-2800-TWT, 2020 U.S. Dist. LEXIS 118209, at *145-146 (N.D. Ga. Mar. 17, 2020); Clifford Colby, *Yahoo data breach: How to file for $358 or more as part of claim settlement*, CNET (Oct. 15, 2019, 5:37 AM), https://www.cnet.com/how-to/yahoo-data-breach-how-to-file-for-358-or-more-as-part-of-claim-settlement.

multiple platforms and devices.[88] Ring experienced a leak that exposed the login information of more than 3,000 users.[89] Also, IoT video startup Wyze experienced a data leak that exposed the personal information of 2.4 million users.[90] Wyze never forced, or even recommended, password resets in response to the breach.[91] These breaches are becoming more common place; Facebook is even trying to normalize them.[92]

Yet one of the most unsettling realities of credential stuffing is that, very often, victims of such attacks do not know that their information has been compromised until months or even years later.[93] While most states have laws that mandate companies report data breaches, some laws allow companies to not alert users if there is an ongoing criminal investigation around the breach.[94] Further, most of these state laws do not put a deadline on how long companies have to tell users of breaches, so users do not necessarily know that they should change passwords unless they take initiative to check themselves.[95] Further, even if consumers are alerted that their information has been compromised, the burden often falls on them to manage the aftermath of such an attack.[96]

c. Big Tech's Defenses: *Hoax vs. Hack*

When cybercriminals use data from such credential stuffing campaigns, they can access a plethora of private information and devices including smart home IoT devices like Alexa and Ring.[97] Big tech companies have responded to recent press criticism and litigation by blaming customers for weak passwords and poor internet security. This is nothing new for such companies, which have a pattern of shifting the blame to users when leaks and large-scale breaches occur.[98] Both Google Nest and Ring have

[88] Newman, *supra* note 84.
[89] Caroline Haskins, *A Data Leak Exposed the Personal Information of Over 3,000 Ring Users*, BUZZFEED NEWS (Dec. 19, 2019, 10:58 AM), https://www.buzzfeednews.com/article/carolinehaskins1/data-leak-exposes-personal-data-over-3000-ring-camera-users.
[90] Christopher Budd, *Wyze data leak: Key takeaways from server mistake that exposed information from 2.4M customers*, GEEKWIRE (Dec. 29, 2019, 5:06 PM)**,** https://www.geekwire.com/2019/wyze-data-leak-key-takeaways-server-mistake-exposed-information-2-4m-customers/.
[91] *Id.*
[92] Cox, *supra* note 60.
[93] Hayley Tsukayama, *Why it can take so long for companies to reveal their data breaches*, WASH. POST (Sept. 8, 2017), https://www.washintonpost.com/news/the-switch/wp/2017/09/08/why-it-can-take-so-long-for-companies-to-reveal-their-data-breaches.
[94] CAL. CIV. CODE §§ 1798.82(c), 1798.29(c).
[95] Tsukayama, *supra* note 93; *Cf. ';--have I been pwned?*, https://haveibeenpwned.com (last visited Jan. 13, 2022) (website where individuals may check if their email or phone has been involved in a data breach).
[96] *See* Tsukayama, *supra* note 93; Yuki Noguchi, *After Equifax Hack, Consumers Are On Their Own. Here Are 6 Tips To Protect Your Data*, NPR (Sept. 14, 2017, 4:34 PM), https://www.npr.org/2017/09/14/550949718/after-equifax-data-breach-consumers-are-largely-on-their-own.
[97] Catalin Cimpanu, *An inside look at how credential stuffing operations work*, ZDNET (April 25, 2019), https://www.zdnet.com/article/an-inside-look-at-how-credential-stuffing-operations-work/; Cooper Quintin & Bill Budington, *Ring Throws Customers Under the Bus After Data Breach*, ELECTRONIC FRONTIER FOUNDATION (Dec. 19, 2019), https://www.eff.org/deeplinks/2019/12/ring-throws-customers-under-bus-after-data-breach.
[98] For example, Facebook has blamed its users for the Cambridge Analytica breach as well as, more recently, the data breach that exposed the information of over 500 million users. David Gilbert, *Facebook Says It's Your Fault That Hackers Got Half a Billion User Phone Numbers*, VICE (April 7, 2021, 6:27

responded to such leaks by insisting that any hacks are a result of weak or compromised passwords rather than defective or compromised devices.[99]

In particular, Google has been quick to blame users for weak passwords that were compromised, insisting that such incidents are a "hoax," not a hack in which the software itself was compromised.[100] Verkada did the same, insisting that the internal software was not compromised and attempted to remedy the situation by explaining that the hack only compromised 2% of the consumer population—only 95 people because Verkada is a startup company.[101] Yet, when applying this math to other companies that sell millions of devices, 2% is extremely significant. Like Google, Ring has also blamed breaches on "hoax" credential stuffing campaigns that absolves the company of liability and shifts the onus elsewhere.[102] In response to *Orange,* Ring insisted that there is "no evidence of an unauthorized intrusion" of its systems or network.[103] Further, in response to its 2019 data breach, Ring sent emails to affected users notifying them that it's systems were not breached and that such breaches were a result of weak passwords used in credential stuffing campaigns.[104]

Notably, Ring implemented mandatory two factor authentication ("2FA") and end-to-end encryption in January 2021, which are some of the strongest security measures in the industry.[105] Yet, Ring's response does not seem to be coincidental since it implemented the changes around the same time as the *Orange* lawsuit. If Ring only furthers security measures in the face of litigation and public scrutiny, then users' private data will continue to be at risk. Silicon Valley companies like Ring and Google Nest are setting the standard for other, smaller companies—indeed, Verkada based its authentication protocols on other tech providers, such as Google's Business Apps log-in.[106] Ring is setting a standard that selling insecure products is the norm and remedying vulnerable security after the fact (largely in response to lawsuits and bad press) is what is reasonable and expected in the industry.

AM), https://www.vice.com/en/article/88awzp/facebook-says-its-your-fault-that-hackers-got-half-a-billion-user-phone-numbers.

[99] Edward C. Baig, *Google says Nest security camera terror warning from North Korea was hoax, not a hack*, USA TODAY (Jan. 24, 2019, 4:27 PM), https://www.usatoday.com/story/tech/talkingtech/2019/01/23/nest-cam-warning-hoax-how-protect-yourself-such-hacks/2659890002/.

[100] *Id.*

[101] Filip Kaliszan, *March 31st – Security Update*, VERKADA: LATEST SECURITY UPDATE (Mar. 31, 2021), https://www.verkada.com/security-update (last visited April 9, 2021).

[102] *Ring's Services Have Not Been Compromised – Here's What You Need to Know*, RING: BLOG (Dec. 12, 2019), https://blog.ring.com/2019/12/12/rings-services-have-not-been-compromised-heres-what-you-need-to-know.

[103] *Id.*

[104] *Id.*

[105] Jon Porter, *Ring enables mandatory two-factor authentication and new privacy controls in response to scandals*, THE VERGE (Feb. 18 2020), https://www.theverge.com/2020/2/18/21141948/ring-two-factor-authentication-default-mandatory-data-sharing-third-party-analytics-advertising; Ring PR, *Ring Launches Video End-to-End Encryption*, RING (Jan. 13, 2021), https://assets.ctfassets.net/a3peezndovsu/rgRilrGwRxRgqWW1qtHJi/aeea76ebac6c1adf6259ab16850a2375/Ring_Launches_End-to-End_Encryption.pdf.

[106] *Firmware & App Security: Best Practices & FAQs*, VERKADA, https://info.verkada.com/security/camera-firmware-app (last visited April 9, 2021).

d. The Persisting Security Problems of IoT Video Devices

The plaintiff's in *Orange* allege that Ring not only knew that its security systems were subpar when users information appeared on black market credential stuffing forums but also that Ring was aware of dark web streaming of home Ring invasions for entertainment.[107] The suit alleges that, despite this knowledge, the company continues to blame the users for the hackings.[108] The lawsuit notes that several of its plaintiff's use strong passwords that are different from other passwords, suggesting that the breach was not necessarily a result of credit stuffing campaigns.[109]

Aside from the pending *Orange* lawsuit, others have also alleged that Ring's online log-in security is subpar and prone to hacking.[110] In late 2019, staffers at Motherboard (Vice's online Technology magazine) tested the security of Ring cameras to determine just how secure the systems were.[111] Motherboard reported that, at the time, Ring did not provide a way to see how many people were logged onto Ring accounts at once, and it failed to provide users with a list of login attempts.[112] This makes it difficult to see if a device has been accessed remotely.[113] This allows credit stuffing campaigns to successfully breach accounts en masse. Further, Motherboard reported that while other online services and video devices restrict users who have entered too many incorrect credentials, Ring did not.[114] These are basic security precautions for online companies that host consumer accounts.[115]

e. A Breach's Impact on the Smart Home Assemblage

For many, one of the most frightening parts of these incidents is the potential for hackers to control other IoT devices within the smart home assemblage. The assemblage is a group interconnected of IoT devices—such as video cameras that are connected to smart locks, smart thermostats, and virtual assistants.[116] Currently, security camera systems are the most commonly hacked IoT devices, followed by printers, and smart televisions.[117] Once one device is hacked, other connected devices become vulnerable to invasions too.[118]

In 2019, security researchers found that Ring video footage is sent without encryption, meaning that "people who are on the same network as the doorbell, or the same network as one of its owners, can easily tap into [the device's] feed."[119] Once the feed is compromised, the researchers found that it would not only be easy to replace the imagery

[107] Orange Complaint, *supra* note 64, at 35.
[108] *Id.*
[109] *Id.* at 16.
[110] Cox, *supra* note 60; Haskins, *supra* note 80.
[111] Cox, *supra* note 60.
[112] *Id.*
[113] *Id.*
[114] *Id.*
[115] *Id.*
[116] Priest and Martin, *supra* note 48.
[117] Danny Palmer, *Cybersecurity: These are the Internet of Things devices that are most targeted by hackers*, ZD NET (June 12, 2019, 9:00 AM), https://www.zdnet.com/article/cybersecurity-these-are-the-internet-of-things-devices-that-are-most-targeted-by-hackers.
[118] *Id.*
[119] Cory Dotorow, *Bad security design made it easy to spy on video from Ring doorbells and insert fake video into their feeds*, BOING BOING (Feb. 28, 2019, 8:44 AM), https://boingboing.net/2019/02/28/recon-mode-active-mode.html.

coming from the doorbell with a fake image, but the hack could spread to other devices absent segmented security measures.[120] Ring has since remedied the bug that allowed hackers to inject application footage.[121] Yet, because Ring initially chose not to encrypt its video packets, the company has had to back-peddle to update its security systems across devices that were already in use.[122]

Much more is at stake when smart home IoT devices are interconnected. According ABI Research, the sales of smart home devices is set to increase by as much as 30% as a result of the Covid-19 outbreak; this is largely attributable to more time spent in the home and the increased desire for the convenience and personalization that the smart home touts.[123] But, as seen in the Verkada breach, a single vulnerability has the potential to compromise the entire system and makes all other connected devices vulnerable. When video cameras have weak security, there is an increased risk that the smart home will, quite literally, turn against its occupants.

Just last year, a research director at ABI Research announced, "A smarter home can be a safer home."[124] To hackers, the smart home is a network of potential access points that, as in Verkada, is an exciting puzzle to crack.[125] As smart home devices continue to become more commonplace, the risk of inter-linked smart device hacking soars when companies roll out new technologies that do not have strong vetted security systems in place. The solutions for consumers are limited beyond implementing strong passwords and two-factor authentication—it should fall on the companies themselves to make sure the product is safe before it becomes publicly available. When companies do not, it is up to Federal Legislature to mandate a certain level of security for these devices.[126]

V. **Leading by Example: What Others Have Done Right**

Last year, the U.S. passed the IoT Cybersecurity Improvement Act § 4(a)(1), which mandates set security standards for only those IoT devices owned or controlled by the Federal Government, but not those that are privately owned.[127] Elsewhere, governments, public agencies, and private companies have taken several steps to further the security of consumer IoT devices. Europe leads in establishing robust, concrete security requirements for IoT manufacturing, followed by a looser California law and effective industry standards set by Google's integrated security measures.

[120] *Id.*

[121] David Bisson, *Ring Doorbell Fixes Flaw that Allowed Attackers to Spy on, Inject Footage*, TRIPWIRE: THE STATE OF SECURITY (Feb. 28, 2019), https://www.tripwire.com/state-of-security/security-data-protection/iot/ring-doorbell-patches-footage-spying-injection-flaw.

[122] *Id.*

[123] *COVID-19 Pandemic Impact: Germ Concern Over Shared Surfaces Will Help Push Near 30% Growth In Smart Home Voice Control*, ABI RESEARCH (April 1, 2020), https://www.prnewswire.co.uk/news-releases/covid-19-pandemic-impact-germ-concern-over-shared-surfaces-will-help-push-near-30-growth-in-smart-home-voice-control-860010057.html; *see* Stacy-Ann Elvy, *Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond*, 44 HOFSTRA L. REV. 839, 845 (2015-2016) (discussing interconnectivity to IoT home devices and data sharing among them).

[124] Alex Riley, *How your smart home devices can be turned against you*, BBC NEWS (May 11, 2020), https://www.bbc.com/future/article/20200511-how-smart-home-devices-are-being-used-for-domestic-abuse.

[125] Hoffman and Novak, *supra* note 31, at 70.

[126] *See infra* part V.C.

[127] Internet of Things Cybersecurity Improvement Act, H.R. 1668, 116th Cong. (2020) (enacted) [hereinafter *IoT Cybersecurity Improvement Act*].

a. The European IoT Standard

Just last year, the European Union introduces a cybersecurity standard for IoT devices. The requirements, established by the European Telecommunications Standards Institute, mandate that companies implement security measures based on industry standards.[128] The order creates baseline requirements for IoT device security in the European Union ("EU"), including the restriction of universal default password use, implementation of mandatory multifactor authentication, utilization of cryptography when transmitting data, and the implementation of systems that make brute force attacks impracticable.[129] Furthermore, the report mandates that companies make it easy for users to delete their data in the interest of transparency and also implement software that isolates compromised devices from other IoT devices.[130]

The European Standard considers, and specifically enumerates, a video stream of a home security camera as sensitive personal data akin to payment and geolocation data.[131] As such, it is information "whose disclosure has a high potential to cause harm to the individual" that must be protected by encryption, not use default passwords, and any IoT network connections between devices must be isolated so that interferences do not spread between devices.[132]

b. On a Local Level: California IoT Law

In the U.S., California was the first state to implement an IoT security law in 2018, followed by Oregon in 2019.[133] In response to the IoT device companies' varied and often insufficient security measures, California's legislature enacted Cal. Civ. Code, § 1798.91.04(a) to force companies to adopt "reasonable" minimum-security features for every IoT device it produces as of January 1, 2020.[134] The statute applies to companies that produce IoT devices that are sold or offered for sale in California specifically.[135]

Maintaining "reasonable" security measures is an intentionally vague phrase that allows for technological advancement over time.[136] The California Department of Justice has issued a report that suggests that foundational "reasonable" measures include compliance with all 20 controls set forth in the Center for Internet Security's (CIS) Critical Security

[128] *Secure by Design: Cyber Security for Consumer Internet of Things: Baseline Requirements*, EUROPEAN TELECOMMS. STANDARDS INST. § 5 (June 2020), https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf [hereinafter *Secure by Design*].

[129] *Id.* at §§ 5.1-5.3.

[130] *Id.* at §§ 5.11-5.12.

[131] *Id.*

[132] *Secure by Design supra* note 128, at §§ 5.6, 5.8-2.

[133] *See* Cal. Civ. Code § 1798.91.04(a) (2018); Or. Rev. Stat. § 646A.813(2) (2019). *See also* Derek Hawkins, *The Cybersecurity 202: California's Internet of Things Cybersecurity Bill Could Lay Groundwork for Federal Action*, WASH. POST (Sept. 17, 2018 4:35 AM), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/17/the-cybersecurity-202-california-s-internet-of-things-cybersecurity-bill-could-lay-groundwork-for-federal-action/5b9e6e331b326b47ec959638.

[134] Cal. Civ. Code § 1798.91.04; *New California IoT Law Requires Security for Connected Devices*, MORRISON FOERSTER (Jan. 24, 2020), https://www.mofo.com/resources/insights/181001-new-california-iot-law.html.

[135] *Id.*

[136] Kamala D. Harris, Cal. Dep't of Justice, *California Data Breach Report* 5 (Feb. 2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

Controls (formerly known as the SANS top 20).[137] This list includes basic, foundational, and organizational CIS controls that should apply to IoT video devices.[138] In particular, the list includes that companies should protect key assets with proper tools and procedures, block access to vulnerable entry points through use of port scanning tools and limiting and controlling remote access, use procedures to protect its data through use of encryption, and control the number of verified users by establishing and securing select administrative privileges.[139]

The California law is much less strict and specific compared to the EU standards. It does not specifically recommend that companies mandate 2FA or specify measures to prevent credential stuffing. Furthermore, it uses broader, more ambiguous language than the EU adopts, which leaves some of the recommendations open to interpretation by corporations. Also, the law does not specifically refer to particularly sensitive IoT devices such as the video and door locks, which means that these devices must have the same level of security as the smart flip flop or the smart toaster despite huge differences in data sensitivity.

c. Leading Measures in the Industry

On the heels of Ring's bad press and privacy litigation, other consumer video technology companies have recognized the need for further security and implemented safeguards to protect users' information.[140] Amazon's other consumer video subsidiary, Blink, has not yet implemented mandatory two-factor authentication despite promising users it was on the way.[141] Unfortunately, companies may continue to implement the bare minimum safeguards until litigation, bad press, or embarrassing hacking incidents force them to do otherwise. While Google has faced its share of lawsuits, the Nest login credentials can be based on pre-existing Google Accounts, which already have built-in security that allow users to view compromised passwords and potential security risks associated with log-in information.[142] Further, Nest began automatically enrolling its users in two-factor authentication in May 2020.[143]

Further, Google looks to the hacking community to test its security for vulnerabilities. In 2010, Google launched its Vulnerability Reward Program that encourages the security research community to find security bugs and report them for a monetary reward.[144] This program encompasses Nest devices.[145] This is not particularly novel, many large

[137] *Id.* at 30.

[138] *The 20 CIS Controls & Resources*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/controls/cis-controls-list (last visited April 3, 2021). The California IoT law does not provide for a private right of action. The Attorney General, a city attorney, county counsel, or a district attorney has the exclusive authority to enforce the law. *Id.*

[139] *Id.*

[140] Thomas Ricker, *Arlo and Blink cameras are boosting security to beat hackers*, THE VERGE (March 10, 2020, 5:34AM), https://www.theverge.com/2020/3/10/21172878/arlo-blink-two-step-verification.

[141] *Id.*

[142142] *Google Nest Help: Don't share your account email and password*, GOOGLE, https://support.google.com/googlenest/answer/9295217?hl=en (last accessed Jan. 24, 2022); *A helpful home is a private home*, GOOGLE, https://safety.google/nest (last accessed Jan. 24, 2022).

[143] *Google Nest Help: Add 2-step verification to your account on the Nest app*, GOOGLE, https://support.google.com/googlenest/answer/9295081 (last accessed Jan. 24, 2022).

[144] *Google Vulnerability Reward Program*, GOOGLE, https://www.google.com/about/appsecurity/reward-program (last visited March 7, 2021).

[145] *Id.*

companies and startups alike implement such programs that cooperate with, and handsomely reward, hackers who breach its systems in good faith. While Amazon does maintain a rewards program, it does not clearly apply to Ring devices.[146] Such programs incentivize some of the best hackers in the world to put security systems to the test often before such vulnerabilities are exploited and should be an industry standard for video device manufacturers. Amazon's introduction of end-to-end encryption eclipses Google's encryption services for the Nest in terms of security, but allegations that Amazon never encrypted video from the start are concerning. Mandatory two-factor authentication should be the industry standard and should have been the default from the start.

VI. FTC & FCC Recommendations

As previously discussed, consumer technology companies are shipping insecure products and only improving them in response to litigation and bad press. The FTC and the FCC have addressed the need for reasonable security measures in IoT devices, but such recommendations are not binding law on corporations that make IoT video devices.

a. FTC Response

The Federal Trade Commission ("FTC") released a "Best Practices" report in 2015 that proposed security recommendations for emerging IoT technologies. The report emphasized the importance of incorporating security measures into devices at the outset "rather than as an afterthought" once products are already launched and in use.[147] It also encouraged companies to minimize the data it collects and retains and inform users of any data breaches.[148] However, the report ultimately concluded that IoT-specific legislation was "premature[.]"[149] If Congress wished to address IoT security via legislation, it stated that such legislation should be broad, flexible, and technologically neutral so as to not apply specifically to IoT technologies.[150] Such protections would reinforce trust in IoT systems while not confining such rapidly developing technology to a narrow set of laws.[151]

This is largely what California Legislature did in passing its IoT law. Today, such recommendations are outdated compared to the rapid advancements of IoT technology. Laws that apply specifically to IoT devices, and even more particularly devices that contain sensitive information, are urgently needed. The FTC's concerns over hindering development cannot take precedent over the security of the devices themselves, and such a recommendation that legislation is not necessary and should be overly broad hinders more than it helps.

[146] *Amazon Vulnerability Research Program*, HACKERONE, https://hackerone.com/amazonvrp?type=team (last visited March 6, 2021).
[147] Fed Trade Comm'n, *supra* note 142, at 38.
[148] *Id.*
[149] *Id.*
[150] *Id.* at 49-50.
[151] *Id* at 51.

b. FCC Response

Just a year after the FTC report was published, the Federal Communications Commission ("FCC") issued its "Order on Internet Privacy" that was based, among other things, on the FTC's Best Practices Report.[152] The FCC order proposed that all IoT devices be incorporated into the Communications Act of 1934 such that there would be a mandated degree of transparency that would make companies alert users of data breaches.[153] It would also mandate that IoT companies comply with reasonable security measures that allow a degree of flexibility for future innovation (similar to regulations in place by the EU).[154] However, the FCC order declined to enumerate specific practices that comply with the order and failed to separate IoT devices by specific category.[155] Rather, it left reasonable practices up to interpretation that are largely based on existing privacy and data laws, best practices, and public-private initiatives.[156] The FCC did this to prevent a "compliance mindset" that is "at odds" with the innovative nature of data security.[157]

However, the order was issued at a politically contentious time. Although it originated during the Obama Administration, a Republication-majority Senate ultimately struck the measure down in late April 2017.[158] If the measure had passed, Amazon would at the very least have been forced to implement similar security measures to its competitors like Google and may not have had as many breaches. Likewise, to remain competitive, other smaller companies like Arlo, Blink, and Wyze would also have to adapt and implement reasonable security measures.

Though the 2016 measure was suspended, in December 2020, the newly elected House of Representatives passed a similar IoT law, the *IoT Cybersecurity Improvement Act*, mandating minimum reasonable security standards for certain devices.[159] However, the law only applies to IoT devices owned or controlled by the federal government.[160] While passing such a law is an important start that will impact IoT security measures, it is useless for consumers if it does not apply to private companies like Ring and Google. Thus, there is still no federal legislative oversight for the consumer IoT industry.[161] Under the new federal law, such accountability for private companies is still nonexistent.

VII. <u>Proposed Mandatory Safeguards: Unfair Practices & Federal Law</u>

The future of IoT video device security relies on action from both the FTC and the FCC. The FTC must hold companies who disclaim responsibility accountable when they deceive consumers. The FCC must review and update a new proposed IoT law that sets a best practices security standard for consumer IoT devices that contain particularly sensitive information.

[152] Report and Order, 16 FCC Rcd. 148, 156 (2016).
[153] *Id.* at 151.
[154] *Id.*
[155] *Id.* at 233.
[156] *Id.*
[157] *Id.* at 131.
[158] S. Res. 34, 115th Cong. (2017).
[159] IoT Cybersecurity Improvement Act of 2020 § 4(a)(1), 134 Stat. 1002.
[160] *Id.*
[161] *Id.*

a. Protecting the Consumer: The Deceptive Defenses of Big Tech

Ring and other companies' historical blame-shifting to consumers for data breaches and device hacking is exactly the type of practice that Section 5 of 15 U.S.C. §45(a) ("The FTC Act") aims to prevent. As previously mentioned, many companies claim that such breaches are a result of a hoax, not a hack. Google has stated that Nest devices were not compromised and there was no security breach in response to allegations of harassment via Nest devices.[162] Likewise, in response to the 2019 data breach and several hacking incidents, Ring stated that there was no "unauthorized intrusion or compromise of Ring's systems or network."[163] This may be technically true, but the average customer does not necessarily know the nuances of such technical jargon, including the difference between a hoax and a hack. Such statements violate the FTC's regulations against deceptive practices and risk injury to consumers.

The FTC Act prohibits unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices.[164] In assessing whether a practice is "deceptive", the FTC looks to whether there was (1) a representation, omission, or practice that is likely to mislead the consumer (false written representations are included), (2) whether it would mislead from the perspective of a consumer acting reasonably in the circumstances, and (3) whether the representation was "material" (in other words, whether the act is likely to affect the consumer's conduct or decision regarding a product or service and leads to likely injury).[165] A "material" misrepresentation or practice is one that is "likely to affect a consumer's choice of or conduct regarding a product; in other words, it is information that is important to consumers."[166]

In a recent complaint, *In the Matter of Zoom Video Communications*, the FTC alleged that Zoom, a video communication company, violated The FTC Act's prohibition on deceptive practices when it advertised that it had a level of encryption that it did not have.[167] The FTC settled with Zoom in January 2021 and mandated that Zoom increase its security measures to include, among many requirements, default randomized passwords, tools to identify credential stuffing attempts, software that limits login attempts, network and database segmentation, quarterly vulnerability scans, and automatic password resets for compromised credentials.[168]

These requirements recognize just how at-risk video technologies can be and go far beyond what is required of IoT video devices that handle arguably more sensitive information than Zoom. Indeed, as previously mentioned, there is no federal law that mandates a set level of IoT device security for consumer devices.[169] Applying the FTC's deceptive practices law to IoT video security hacks, the defenses and statements

[162] *Id.*
[163] *Ring's Services Have Not Been Compromised – Here's What You Need to Know*, *supra* note 93.
[164] 15 U.S.C. § 45(a)(1) (2006).
[165] *Id.*; See FTC Policy Statement on Deception, Oct. 14, 1983, appended to decision in *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984).
[166] FTC Policy Statement on Deception, *supra* note 165 ("[i]f inaccurate or omitted information is material, injury is likely").
[167] Complaint, *In the Matter of Zoom Video Comms., Inc*, No. C-4731, at 4-5 (Nov. 2020).
[168] Decision and Order, *In the Matter of Zoom Video Comms., Inc.*, No. C-4731 (Jan. 2021).
[169] *See supra* text accompanying note 127.

of Ring and Google are deceptive for two reasons: (1) they imply that consumers devices are fine when they might not be, and (2) they suggest that the company has taken all of the security measures necessary and is thus not to blame.

First, the statements by Ring and Google that the systems are secure, even if true, are deceptive. Such statements imply, falsely, that the devices are secure because the internal systems have not been breached.[170] Similar to *In the Matter of Zoom Video Communications*, Ring and Google are misleading users into believing that current security measures are stronger than they actually are. Stating that the breach was not a result of compromised internal security may lead a consumer to not take necessary additional security measures—such as resetting a password or enabling 2FA—because he believes that the systems are already sufficiently secure. The implied distinction between the internal systems and the devices themselves is important yet nebulous to the consumer. Ring and Google use this technical language to their advantage because stating that there was no breach of company security systems is true and shifting the blame to weak passwords takes the blame off the company. However, such misrepresentations lead consumers to believe that their device is not compromised and no further action is needed. This creates material harm to the consumer who assumes that just because the company said its systems were secure, they actually are.

Second, such statements imply that the company's security has not been breached, and there is nothing more that should be (or can be) done by the company. This is misleading since the systems should not have been susceptible to credential stuffing campaigns in the first place. Further, Ring and Google's defense statements could influence consumers to believe that the company did not have the ability to take measures to prevent such attacks. Lastly, such statements promote material harm because they encourage the blame-shift rhetoric that allows many companies (as seen with Google, Ring, and Verkada) to get away with lax security measures and ultimately keep consumers vulnerable to future attacks.

While such misleading statements by Ring and Google are accompanied by suggestions for how to increase security (such as recommending 2FA and unique passwords), such recommendations do not mean much when they follow a statement that incorrectly suggests that the video device itself is not compromised. It is illogical to assume that the consumer would take additional precautions when they read a statement that implies their device is secure. Because these companies' defenses are ultimately deceptive, the FTC must investigate and regulate these deceptive defenses to IoT video breaches. It is unreasonable to expect consumers to understand the difference between a device breach and a company breach, and such responses set a dangerous precedent that leads consumers to incorrectly believe that their sensitive devices are secure when they may not be.

b. The Need for a Federal IoT Law Specific to Sensitive Devices

While the FCC and Congress have recognized the need for further security for IoT devices, it is somewhat ironic, and unhelpful, that they would pass a law that does not apply to consumer devices. The FCC and Congress cannot stand idly by while the most

[170] Baig *supra* note 99; *see supra* text accompanying notes 85-88.

intrusive IoT devices are vulnerable to security breaches. Today's IoT technology has evolved beyond the scope of the FTC report and even the scope of the proposed 2016 measure. There is a very real threat that, as consumers continue to integrate more smart devices into the home, they increase their susceptibility of a cyberattack. The FCC was on the right track—the law must be flexible such that it can adapt to evolving technologies and companies must be required to alert users of security and data breaches. However, even if the FCC order was passed (or a similar measure that applies to private companies is passed in the future), such a law would not go far enough to protect certain IoT devices.

The FCC must re-draft an order that identifies and regulates internet-connected devices (or certain classes of data) that have a heightened risk of causing physical or financial harm should they become compromised (like smart locks and video surveillance systems). These high-risk devices should be held to cybersecurity standards that reflect the sensitive nature of the information stored on them. Such a standard should include industry best practices comparable to systems designed for more traditionally sensitive information like banking and medical data.

Best practices are industry-accepted ways of operating and are context specific.[171] For example, in the video game industry, a player's movement input may not be encrypted in most online games (because it is not sensitive, unique information), but a credit card number when making a purchase is. Both are perfectly acceptable in their respective contexts according to industry "best practices." As previously mentioned, the problem with both the California Law and the proposed FCC law is that they do not classify IoT devices by the sensitivity of the data that the devices contain.[172] What may be considered "best practice" for a smart flip flop or toothbrush, for example, may not be sufficient when applied to a smart lock or home video surveillance device. This is illustrated by the Verkada breach: the systems used in the hospitals were HIPAA compliant but were still easily breached by hackers largely looking for entertainment.

With a measure like this in place, Ring would not have been legally permitted to allow excessive incorrect log-in attempts without any type of notice; it would have had to implement some kind of lockout, anti-brute force mechanism, and alert users of new login locations. Likewise, systems that prevent credit stuffing campaigns mean that Verkada may not have been as easily compromised. Companies must be required to implement a system that warns users of password vulnerabilities. As previously mentioned, Google currently scans the dark web to discover its users' compromised information. While difficult, such processes should become normalized across video security platforms so that users know of any compromised passwords or unauthorized users. Unfortunately, this proposed law ultimately favors companies that can afford to implement such dynamic and robust security measures; smaller companies attempting to compete may inevitably fail. Alternatively, such a measure could spark new tech startups who aim to make costly security measures, like Google's dark web scanning, more accessible to smaller competitors.

[171] *14 Tech Industry 'Best Practices' Your Business Would Be Better Off Avoiding*, FORBES (Nov. 21, 2019), https://www.forbes.com/sites/forbestechcouncil/2019/11/21/14-tech-industry-best-practices-your-business-would-be-better-off-avoiding/?sh=271936a6a036.
[172] *See supra* part VI.B, at 28.

VIII. Conclusion

Affordable home security may be something to celebrate, but it should not mean sacrificing privacy. As home security technology further progresses and becomes financially accessible and convenient, user error should not be a defense when companies fail to take proper security precautions and only remedy vulnerabilities after millions of users have already purchased and relied upon the product. It is up to the FTC to hold IoT video companies accountable for deceptive defenses.

It is also up to the FCC and Congress to implement a law that mandates particularly sensitive IoT devices meet industry best practices of comparable sectors such as the medical and finance industries that deal with comparably sensitive information. The proposed 2016 federal law applies to all IoT devices and leaves devices that transmit the most sensitive information insufficiently protected from unwanted intruders. Until such measures are taken, consumers will ultimately bear the brunt of the harm—there is only so long a canary in a coal mine can sing before serious physical harm ensues.