2018

Smart Baby Monitors: The Modern Nanny or a Home Invader

Sarah Ensenat
SMART BABY MONITORS: THE MODERN NANNY OR A HOME INVADER

Sarah Ensenat +

Washington state parents Sarah and Jay used a smart baby monitor to ensure the safety of their child.1 The couple became concerned when their three-year-old son told them he was talking to a man in his room at night.2 One night Sarah and Jay waited in their son’s room and heard a voice over the smart baby monitor say, “Wake up little boy. Daddy’s looking for you.”3 The couple also observed the camera of the smart baby monitor following them when they were in the room with their son.4 Stories like Sarah and Jay’s are unfortunately common.5 Recently in the news, smart baby monitors reportedly have been hacked in Indiana, Texas, and Minnesota.6

Smart baby monitors exist to help parents protect and watch over their children.7 Parents buy smart baby monitors so they can watch and listen to see if

---

+ J.D. Candidate, May 2018, The Catholic University of America Columbus School of Law; B.A. 2014, Franklin and Marshall College. The Author would like to thank Professor Lisa Martin for her assistance and support in the research and writing of this comment. The Author would also like to thank the hard work and dedication of the associates and editors of the Journal of Law and Technology for their hard work on the preparation of this comment.


2 Id.

3 Id.

4 Id.

5 Id.; see also Rochester Family Finds Their “Nanny Cam” Hacked For The World to See, KTTC (Dec. 31, 2015), http://www.kttc.com/story/28712087/2015/04/03/rochester-family-finds-their-nanny-cam-hacked-for-the-world-to-see (recounting a nation-wide increase in the hacking of smart baby monitors).

6 Kelly, supra note 1; see also Rochester Family Finds Their “Nanny Cam” Hacked For The World to See, supra note 5.

their infant or child is in need of help. Low-tech hackers are able to compromise smart baby monitors and use the footage of infants and children for nefarious purposes. Hackers upload the videos of children to illegal websites or keep the videos for their personal use. Additionally, burglars can use the footage from smart baby monitors to break into homes.

Older baby monitors, or analogue baby monitors, worked over radio waves and were easily hacked. People would listen to private conversations or say threatening and lewd things to children. As technology advanced, companies manufactured smart baby monitors that worked over the Internet and connected to a home’s personal router. Unfortunately, most homeowners’ personal routers are not secured, leaving some smart baby monitors accessible to anyone who can find the camera’s Internet address.

Security of smart baby monitors has always been an issue that has not been properly addressed by federal and state legislatures. Regulations such as the Children’s Online Privacy Protection Act (COPPA) are in place to force technology companies targeting children to prioritize the privacy of the children’s personal information. These regulations do not adequately address security for personal smart products such as smart baby

---

8 Flannigan, supra note 7; see also Ross, supra note 7 (describing how parents can protect their smart baby monitors from hackers).
9 Flannigan, supra note 7; see also Ross, supra note 7 (describing how parents can protect their smart baby monitors from hackers).
10 See Flannigan, supra note 7 (discussing the ease in which smart baby monitors can be hacked and identifying who are the likely hackers of the monitors).
12 Ross, supra note 7.
13 Id.
monitors. COPPA focuses on advertising companies and websites collecting personal information on children and not personal-sized smart objects.

This Comment advocates for stricter federal security legislation for smart baby monitors that requires: 1) stricter login credentials for the smart baby monitor’s network, 2) a department to monitor the security of a product and the potential breaches of privacy, 3) training and continuing education for individuals monitoring the security of products, and 4) the notification of consumers if their privacy has been breached and the provision of free services to remedy the breach. Section I of this Comment introduced the lack of security surrounding smart baby monitors. Section II of this Comment provides a background in the rise of Internet hacking and discusses the history of legislation for personal smart technology products like smart baby monitors. Section II also illustrates a failed attempt to create stricter security legislation and new legislation in New Jersey. Section III of this Comment addresses existing regulations the Federal Trade Commission (FTC) has put in place to promote better security measures for smart baby monitors. This Section then discusses where smart baby monitor security stands today, and addresses the attempt to enforce regulations through a previous FTC suit against a smart baby monitor manufacturer. Section IV of this Comment explores a current case filed by the FTC against a smart baby monitor technology company. This case could change the way smart baby monitor manufacturers and Congress address legislation regulating the security of smart devices. Section V of this Comment continues to evaluate how the FTC has applied existing federal legislation and regulations to smart baby monitor manufacturers. Section VI of this Comment proposes and analyzes suggestions for federal legislation to protect consumers from smart baby monitors. Finally, Section VII of this Comment concludes with a recommendation to Congress to revise COPPA or create new smart baby monitor focused legislation. New legislation focused on improving the security of smart baby monitors must be promulgated to ensure the protection of consumer privacy. Without new legislation, Congress and the FTC cannot ensure that all smart baby monitor manufacturers are applying the best security measures to their smart devices and providing the best support for consumers when hackers invade their privacy.

18 See generally Davenport, supra note 11 at 261 (explaining that “there is more work need to minimize these risks that come along with the convenience of using IoT de-


20 See generally TRENDnet, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 78 Fed. Reg. 55,717 (Sept. 11, 2013) (analyzing the proposed consent order be-
tween the FTC and TRENDnet).
THE RISE OF INTERNET HACKING AND THE HISTORY OF IoT LEGISLATION

Hacking low-security technology can be easily learned.\(^{21}\) Widely available books and classes have made it easier for one to take a course or check out a book at a local library.\(^{22}\) Anyone with vocational training or self-taught training in computer programming can learn to hack Internet devices.\(^{23}\) Personal smart technology items such as phones, smart-watches, and baby monitors are difficult to protect with strong security measures.\(^{24}\) The danger of personal smart devices is the insecurity of the Internet of Things (IoT), which connects smart devices.\(^{25}\) The IoT comprises “everyday devices that are connected to the Internet” that can be “remotely controlled or sensed.”\(^{26}\) The IoT is connected to everything used in daily life and viewed as connected to products essential to every man, woman, and child.\(^{27}\) These everyday devices include smart baby monitors.\(^{28}\)

A. History of IoT Security Measures


\(^{23}\) See generally wikiHow to Become a Hacker, supra note 21.


\(^{25}\) Laura Jehl, Jonathan Meyer & Sonja Carlson, Attack of The Zombie Webcams: DDoS Attacks And The Insecure IoT, LAW 360 (Nov. 14, 2016), https://www.law360.com/articles/861699/attack-of-the-zombie-webcams-ddos-attacks-and-the-insecure-iot; see Rachel Metz, Finding Insecurity in the Internet of Things, 119 MIT TECH. REV., Mar.–Apr. 2016, at 76 (acknowledging that “by 2020, almost 21 billion gadgets will be connected to the Internet” and in effect, such connectivity increases the “potential ways for cyberattackers to wreak havoc.”).

\(^{26}\) Jehl et al., supra note 25 (recognizing that many consumers do not realize IoT devices sold by manufacturers come with default usernames and passwords capable of being reset and warning consumers to be aware of similar devices that do not permit such change).

\(^{27}\) See generally Cate Lawrence, IoT Security Concerns Show an Industry Struggling to Keep Up, READWRITE (Feb. 5, 2016), https://readwrite.com/2016/02/05/iot-security/ (stating the numerous smart products that are used by both adults and children are vulnerable); see also Jehl et al., supra note 25 (illustrating that connected devices includes both obvious connected devices and non-obvious devices including "toasters and lightbulbs").

\(^{28}\) Jehl et al., supra note 25.
The IoT does not have a strong history of security legislation or regulation. Hackers have the ability and incentive to take over these smart devices, including smart baby monitors. Whether their purpose is to create a digital army or steal the personal information including video footage of consumers, hackers can hijack a baby monitor without the parents even knowing. The IoT device security is “ripe for government regulation,” but manufacturers do not have strong incentives to secure their devices until customers demand it. As long as consumers continue to buy their products, manufacturers do not feel a need to increase security.

B. History of Federal Legislation

There are currently some existing federal security laws and regulations to enforce cybersecurity, but they do not address smart baby monitors. They address Internet use and company storage of children’s personal and private information. The laws and regulations especially focus on advertisers targeting children and their collection of the children’s private information.

In 1998 Congress passed COPPA to protect the personal information of children and minors. The purpose of COPPA is to regulate “unfair and deceptive acts and practices in connection with collection and use of personal information from and about children on the internet.” As technology evolved, the Federal Trade Commission attempted to strengthen COPPA by passing an amendment

---

30 Jehl et al., supra note 25.
31 A “digital army” consists of two or more hackers that take control of millions of IoT devices to launch an attack on major service providers. Unsecured devices such as smart baby monitors can be used to infect other devices in the vicinity and easily hijack connected devices. See id.
32 Id.
33 Id.
34 Id.
to COPPA on July 1, 2013. Children’s personal information was further protected by clarifying the definitions of “operator,” “website or online service directed to children,” and “support for internal operations.” The new COPPA requirements also changed requirements for obtaining informed consent of parents, strengthened safe harbor programs, and created strong provisions to keep kids information confidential and secure. Requirements were not set for manufacturers of smart baby monitors and other smart products that work over the Internet; requirements were only set for web operators and the third parties to which they sell the children’s personal information.

C. Failed Federal Amendment

The federal government has tried to pass legislation to improve the regulation of baby monitors. In March of 2012, the House rejected Crowley Amendment

---


41 Operator is defined as “an operator of a child-directed site or service where it allows outside services, like plug-ins or advertising networks, to collect personal information from visitors.” Fair, supra note 40; see also Amended COPPA Rule Comes into Effect, supra note 40.

42 Website or online service directed to children is defined as “a plug-in or ad network when it has actual knowledge that it’s collecting personal information through a child-directed website or service...requiring them to provide notice and get parental consent only for those who identify themselves as under 13.” Fair, supra note 40.

43 Support for internal operations “include[s]...contextual advertising, frequency capping, legal compliance, site analysis, and network communications. Operators may not, without parental consent, use or disclose information collected to contact a specific person, including through behavioral advertising, to amass a profile on that person or for any other purpose.” Id.

44 “Operators must send [notice] directly to parents before collecting personal info from their kids.” The notice must be “to-the-point” and include “what operators have to put in their online privacy policies about their information practices.” Id.

45 Safe harbor programs provide incentives for companies to self-regulate and ensure they are in compliance with COPPA. Id.; see 15 U.S.C. §§ 6501–06 (2012).

46 COPPA created strict provisions, which companies must follow, and they will improve the confidentiality and security of children’s information. Under these provisions, “[o]perators are required to take reasonable steps to ensure that children’s personal information is disclosed only to service providers and third parties capable of maintaining the confidentiality, security, and integrity of such information.” Amended COPPA Rule Comes into Effect, supra note 40.

47 Fair, supra note 40.

48 See S. Res. 110, 114th Cong. (2015) (enacted) (providing that the Senate recommends the United States develop a strategy for the Internet of Things to promote economic
No. 1, which would have affected any regulation relating to baby monitors promulgated by the Federal Communications Commission (“FCC”). The purpose of the FCC is to control “communication laws, regulations, and technological innovation.” The Crowley amendment would have required baby monitors to display a warning label to inform consumers that the video and sound captured by baby monitors and smart baby monitors could be easily viewed or heard by someone outside of the home.

The FCC is not the only government agency that has attempted to compel Congress to reform security requirements. After the Amendment failed, the FTC released a report detailing a privacy framework intended to “articulate best practices for companies that collect and use consumer data.” The attempts have been unsuccessful because of limited public interest and lackluster Congressional oversight. Unless constituents alert Congress to the security problems and media outlets draw Congress’ attention, congressional oversight is a common problem.

D. Enacted State Legislation

Not only has the majority of the proposed legislation not been passed, the proposed legislation does not sufficiently restrict bad behavior or promote the

---

growth and consumer empowerment); 158 CONG. REC. 50, H1624 (daily ed. Mar. 27, 2012) (proposed Floor Amend. 1 to H.R. 3309, 112th Cong.); see generally H. Amend. 1 to Federal Communications Commission Process Reform Act of 2012, H.R. 3309, 112th Cong. (proposed to House, Mar. 27, 2012) (recommending that “the packaging of an analog baby monitor to display a warning label” so that families are informed that video and sounds “may be easily viewed or heard by potential intruders.”).


51 About the FCC, FCC.GOV, http://www.fcc.gov/about/overview (last visited Dec. 19, 2017) (explaining that the FCC is an independent agency overseen by Congress that “regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states . . .”).


53 About the FTC, FTC.GOV, https://www.ftc.gov/about-ftc (last visited Dec. 19, 2017) (explaining that the FTC is an independent agency overseen by Congress whose purpose is to prevent “anticompetitive, deceptive, and unfair business practices . . .”).


55 Id.

56 See generally Jared Bomberg, FTC litigation prompts changes to congressional oversight, IAPP (Oct. 27, 2016), https://iapp.org/news/a/ftc-litigation-prompts-changes-to-congressional-oversight/ (stating that new litigation prompted congress to take a closer look at regulations and common practices).
security of IoT devices.\textsuperscript{56} Much of the legislation proposes a warning label on all smart baby monitors that warns parents of their potential to be hacked.\textsuperscript{57} Anything more restrictive has experienced difficulty being passed or has not been drafted at all.\textsuperscript{58} While the federal government has been unsuccessful in passing legislation to secure smart baby monitors, states have begun to fill the gaps.\textsuperscript{59}

New Jersey passed legislation that requires greater security measures for smart baby monitors.\textsuperscript{60} Once the Assembly passed the legislation, the Senate reviewed it.\textsuperscript{61} After amendments by the Senate were included, the Senate passed the legislation and sent it to the Assembly for a “second reading on concurrence.”\textsuperscript{62} The Assembly again passed the legislation and Governor Chris Christie signed the bill.\textsuperscript{63} The passing of this legislation could provide a great start to holding manufacturers of smart baby monitors accountable for their security breaches of consumer privacy.\textsuperscript{64}

The language of the original proposed bill required:

[b]aby monitor[s] that broadcasts audio or video through an internet connection shall be sold or offered for sale in the States unless it includes: (1) security features to prevent unauthorized users from hearing or viewing activity; and (2) a label or notice warning consumers of the risks associated with an unsecured baby monitor connection, and the importance of accessing the baby monitor securely and using its security features.\textsuperscript{65}

The smart baby monitors sold in New Jersey must contain a clearly worded

\begin{footnotes}
\item[56] Dourado & Castillo, supra note 16.
\item[59] Id.
\item[62] Id.
\item[63] Id.
\end{footnotes}
warning about potential security risks and technical features designed to thwart such infiltration. The legislation continues to describe the security requirements for the smart baby monitor. The bill’s final language, now law, says that smart baby monitor manufacturers are required to follow five security measures that state manufactures must:

1. provide end-to-end encryption;
2. provide Certificate-based Authentication for manufacturer access when obtaining updates, registering, or relaying audio or video between Internet servers;
3. prohibit unauthorized access, including prohibiting implied third-party trusted access;
4. prevent a consumer from disabling security measures; and
5. include conspicuous and easily understandable instructions supplied by the manufacturer notifying consumers about the proper use of the baby monitor and its security enhancement.

New Jersey could inspire other states to adopt legislation securing smart baby monitors that would hopefully draw Congress’ attention in the near future. Congressional enforcement of stricter security legislation is the consumers’ best hope in ensuring the privacy of their family and children.

FEDERAL REGULATION

To enforce federal law, federal agencies work to ensure smart baby monitor manufacturers are able to understand enacted legislation. Additionally, agencies promulgate regulations to fill gaps in the law to make it more efficient and effective. If manufacturers do not comply with regulations, then agencies bring actions to enforce compliance.

A. History of Federal Regulation

---

66 See id.
67 Stainton, supra note 64.
69 See id. (quoting the bill’s five required security measures).
71 Id.
72 About the FTC, supra note 52.
In response to Congress passing COPPA, the FTC promulgated regulations to inform the public how they would apply COPPA. The FTC is an agency that was created in 1914 by Congress to “prevent unfair methods of competition in commerce.” Congress has given “the agency greater authority to police anticompetitive practices over the years.” In 1938, Congress directed the FTC to apply several consumer protection laws “including the Telemarketing Sales Rule, the Pay-Per-Call Rule, and the Equal Credit Opportunity Act.” Then in 1975, Congress authorized the FTC to regulate trade rules of industry.

Now, the FTC’s purpose is to prevent “anticompetitive, deceptive, and unfair business practices...” The FTC protects consumers by filing suits against businesses and corporations not following safety and security requirements. In 1975, Congress granted the FTC authority to regulate the technology field. COPPA falls primarily under the FTC’s jurisdiction, allowing the agency to create regulations as standard practices for technology companies that are intertwined with children’s products. The FTC regulations §§ 312.1-312.12 describe how the FTC applies COPPA to the industry. Specifically, the regulations require technology companies that provide services over the internet to notify parents of any data retention of their children’s personal information, to obtain parental consent for any retained personal data, and to prevent the storage and collection of children’s personal information over the Internet.

COPPA and the FTC regulations only focus on operators’ data collection and storage. Consequently, they do not identify security measures smart baby manufacturers must take to prevent hackers from collecting and storing children’s personal information. The FTC has issued press releases and policy reports encouraging stricter asking Congress to approve legislation and create regulations for security and privacy of smaller technology products such as smart phones,

---

76 About the FTC, supra note 52.
77 Id.
78 Id.
79 Id.
80 Id.
82 About the FTC, supra note 52.
85 See id.
smart watches, and baby monitors.\textsuperscript{88} The FTC has been unable to sway Congress thus far.\textsuperscript{89} Without legislation for these new smart products, they are vulnerable to potential hackers.\textsuperscript{89} As a result of Congress’ lack of response, the FTC attempts to implement their recommendations by charging manufacturers of smart baby monitors with deceptive and unfair practices.\textsuperscript{91}

B. Gaps in Regulation

In February 2016, President Obama issued Executive Order 13718 to create the Commission on Enhancing National Cybersecurity (CENCS) in an attempt to improve national security and develop new technical solutions.\textsuperscript{92} The purpose of the CENCS is to:

- make detailed recommendations to strengthen cybersecurity in both the public and private sectors while protecting privacy, ensuring public safety and economic and national security, fostering discovery and development of new technical solutions,
- and bolstering partnerships between Federal, State, and local government and the private sector in the development, promotion, and use of cybersecurity technologies, policies, and best practices.\textsuperscript{93}

The CENCS’ December 2016 report included six main imperatives and various recommendations and actions that should be taken to better reinforce cybersecurity.\textsuperscript{94} While their recommendations and actions are commendable and can be applied to smart baby monitors, they only provide advice on what should be

\textsuperscript{89} See Bomberg, supra note 55 (stating that new litigation prompted congress to take a closer look at regulations and common practices).
\textsuperscript{91} See generally Complaint for Permanent Injunction and Other Equitable Relief at 2, FTC v. D-Link Corp., No. 3:17 Civ. 39 (N.D. Cal. 2017), 2017 WL 65168 (asserting the alleged violations of D-Link Corp. and their alleged deceptive act or practice).
\textsuperscript{92} Exec. Order No. 13718, 81 Fed. Reg. 29, 7441 (Feb. 9, 2016) (creating the Commission on Enhancing National Cybersecurity).
\textsuperscript{93} Id.
done. The CENCS does not have the power to enforce any of its recommendations or take the actions it requests. Instead, that power lies only with the leader of the executive branch, or the President.

Per the December 2016 report issued, any recommendations that are to be implemented will occur during the Trump administration. President Trump was scheduled to sign an executive order on cybersecurity on January 31, 2017, but abruptly failed to sign at the last minute. In turn, President Trump announced that “the U.S. will take quick action to secure critical infrastructure and networks and modernize IT systems.”

In addition to national security, President Trump wants to focus on improving the private sector. When President Trump held off signing the executive order on cybersecurity, he stated that the federal government “must work with the private sector . . . to make sure that owners and operators . . . have the support they need from the federal government to defend against cyber threats.” In early May 2017, President Trump signed a new executive order on cybersecurity. President Trump’s executive order provides that federal “agencies should be held accountable for their own cybersecurity and requires . . . that they introduce the cybersecurity framework developed by the National Institute of Standards and Technology (NIST).” Only time will tell if the new executive order is effective.

C. FTC Suit to Enforce Regulations

Previously, the FTC filed suit against a smart baby monitor manufacturer for its failure to adhere to the regulations promulgated by the agency to ensure proper implementation of COPPA. In the settlement of the suit, the FTC issued
additional recommendations to remedy these issues industry-wide. In 2013, the FTC brought suit against TRENDnet, Inc., a producer of IP cameras used in smart baby monitors. An IP Camera is a camera used for video surveillance through a network connection. Most IP Cameras can be adjusted and viewed from any web browser through Internet access if the IP Camera’s network is known. Before the suit went to court, TRENDnet settled with the FTC and a Consent Order was issued.

The FTC alleged that TRENDnet had (1) publicly transmitted consumer login credentials over the Internet; (2) stored consumers’ login credentials on personal smart devices that was easily readable; (3) failed to monitor and correct vulnerabilities and security breaches; and (4) failed to provide reasonable security in the design and testing of the software in the IP cameras. By failing to abide by the FTC promulgated regulations, the company subjected their consumers to a

---


110 A Consent Order is “a voluntary agreement worked out between two or more parties to a dispute...[and] has the same effect as a court order and can be enforced by the court if anyone does not comply with the orders.” Consent Order Law and Legal Definition, US LEGAL, https://definitions.uslegal.com/c/consent-order/ (last visited Dec. 19, 2017). Administrative agencies, such as the FTC, may issue Consent Orders in which a manufacturer agrees to “the imposition of certain disciplinary sanction.” Consent Orders allow the parties involved to “resolve a disciplinary proceeding initiated by the agency without the time and expense” of going to court. Id.


significant risk that the live feeds of their smart baby monitors would be compromised, exposing young children to the chance of being observed and recorded by strangers.\footnote{113} TRENDnet marketed its cameras as secure but they had faulty software “that left them open to online viewing, and in some instances listening, by anyone with the cameras’ Internet address.”\footnote{114}

The consent order required TRENDnet to create a better security program and apply safeguards to prevent consumers’ privacy from being compromised.\footnote{115} In addition, TRENDnet was ordered to retain third-party service providers outside of its company to maintain the security of its smart baby monitors and alert consumers when they have been affected by a breach in security.\footnote{116} The specificities of the consent order fall under nine parts.\footnote{117} Part I of the consent order prohibits TRENDnet from misrepresenting the level of its security measures or the level of protection over which the consumer has control.\footnote{118}

Part II of the consent order establishes eight explicit requirements to create an effective security program.\footnote{119} The eight requirements necessitate the creation of a new position to organize and run a security program that identifies risks to security and consumer privacy.\footnote{120} They also require a more secure design process and regular testing of the security of their devices.\footnote{121} The manufacturer must adopt any new developments in cybersecurity to ensure the best protection of its consumers’ privacy at all times.\footnote{122}

Part III of the consent order requires TRENDnet to implement a security program that meets the requirements of Part II of the consent order, and that the security program operates with “sufficient effectiveness.”\footnote{123} Part III also requires TRENDnet to biennially obtain a report from a third-party on the effectiveness of its security.\footnote{124}

\footnote{115} Id.; see generally TRENDnet, Inc.; Analysis of Proposed Consent Order To Aid Public Comment, 78 Fed. Reg. at 55,718.
\footnote{117} See TRENDnet, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 78 Fed. Reg. at 55,719.
\footnote{118} Id.
\footnote{119} Id.
\footnote{120} Id.
\footnote{121} Id.
\footnote{122} Id.
\footnote{123} See id.
\footnote{124} See id.
Part IV of the consent order requires TRENDnet to notify consumers whose smart baby monitors security has been breached. TRENDnet also must provide free instructions to consumers on how to remove the flaw and uninstall or update its IP cameras. Parts V through IX focus on reporting and compliance provisions that dictate how long TRENDnet is required to follow the provisions. The hope is TRENDnet will maintain the requirements on its own once the requirements have been implemented and followed for 20 years.

FTC SUIT AGAINST D-LINK

On January 5, 2017, the FTC filed suit against D-Link and its United States subsidiary in San Francisco’s federal court. D-Link is a producer of the Digital Baby Monitor Day/Night cloud Camera and Wireless Network Camera, both of which are smart baby monitors. The complaint states D-Link failed to take reasonable steps to secure the routers and Internet protocol cameras that it designed, marketed, and sold, especially in the form of smart baby monitors. The FTC alleges D-Link’s signing key was exposed on a public website, and since the default passwords were hardcoded into their machines, its products were easier to hack. Hackers who break into smart baby monitors are able to observe families and their homes through the cameras, sometimes speak to vulnerable children, and listen to private conversations in the home. Some hackers are pedophiles who wish to spy on children, and others are criminals who either use the device to gather personal information or case the home to rob the family.

125 Id.
126 Id.
127 Id.
128 Id.
130 Pagliery, supra note 74.
133 Pagliery, supra note 74.
135 See Cuthbertson, supra note 14 (noting how hacking instances of baby monitors are becoming more common and providing advice on how families can protect themselves);
The FTC has repeatedly warned D-Link about these “back door” flaws since 2007 but to no avail.136 D-Link has always stated that it is in compliance with COPPA and has not misled its consumers in the level of security its baby monitors contain.137 The FTC has not alleged any breach of product sold by D-Link, only that its routers and IP cameras used in smart baby monitors show a pattern of poor security practices.138 In the suit against D-Link, the FTC charged D-Link with six violations of FTC regulations which specifically enforce COPPA.139 The FTC alleges D-Link “failed to take reasonable steps to secure the software for their routers and IP cameras” exposing consumers’ local networks and allowing unauthorized access to sensitive personal information.140 Additionally, the FTC alleges that D-Link misrepresented the quality of the security it was providing to customers in all of its products, including its smart baby monitors, and therefore constitutes a deceptive act or practice.141 The FTC requested the court “enter a permanent injunction to prevent future violations of the FTC Act.”142 The FTC also asked the court to award the costs of bringing the action to the FTC and any additional relief the Court determines to be appropriate.143

On September 19, 2017, the court issued an Order Re Motion to Dismiss, granting in part and denying in part D-Links’ motion to dismiss.144 Counts I, IV, and V of the FTC’s complaint were dismissed with leave to amend and the agency was given until October 20, 2017 to revise their complaint against D-Link.145 The judge asserted that the complaint failed to specifically identify an incident where a consumer was harmed, and only alleged that the lack of security could lead to a breach in consumer’s personal information.146 Additionally, the

---

136 Pagliery, supra note 74.
138 Id.
139 Complaint for Permanent Injunction and Other Equitable Relief, supra note 131 at 11-13 (stating the alleged violations of D-Link Corporation).
140 Id. at 6,11 (“An attacker could compromise a consumer’s router, thereby obtaining unauthorized access to consumers’ sensitive personal information.”).
141 Id. at 12 (describing D-Link’s alleged promotional misrepresentations).
142 Id. at 13.
143 Id.
145 Id. at *6.
judge encouraged the FTC to focus on their deception claims rather than those which pose potential harm to American consumers. On October 17, 2017 the court granted an extension for the FTC to file an amended complaint until January 12, 2018.

The case is ongoing and represents the first instance a smart baby monitor manufacturer has not settled with the FTC. The outcome of this case is critical to the future of personal smart products, including smart baby monitors. Now that this case is in federal court, it should alert Congress to the need to promulgate new legislation to improve security for smart baby monitors.

FTC ATTEMPTS TO RECTIFY SECURITY ISSUES

Security measures have continued to adapt as technology has evolved. Smart baby monitor manufacturers have the technological capabilities and the resources to enhance the security of their products, but because of either negligence or lack of knowledge, do not take advantage of the protections available. To remedy the lack of knowledge, better communication and education of proper security measures needs to be available to manufacturers. In hopes of remedying this problem, the FTC issued recommendations and regulations for manufacturers of smart baby monitors. To comply with the FTC’s recommendations

---

147 Id.
149 See Pagliery, supra note 74 (recognizing that usually these types of suits settle).
150 See generally id. (commenting on the risk that baby monitors pose is how easily they may be hacked); Jared Bomberg, FTC Litigation prompts changes to congressional oversight, IAPP (Oct. 27, 2016), https://iapp.org/news/a/ftc-litigation-prompts-changes-to-congressional-oversight/ (describing Congress’ increased attention to FTC suits at the behest of the corporations that the FTC has filed suit against).
152 Cuthbertson, supra note 14 (describing the protections available to protect parents from baby monitor hacking); see also Flannigan, supra note 7) (discussing the security risks around wireless home devices, including baby monitors, and how while the device may have some security risks it is also crucial that the owner keep up with updates and determine which manufacturers are most compliant with FTC regulations).
154 Id.
and regulations, the manufacturers need to regularly check and monitor the regulations posted by the FTC.\(^\text{155}\) They must do so to ensure compliance and demonstrate they are consistently up to date with the new security and privacy measures available to manufacturers of smart baby monitors.\(^\text{156}\)

The FTC has attempted to remedy the negligence of smart baby monitor manufacturers, but their methods have been ineffective.\(^\text{157}\) The FTC has had some success via the judiciary system.\(^\text{158}\) One smart baby monitor manufacturing company, TRENDnet, settled with the FTC and agreed to implement extensive regulations for its security.\(^\text{159}\) Another smart baby monitor manufacturer, D-Link, refused to settle and is fighting the FTC’s allegations in court.\(^\text{160}\) The Circuit Court’s decision will either apply the broad requirements of COPPA to the narrow regulations created by the FTC, or they will recommend to Congress that COPPA needs to be amended to include stricter security measures and procedures for smart baby monitors.\(^\text{161}\) Even if the Court applies the broad terms of COPPA and the FTC regulations to force D-Link to apply stricter security measures and procedures, Congress should still draft legislation to reflect the application of COPPA provided by the court.

The appropriate remedy to protect the privacy of consumers of smart baby monitors is stricter security laws and regulations for the manufacturers of these products.\(^\text{162}\) The FTC has pleaded with Congress to enact legislation based on its regulations and recommendations.\(^\text{163}\) The FTC has stringent regulations that can be effectively transformed into legislation, such as establishing and maintaining “reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children” and preventing data retention of

\(^{155}\) Id.

\(^{156}\) Id.

\(^{157}\) See generally id. (discussing that despite the information and technology available to smart baby monitor manufacturers, stricter security measures and stronger consumer privacy protection has not occurred despite FTC encouragement to adopt better practices).


\(^{160}\) Pagliery, supra note 74 (describing D-Link products and their lack of security).


\(^{162}\) See id.

\(^{163}\) FTC IoT REPORT, supra note 148 (explaining that despite FTC encouragement to adopt better practices, stronger consumer privacy protection measures that could institute permitted and prohibited uses have not commenced).
personal information collected from children. Additionally, the conditions outlined in settlement of the TRENDnet suit are strong requirements that should be adopted by Congress. If Congress adopts the requirements expressed in the TRENDnet consent order, the security of smart baby monitors will increase dramatically. This will provide more safety for consumers of smart baby monitors when using the products.

PROPOSED SOLUTIONS TO SECURE SMART BABY MONITORS

Some manufacturers of smart baby monitors have adopted their own regulations based on the TRENDnet suit. Two smart baby monitor manufacturers that have embraced self-regulation and increased security measures are Mattel and Amazon. These manufacturers can serve as examples to Congress and other smart baby monitor manufacturers of the ways they can follow best practices of the protection of consumer privacy. For those smart baby manufacturers that do not self-regulate their security measures, federal legislation must be imposed.

There are a few key points from the TRENDnet suit that can be proposed as legislation to increase security and the protection of consumers’ privacy. Suggested legislation would require 1) stricter login credentials; 2) a department to monitor the security of a product and the potential breaches of privacy; 3) training and continuing education for individuals in charge of monitoring the security of products; and 4) the manufacturer to notify consumers if their privacy has been breached and provide free services to remedy the breaches. These four proposed security measures for smart baby monitor manufacturers are further discussed below.

A. Stricter Login Credentials and Updates to Programs

164 15 U.S.C. §6502(b)(1)(D) (2012); see generally Cooper, supra note 156 (stating that the Federal Trade Commission regulations have effectively acted like federal statutes and have removed the harm requirement of the regulations).
165 See generally TRENDnet, Inc.; Analysis of Proposed Consent Order To Aid Public Comment, 78 Fed. Reg. at 55,719.
166 See generally id.
167 See Mark Wilson, Mattel is Building an Alexa For Kids, FAST CO.: CO. DESIGN (Jan. 3, 2017), https://www.fastcodesign.com/3066881/mattel-is-building-an-alexa-for-kids (describing their new product Aristotle and their focus on COPPA compliance and protecting children’s personal information).
168 See id.
169 See id.
170 See generally TRENDnet, Inc.; Analysis of Proposed Consent Order To Aid Public Comment, 78 Fed. Reg. at 55,719.
First, stricter login credentials for smart baby monitors can be easily achieved and protected. Consumers usually leave login credentials for their smart baby monitors at factory settings because consumers are unaware of the risks they face.\textsuperscript{171} Factory login credentials are historically easy to hack.\textsuperscript{172} The average consumer does not understand the risks to their privacy or even how to change their login credentials on their smart baby monitors.\textsuperscript{173} Some smart baby monitors do not even allow the factory set passwords to be changed.\textsuperscript{174} The login keys are not protected by the manufacturers and are even publicly transmitted over the Internet.\textsuperscript{175} The easiest remedy to mitigate this risk is to require smart baby monitor manufacturers to have stricter login credentials.\textsuperscript{176} For those devices that have fixed login keys, creating login keys that can be changed by the consumers allows for an extra level of protection aside from the protections that should be built into the smart baby monitors.\textsuperscript{177}

Second, there needs to be advanced encryption of login keys.\textsuperscript{178} There are methods for transmitting login keys safely over the Internet that are available to manufacturers, but manufacturers do not use these methods.\textsuperscript{179} The lax security of login credentials is not due to unavailability of appropriate technology, but to the negligence of the manufacturing companies.\textsuperscript{180} The best practices for code

\textsuperscript{171} See generally Jehl et al., supra note 25.
\textsuperscript{172} See generally id.
\textsuperscript{173} See generally id.
\textsuperscript{174} See id.
\textsuperscript{175} Cuthbertson, supra note 14 (explaining that manufacturers publicly transmit data over the Internet for parents to view live feeds, many of which are not protected); Press Release, Fed. Trade Comm’n, Sept. 4, 2013, supra note 15.
\textsuperscript{176} Login credentials are encrypted login keys, or a type of coded password, that are created by the manufacturers. Cuthbertson, supra note 14 (exploring the most effective ways to mitigate the risk of security breaches, including stricter login credentials); Press Release, Fed. Trade Comm’n Sept. 4, 2013, supra note 15.
\textsuperscript{177} Cuthbertson, supra note 14.
\textsuperscript{178} See generally Shivali Best, Are Hackers Watching You and Your Children? Yet Another Flaw in Samsung’s Security SmartCam Could Let Criminals Spy on Your Home, MAILONLINE: SCL (Jan. 19, 2017), http://www.dailymail.co.uk/sciencetech/article-4136412/Are-hackers-watching-home.html (discussing the opportunity hackers have to access a parent’s network, turn the camera on, and potentially lock their account without advanced encryption of login keys); TRENDnet, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 78 Fed. Reg. at 55,719.
\textsuperscript{179} Best, supra note 173 (exemplifying Samsung as a manufacturer that has chosen not to utilize available methods for safely transmitting login credentials, and instead chose to remove the web interface feature altogether); see generally TRENDnet, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 78 Fed. Reg. at 55,718.
\textsuperscript{180} Best, supra note 178 (exemplifying Samsung has a manufacturer that has chosen not to utilize available methods for safely transmitting login credentials, and instead chose to remove the web interface feature altogether).
signing, or encryption of login keys, are (1) to minimize unauthorized access to private keys; (2) to protect private keys with cryptographic hardware; (3) to time stamp the code for easy verification; (4) to use test-signing; (5) to authenticate all and any codes; (6) to scan for viruses before signing keys; and (7) to change the use of keys and certificates often and revoke signing keys when a security flaw is discovered. Instead of relying on the inexperience of consumers, manufacturers should be required to protect the transmittance of login credentials so the easily hacked network keys are no longer an issue. Security login credentials are not the only problem smart baby monitor manufacturers need to remedy.

In addition to a lack of secure login credentials, manufacturers leave holes for hackers to enter products around the updates they send to consumers. Often the php files, which provide updates to baby monitor cameras, are not properly secured. The scripts often have bugs that allow non-admin users to gain remote access to the smart devices. The updates consumers receive are to improve the functions of the application used to control the smart baby monitors. Smart baby monitor manufacturers are constantly updating the applications to prevent bugs in the programming. When manufacturers provide updates to consumers

---

181 “Code signing is the method of using a . . . digital signature...in order to verify the author’s identity and ensure that the code has not been changed or corrupted since it was signed by the author.” If the code has been changed or corrupted since the author signed it, it has been hacked. What is Code Signing?, SSL SHOPPER, https://www.sslshopper.com/what-is-code-signing.html (last visited Dec. 19, 2017).


183 Id. (quoting Test-signing certificates “[help] ensure [the] test certificates are trusted only within the intended environment.”).

184 Id.


186 Best, supra note 178.


188 See Best, supra note 178.

189 Id.


to improve the security of their smart devices, the manufacturers need to ensure that the update is sent safely to consumers.

B. Security Monitoring Department

Manufacturers, especially large manufacturers, have difficulty securing their smart devices. Another simple way for large manufacturers to prevent the invasion of consumer privacy and violation of their security is to require the manufacturers of smart baby monitors to create a department to monitor the security of their products. Third parties will often test the security of smart baby monitor products and their networks to determine their ability to be hacked. Third parties will then notify the manufacturers of the flaws, but manufactures often do not respond to the notifications. The holes in the smart baby monitor products and networks are easily penetrated and never repaired by the manufacturers.

If the manufacturers establish a department dedicated to probing for holes and remedying any breaches they discover, the smart baby monitor products and networks could be constantly updated to prevent any new threat. These departments will ensure the security of their smart baby monitor products and networks is repeatedly reinforced and can assure the continued protection of consumer privacy. Many companies have not created a security-monitoring department due to an apathy towards security and improper budgeting. Smart personal product companies such as Mattel and Microsoft prioritize the security of their consumers’ personal information. By prioritizing security, they have ensured

---

192 Best, supra note 178.
194 Best, supra note 178.
195 Id.
196 Id.
198 Press Release, Fed. Trade Comm’n Feb. 7, 2014, supra note 74 (stressing the importance of these security departments in protecting security, confidentiality, and integrity of information); see generally TRENDnet, Inc.: Analysis of Proposed Consent Order to Aid Public Comment, 78 Fed. Reg. at 55,719.
199 See generally Vaas, supra note 190 (acknowledging that manufacturers still aren’t incorporating adequate security into their products, leaving consumers responsible to add layers of protection themselves).
200 See Mark Hachman, Mattel and Microsoft reveal Aristotle, a tabletop digital nanny
their security monitoring departments receive the proper training and funding they need to be effective. Other manufacturers of smart baby monitors have no excuse for not establishing an effective security-monitoring department. Even if manufacturers claim they cannot afford to establish a new in-house security monitoring department due to the expense, they already possess the requisite resources to do so.

If the manufacturer cannot establish an in-house security monitoring department, then it should be required to engage a third party security monitoring company. When there is a risk for a breach of customers’ privacy, these third party security monitoring companies can either enhance the security measures of the manufacturers’ smart devices or issue a report to manufacturers informing them of the necessary changes to their smart devices they must take to remedy potential breaches in consumer privacy. Third parties often supply manufacturers with reports warning the manufacturers of potential risks, but they are frequently ignored. By forcing manufacturers to employ their own department or third party security monitoring company, they will have the advice of the reports provided to them.

There should also be an additional requirement obligating manufacturers of smart baby monitors to apply the advice and findings of the reports. Simply obtaining the reports does not ensure the manufacturing companies will apply the findings of the reports. These reports, whether obtained in house or through third-parties, provides valuable insight to any gaps or holes in their smart baby monitors’ security.

C. Training and Education

Some manufacturers have existing departments for monitoring security that


201 See Hachman, supra note 200; Wilson, supra note 167.

202 See Hachman, supra note 200; Wilson, supra note 167.

203 See generally TRENDnet, Inc.; Analysis of Proposed Consent Order To Aid Public Comment, 78 Fed. Reg. 55,719.

204 See generally id. (ordering an assessment and report from a third-party professional that the security provided offers sufficient, effective protection of TRENDnet’s customers).

205 See generally id.

206 Best, supra note 178.

207 See generally id.

208 See generally id.

209 See generally id.
are not properly trained or updated on changes in the security field.\textsuperscript{210} As the ability of Internet hackers to break through security defenses increases daily, manufacturers must ensure their security-monitoring department is constantly evolving to best keep out Internet hackers.\textsuperscript{211} The security monitoring departments are the first and last lines of defense for the protection of consumer privacy.\textsuperscript{212} By providing training and education for their security monitoring departments, manufacturers can provide the best service available to protect their customers.\textsuperscript{213}

D. Consumer Notification and Remedies

As discussed above, there have been attempts by some state and federal legislatures to provide adequate notification to consumers but it has not been enough.\textsuperscript{214} Some of the proposed legislation has not passed and some has passed.\textsuperscript{215} To make consumers aware of the dangers and liability they face in purchasing smart baby monitors, manufacturers should be required to provide more than a mere warning label on the box. While a warning label on the smart baby monitor boxes is helpful, manufacturers should be required to make the warning labels easily readable. The law should require manufacturers to provide information in a manual on how consumers can best protect themselves from harm and a violation of their privacy.\textsuperscript{216} The manufacturer should include the

\begin{itemize}
  \item \textsuperscript{210} See generally id.
  \item \textsuperscript{211} See Thomas Fox-Brewster, It’s Depressingly Easy to Spy on Vulnerable Baby Monitors Using Just a Browser, FORBES (Sept. 2, 2015, 9:46 AM), https://www.forbes.com/sites/thomasbrewster/2015/09/02/baby-surveillance-with-a-browser/#485918de1aa0 (showcasing how easy it is for hackers to access information and gain control of baby monitors).
  \item \textsuperscript{212} See Best, supra note 178.
  \item \textsuperscript{213} See generally TRENDnet, Inc.; Analysis of Proposed Consent Order To Aid Public Comment, 78 Fed. Reg. at 55,718-19.
  \item \textsuperscript{214} Jehl et al., supra note 25.
  \item \textsuperscript{215} See S. Res. 110, 114th Cong. (2015); see generally Sen. B. 2582, 217th Leg., Reg. Sess. (N.J. 2016) (requiring “baby monitors with internet connection to include security features and warning.”); Process Reform Act of 2012, H.R. 3309, 112th Cong. (2nd Sess. 2012) (articulating that “the packaging of a new baby monitor [is required] to display a warning label so that families are informed that video and sounds ... may be easily viewed or heard by potential intruders.”). \textsuperscript{216} See Process Reform Act of 2012, H.R. 3309, 112th Cong. (2nd Sess. 2012) (quoting “the packaging of a new baby monitor [is required] to display a warning label so that families are informed that video and sounds ... may be easily viewed or heard by potential intruders.”); Sen. B. 2582, 217th Leg., Reg. Sess. (N.J. 2016) (requiring “baby monitors with internet connection to include security features and warning.”); see generally S. Res. 110, 114th Cong. (2015).
manual in the box with any installation and use instructions. While manufacturers cannot guarantee consumers will read this information, it is still important to provide the warnings. Other methods such as promotional campaigns on television or the Internet can spread awareness to consumers of the dangers and steps they can take to ensure their privacy is protected.

When the warnings, security monitoring departments, stricter login credentials and software updating procedures fail, manufacturers should have a plan to remedy the security breach. The law should require manufacturers to notify consumers of the breach in security and the potential invasion of their privacy. Then, the law should also require manufactures to fix the bugs and create a patch for the smart baby monitors to prevent future breaches from occurring. Manufacturers should provide support for consumers whose privacy has been compromised to recommend steps consumers could take to rectify the violation and provide recommendations on how to help prevent future breaches from occurring.

Smart baby monitor manufacturers should be held accountable for their actions and be required to do more than alert consumers to the security breach, and the potential exposure of consumers’ private and personal information. By compelling smart baby monitor manufacturers to patch the breach, future security breaches of consumer personal information would decrease significantly. Additionally, spending the money and resources to help consumers contain the damage they have suffered by the exposure of their personal information will encourage smart baby monitor manufacturers to improve their security. The expense they will incur is all the motivation smart baby monitor manufacturers need to strengthen security. Some smart baby monitor manufacturers are taking note of the FTC suits and are motivated to improve their security.

218 See generally Sen. B. 2582, 217th Leg., Reg. Sess. (N.J. 2016), (requiring “baby monitors with internet connection to include security features and warning.”).
219 See generally id. (highlighting that recent news articles have raised awareness about baby monitors, by raising awareness to consumers of the dangers, they can take proactive steps to ensure privacy).
221 See id.
225 See generally id.
226 See generally id.
227 See Jerry Lee, Mattel Nabi Announces First-Ever Connected Kids Room, Powered by IOT: MICROSOFT: BLOG (Jan. 5, 2017), https://blogs.microsoft.com/iot/2017/01/05/mattel-
E. Aristotle

One manufacturer of baby monitors recognized the need for stricter security regulations to protect the privacy of families and children. Mattel and Microsoft partnered to create Aristotle, a smart baby monitor branded as a “tabletop digital nanny.” Aristotle is “a voice-activated smart assistant.” It answers questions for the parents and children, orders baby supplies when they get low, sings babies to sleep, and plays games with the children. Aristotle is controlled through an application on consumers’ cellular phones. Aristotle uses a voice-activated speaker, streams encrypted video to the consumers’ smart phone, and uses special software designed to increase the security of the smart baby monitor and protect consumer privacy.

Executives from Mattel and Microsoft assert that the companies built Aristotle in accordance with COPPA compliance to ensure children’s privacy is maintained. Additionally, there are no default passwords. Without default passwords, the smart baby monitor is less exposed to hackers. Mattel and Microsoft designed the technology so that “the phone and Aristotle forget their own encrypted connection via Bluetooth... [and] [a]ll data is always encrypted to and from devices and to and from the cloud.” Mattel and Microsoft were not compelled by the FTC to incorporate these security measures into their new device they chose to regulate themselves. Congress can use the success of Mattel and Microsoft’s Aristotle to promulgate legislation for other smart baby monitor manufacturers with which to comply. Other smart baby monitor manufacturers should look to Mattel and Microsoft’s example if they wish to prevent future

See generally Lee, supra note 227 (“[U]sing Mattel and Microsoft as an example of companies who have ‘taken security very seriously’ and discussing various security features they have implemented”).

---

228 See id.
229 Hachman, supra note 200.
231 Id.
232 Hachman, supra note 200.
233 Id. (discussing how Aristotle has been built in compliance with COPPA, which ensures privacy by eliminating default passwords, as well as streaming data and using a connection that is encrypted); Hollister & Priest, supra note 230 (discussing Aristotle’s secure features such as voice-activated smart assistance, and encrypted video).
234 Hachman, supra note 200.
235 Id.
236 Id.
237 Id.
litigation and security breaches of their consumers’ privacy.

Despite the enhanced regulations Mattel and Microsoft have applied to Aristotle, the smart baby monitor will not be impervious to hackers, but it will be significantly safer. Mattel and Microsoft should still ensure they have an easily readable warning label, an effective security-monitoring department, increased education and training for the security-monitoring department, and established remedies for the consumers when their privacy is compromised.

Aristotle is the start to a safer smart baby monitor, but more can always be done to ensure stronger security. Congress cannot rely on all smart baby monitor manufacturers like Mattel and Microsoft to adopt effective security measures on their own. Congress must promulgate laws to force the compliance of other smart baby monitor manufacturers and to enhance the security measures some smart baby monitor manufacturers are already taking.

CONCLUSION

The FTC suit against D-Link and the progressive actions of Mattel and Microsoft are only the beginning of increased security measures in smart baby monitors. Hopefully, other smart baby monitor manufacturers will realize the importance of protecting the privacy of their consumers and the consumers’ children. Once other manufacturers of smart baby monitors detect the changes occurring in the industry, they will begin their own processes to increase the security of their smart devices.

Congress cannot rely on manufacturers of smart baby monitors to take on this daunting task of implementing stricter security measures on their own. Congress must promulgate new legislation specifically to protect the privacy of children involving smart baby monitors. Whether COPPA is to be modernized, a new federal law is established, or there is multiple new state laws regulating smart baby monitors and the manufacturers individually, something needs to change.

Regulating the security of baby-monitors is important to the privacy and safety of children, and new legislation should be adopted to enforce security. Few smart baby monitor-manufacturing companies are motivated to improve

---

238 Hachman, supra note 200 (describing their new smart baby monitor and the safety measures they took to comply with COPPA to ensure the protection of their consumers’ privacy and personal information).


240 See generally TRENDnet, Inc.; Analysis of Proposed Consent Order To Aid Public Comment, 78 Fed. Reg. at 55,719; Press Release, Fed. Trade Comm’n Feb. 7, 2014, supra note 74 (describing the various safety and security requirements for TRENDnet’s smart baby monitor products in their consent order with the FTC); Hachman, supra note 200.
security to protect consumers’ privacy and personal information. The FTC suits and regulations are not strict enough to force compliance of an entire industry. Hackers are becoming more sophisticated every day, making smart baby monitors vulnerable to those who wish to invade the privacy of families and young children.