DEVELOPING A BALANCED PRIVACY FRAMEWORK

ANNA KARAPETYAN*

TABLE OF CONTENTS

I. INTRODUCTION

Emerging technologies are impacting all industries and creating a world which is increasingly connected due to advances such as artificial

intelligence, self-driving vehicles, and the "Internet of Things" ("IoT"),[1] a network of "smart" devices that communicate with each other by sending and receiving data. This current trend of automation and data exchange has been called the "Fourth Industrial Revolution," and it is predicted to fundamentally alter our lifestyles and challenge our current beliefs.[2]

Voice-controlled digital assistants are at the forefront of this fundamental change. Digital assistants are devices which use speech recognition software to execute commands spoken in natural language.[3] Both consumers and companies are rapidly adopting these voice-controlled assistants, as evidenced by the Consumer Electronics Show ("CES"), an annual technology conference that reveals the trends for the coming year.[4] The 2017 CES presented a world in which voice assistants were integrated into products from nearly every category of goods, including refrigerators, fitness trackers, washing machines, and cars.[5] The 2018 CES took this

---

* J.D. 2018, University of Southern California Gould School of Law; B.S. Psychology 2014, University of Southern California. I would like to express my gratitude to Professor Valerie Barreiro for sparking my interest in privacy law and providing valuable guidance and feedback on this Note. In addition, I am grateful to the staff and editors of the *Southern California Review of Law and Social Justice* for their excellent work.

[1] Nicole Kobie, *What is the Internet of Things?*, THE GUARDIAN (May 6, 2015), https://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google.

[2] *See, e.g.*, Bernard Marr, *Why Everyone Must Get Ready for the 4th Industrial Revolution,* FORBES (Apr. 5, 2016), https://www.forbes.com/sites/bernardmarr/2016/04/05/why-everyone-must-get-ready-for-4th-industrial-revolution/#3243def23f90 ("These new technologies will impact all disciplines, economies and industries, and even challenge our ideas about what it means to be human...These technologies have great potential to continue to connect billions more people to the web, drastically improve the efficiency of business and organizations...."); PRICEWATERHOUSE COOPERS, INDUSTRY 4.0: BUILDING THE Digital ENTERPRISE 4 (Apr. 2016), http://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf (stating that the fourth industrial revolution will fundamentally change companies and "transform market dynamics" across industries); Deloitte Insights, The Fourth Industrial Revolution is Here—Are You Ready? 20 (Jan. 1, 2018), https://www.forbes.com/forbes-insights/wp-content/uploads/2018/01/Deloitte-FourthIndustrialRev_REPORT_FINAL-WEB.pdf ("Industry 4.0 represents the ways in which smart, connected technology becomes embedded within organizations, as well as people's daily lives.").

[3] *What is a Digital Assistant?*, GCF LEARNFREE, http://www.gcflearnfree.org/using-the-web-to-get-stuff-done/what-is-a-digital-assistant/1/.

[4] Jim McGregor, *CES (Consumer Electronics Show) 2017 Preview*, FORBES (Jan. 3, 2017, 2:31 PM), https://www.forbes.com/sites/tiriasresearch/2017/01/03/ces-consumer-electronics-show-2017-preview/#fb69f7847f5b; Mark Bergen & Olga Kharif, *At CES, New Digital Assistants Restart Smart Home Race*, BLOOMBERG (Jan. 5, 2017), https://www.bloomberg.com/news/articles/2017-01-05/at-ces-new-digital-assistants-restart-smart-home-race.

[5] *CES 2017 Catapults a Connected World*, CES, http://www.ces.tech/News/Press-Releases/CES-Press-Release.aspx?NodeID=81a5ac51-9557-415f-8801-fe11af699a7a; Ryan Chiavetta, *Voice*

integration to a higher level, with voice assistants taking the spotlight.[6] The rapid and continuous integration of voice assistants and their millions of embedded sensors into everyday appliances has resulted in the collection of an unprecedented amount of data.[7] This digital universe doubles in size nearly every two years, and by 2020 is predicted to contain as many bits of data "as there are stars in the universe."[8]

The integration of voice assistants into an array of product categories raises privacy concerns for consumers because it challenges their ability to control the use of their personal information. Digital assistants are always on and are constantly listening to consumers in their most private spaces. They can record intimate conversations from inside a home and transmit the data to outside company servers, after which it could be used or disclosed by the company with almost no restrictions.[9]

Consumers' rapid adoption of increasingly prevalent digital assistants that are constantly listening presents challenges to current privacy regulations. Existing sectoral federal privacy statutes create a fragmented system of regulation that leaves data collected by digital assistants

---

Assistants, Smart Gadgets Dominate CES 2017, IAPP (Jan. 6, 2017), https://iapp.org/news/a/voice-assistants-and-other-smart-devices-dominate-ces-2017/.

[6] Ben Fox Rubin, *Alexa, Google Assistant Want to Be Everywhere in 2018*, CNET (Jan. 16, 2018), https://www.cnet.com/news/ces-2018-voice-assistant-alexa-google-echo-smart-home-bixby/; Michelle Fitzsimmons, *How Google Assistant and Amazon Alexa Took Over CES 2018*, TECHRADAR (Jan. 11, 2018), http://www.techradar.com/news/how-google-assistant-and-amazon-alexa-took-over-ces-2018.

[7] Michael Kanellos, *152,000 Smart Devices Every Minute In 2025: IDC Outlines the Future of Smart Things*, FORBES, (Mar. 3, 2016), https://www.forbes.com/sites/michaelkanellos/2016/03/03/152000-smart-devices-every-minute-in-2025-idc-outlines-the-future-of-smart-things/#2879c6b84b63 ("[A]pproximately 11 billion devices connect to the Internet now. The figure is expected to nearly triple to 30 billion by 2020 and then nearly triple again to 80 billion five years later.).

[8] DELL EMC, THE DIGITAL UNIVERSE OF OPPORTUNITIES: RICH DATA AND THE INCREASING VALUE OF THE INTERNET OF THINGS 2 (Apr. 2014), https://www.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf.

[9] *See* Eric Boughman et al., *"Alexa, Do You Have Rights?": Legal Issues Posed by Voice-Controlled Devices and the Data They Create*, AMERICAN BAR ASSOCIATION (July 2017), https://www.americanbar.org/publications/blt/2017/07/05_boughman.html (discussing Fourth Amendment case law indicating that individuals have "no reasonable expectation of privacy in information disclosed to a third party.").

unregulated.[10] The Federal Trade Commission ("FTC") steps in to fill this gap and regulates this data under its Section 5 authority.[11]

Although the FTC is tasked with the important mandate of protecting consumers while promoting competition, it falls short in its privacy regulation. Numerous recent cases show that always-listening devices can surreptitiously record conversations, spy on consumers, and even sell licenses to listen to consumers in their homes.[12] FTC regulations do not do enough to address such risks and must be strengthened. FTC regulations do not protect consumers because they are grounded on flawed analysis which fails to account for important factors. The FTC must evaluate the effects of its regulation and reshape its approach to properly account for, and examine, relevant considerations.

This Note argues that the FTC should make changes to how it regulates, to act in a way that is calculated to ensure consumer privacy. First, the FTC should consider the market and act to correct any existing defects and inequities. Second, the FTC should lead the industry by acting to proactively prevent privacy harms instead of attempting to remedy past injuries. Third, the FTC should carefully analyze any action it takes and carefully weigh all relevant factors. In doing so, it should consider both the short-term and long-term effects of its regulation. The FTC will take bigger strides towards its goals if it adopts these changes, and its actions will more likely result in the most effective outcomes.

Part I of this Note defines digital voice assistants, describes how the technology works, and provides examples of their uses. Part II sets forth a definition of privacy and broadly reviews current privacy regulations in the United States. It examines how existing regulations apply to voice assistant data and concentrates on FTC regulation of privacy. Part III evaluates how the FTC has acted to protect privacy and argues that its regulation has not done enough to protect consumers. It reviews specific instances of regulation and asserts that any regulation shortcomings are an effect of misguided analysis. Part III next argues that the FTC should change its

---

[10] *See* Daniel J. Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TEACHPRIVACY (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law/ (discussing how the sectoral approach results in "a ton of complexity, inconsistency, and uncertainty in the law.").

[11] *Privacy & Data Security Update (2016)*, FED. TRADE COMM'N (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016 (Section 5 "prohibits unfair or deceptive practices in the marketplace").

[12] *See* Jay Stanley, *The Privacy Threat From Always-On Microphones Like the Amazon Echo*, ACLU (Jan. 13, 2017), https://www.aclu.org/blog/privacy-technology/privacy-threat-always-microphones-amazon-echo.

regulation to more effectively pursue its dual goal of protecting consumers and promoting competition. Finally, Part III sets forth specific proposals for change and evaluates their potential effects.

II. DIGITAL VOICE ASSISTANTS

A. WHAT ARE VOICE ASSISTANTS?

Voice-controlled digital assistants are a category of microphone-enabled devices which can recognize and process voice commands using artificial intelligence algorithms.[13] These virtual assistants come in many forms and can be found on a variety of devices, including the widely-known Siri on Apple iPhones.[14] Users can interact with the assistant simply by speaking in a conversational voice and saying anything from "Tell me the weather" to "Play music." Currently, four prominent voice-controlled assistants dominate the market: Amazon's "Alexa," Google's "Assistant," Microsoft's "Cortana," and Apple's "Siri,"[15] with the former two leading the way.[16] Both Alexa and Assistant are available on each company's speaker, the Echo[17] and the Google Home,[18] respectively.

Voice assistants are powered by speech recognition software and contain embedded sensors to detect a user's voice. The value of voice assistants comes in large part from the fact that they are always on call, ready within moments to perform any of a user's commands. As a necessary corollary, the device is constantly on, listening for a cue to begin processing information. This cue comes in the form of a "wake word," the trigger that

---

[13] Edward C. Baig, *Personal Digital Assistants Are On the Rise (and They Want to Talk)*, USA TODAY (May 8, 2016), http://www.usatoday.com/story/tech/columnist/baig/2016/05/08/personal-digital-assistants-rise-and-they-want-talk/83715794/#; THE 2017 VOICE REPORT: EXECUTIVE SUMMARY, VOICELABS.CO 2–3, https://s3-us-west-1.amazonaws.com/voicelabs/report/vl-voice-report-exec-summary_final.pdf [hereinafter 2017 VOICE REPORT].

[14] *Siri*, APPLE, http://www.apple.com/ios/siri/.

[15] Shreya Bhattacharya, *Who's the Best? – Digital Voice Assistants*, THETECHY (Mar. 21, 2017), https://www.thetechy.com/whos-the-best-digital-voice-assistant/.

[16] Tom Warren, *Microsoft's Cortana falls behind Alexa and Google Assistant at CES*, THE VERGE (Jan. 15, 2018), https://www.theverge.com/2018/1/15/16892462/microsoft-cortana-alexa-google-assistant-ces-2018.

[17] *Echo & Alexa Devices*, AMAZON, https://www.amazon.com/Amazon-Echo-And-Alexa-Devices/b?ie=UTF8&node=9818047011; Ben Gilbert, *Amazon's Echo vs Google's Home: Here's How the Two Families Stack Up*, BUSINESS INSIDER (Jan. 15, 2018), http://www.businessinsider.com/amazon-echo-vs-google-home-2017-10.

[18] *Google Assistant*, GOOGLE, https://assistant.google.com/platforms/speakers/; Gilbert, *supra* note 17.

prompts the device to begin processing the voice command to determine how to respond.[19] For example, Amazon's Alexa is activated by "Hey, Alexa" and the Google Home is activated by "OK, Google."[20] The powerful sensors in these devices can detect voice commands and easily identify a user's voice despite background noises[21]—such as barking dogs or a television—over even relatively large distances, such as from a different room.

Once the device detects the wake word through its embedded sensors, the user's voice is recorded and streamed to the cloud, where the request is processed to perform the task. The audio stream to the cloud begins a fraction of a second before the wake word is detected and continues until the question or command has been processed.[22] Even before the wake word triggers active listening, the device's embedded microphone constantly records sounds locally and passively listens until it is triggered to begin processing.[23] Generally, assistants can be set to alert users when a wake word is detected and recording begins. For example, Amazon's Alexa can be programmed to produce a sound, [24] and Google Home has flashing lights to notify users the recording function is activated.[25]

---

[19] *See, e.g.*, *Alexa & Alexa Devices FAQs*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 (Alexa also lets you change the wake word to either "Computer," "Amazon," or "Echo.") [hereinafter *Alexa FAQ*]; *Google Home*, GOOGLE, https://madeby.google.com/home/ (Google lists a large quantity of features regarding their hands-free experience). *See also* Rowan Trollope, *7 Things You Didn't Know About Wake Words*, MEDIUM (Nov. 29, 2017), https://medium.com/@rowantrollope/7-things-you-didnt-know-about-wake-words-d4e9e041d11d (wake words are the "gateway between you and your [voice assistant]").

[20] *Google Home*, *supra* note 19.

[21] *Id.*

[22] *Alexa FAQ*, *supra* note 19.

[23] STACEY GRAY, FUTURE OF PRIVACY FORUM, ALWAYS ON: PRIVACY IMPLICATIONS OF MICROPHONE-ENABLED DEVICES, FUTURE OF PRIVACY FORUM 4 (Apr. 2016), https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf; *Data Security & Privacy on Google Home*, GOOGLE, https://support.google.com/googlehome/answer/7072285 (click "Is Google Home recording all of my conversations" under Privacy) ("Google Home listens in short (a few seconds) snippets for the hotword. Those snippets are deleted if the hotword is not detected, and none of that information leaves your device until the hotword is heard.") [hereinafter *Google Support*].

[24] *Alexa FAQ*, *supra* note 19.

[25] *Google Support*, *supra* note 23 (follow "Privacy" then "Is Google Home recording all of my conversations") ("When Google Home detects that you've said 'Ok Google' or that you've physically long pressed the top of your Google Home device, the LEDs on top of the device light up to tell you that recording is happening").

Voice assistants collect a variety of information, including a sample voice recording of the user, an audio transcription, and location data.[26] Voice recordings are stored on the cloud and used to learn more about the user, including the user's speech patterns and personal preferences.[27] Digital assistants allow users to access past recordings and delete them;[28] however, it is not clear whether the company still retains the voice recording transcription after deletion of the audio.[29] Information collected by a voice assistant is kept in the company's data center.[30] Consumer information can be combined with a variety of third party data and analyzed to infer specific user characteristics and provide personalized recommendations.[31]

B. INCREASING PREVALENCE AND INTEGRATION

The ability to gather and analyze a tremendous amount of data and use the resulting insights to adapt to each user and provide a personalized experience makes digital assistants a great resource. Voice-controlled assistants allow natural interaction and facilitate everyday tasks, creating a seamless experience for consumers through intuitive hands-free control. Commands ranging from ordering new household supplies to calling an Uber can all be executed simply by speaking aloud. Further, digital

---

[26] *See, e.g.*, *Google Support*, *supra* note 23 (follow "Services" then "Does the third-party service provider get an audio recording of what I said?") ("Google transcribes what you say and sends the text, but not the audio, to the third-party service provider."); *Google Support*, *supra* note 23 (follow "Privacy" then "Who can hear my location/search/conversation history?") ("Anyone who is near your Google Home device can request information from it").

[27] *See, e.g.*, *Echo Dot*, AMAZON, https://www.amazon.com/gp/product/B01DFKC2SO/; Tim Moynihan, *Alexa and Google Home Record What You Say, But What Happens to that Data?*, WIRED (Dec. 5, 2016), https://www.wired.com/2016/12/alexa-and-google-record-your-voice/.

[28] *View Your Dialog History*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602040 (Alexa users can find a running list of their queries in the Alexa app by clicking Settings then History); *Google Home*, *supra* note 19 (Google users can find everything they've asked for by visiting myactivity.google.com while they are logged into their accounts.).

[29] *Google Home & Your Child's Google Account*, GOOGLE, https://support.google.com/families/answer/7521263?hl=en (follow "How non-Google apps work" then "Privacy"). Notably, both Amazon and Google warn that deleting audio may degrade user experience. It seems that even when audio is not shared, the transcription may be. Google states, "Google won't share audio recordings ... with [third party] apps. However, a transcript ... can be sent to these apps."

[30] *See* Moynihan, *supra* note 27.

[31] John M. Simpson, *Home Assistant Adopter Beware: Google, Amazon Digital Assistant Patents Reveal Plans for Mass Snooping*, CONSUMER WATCHDOG (Dec. 13, 2017), http://www.consumerwatchdog.org/privacy-technology/home-assistant-adopter-beware-google-amazon-digital-assistant-patents-reveal.

assistants can effectively function as command centers for the home by connecting a user's smart devices to one point.[32] These connections enable a consumer to simply speak a command to turn down the thermostat, turn off the lights, and even lock the door.[33] It is no wonder that consumers are adopting digital assistants more rapidly than any other recent consumer technology.[34] Sales of digital voice assistants are projected to double from 2017 to 2018, and research companies have predicted that this upward trend will continue.[35] An estimated 6.5 million voice-enabled devices were sold in 2015 and 2016,[36] close to 25 million sold in 2017, and a predicted 36 million will be sold in 2018.[37]

Partly contributing to the influx of connected devices into the digital universe was Amazon's release of its Alexa Skills Kit, which allowed developers to integrate Alexa voice technology into connected devices.[38] This type of integration is not limited to any industry and companies are rushing to be at the forefront of this innovation. Digital assistants are increasingly integrated into more and more products and are slowly establishing a constant presence across technologies.[39] For instance, LG's Family Hub refrigerator allows families to track their food consumption,

---

[32] *See, e.g.*, Don Clark, *The Race to Build Command Centers for Smart Homes*, WALL ST. J. (Jan. 4, 2015), https://www.wsj.com/articles/the-race-to-build-command-centers-for-smart-homes-1420399511 ("Nest and Wink offer software and Web services to orchestrate interactions among their own home gadgets and those made by other companies, which are churning out Internet-connected light bulbs, security cameras, entertainment devices, ovens, water heaters and washing machines.").

[33] *Id.*

[34] *See* CANALYS, SMART SPEAKERS ARE THE FASTEST-GROWING CONSUMER TECH; SHIPMENTS TO SURPASS 50 MILLION IN 2018 1 (Jan. 4, 2017), https://www.canalys.com/static/press_release/2018/press-release-040118-smart-speakers-are-fastest-growing-consumer-tech-shipments-surpass-50-million-2.pdf.

[35] *See id.* at 2.

[36] 2017 VOICE REPORT, *supra* note 13, at 4,.

[37] *See* ASSOCIATED PRESS, *Smart Speaker Sales More Than Tripled in 2017*, BILLBOARD (Dec. 28, 2017), https://www.billboard.com/articles/business/8085524/smart-speaker-sales-tripled-25-million-year-2017. *See also* 2017 VOICE REPORT, *supra* note 13.

[38] *See generally Amazon Introduces the Alexa Skills Kit – A Free SDK for Developers*, BUSINESS WIRE (June 25, 2015), http://www.businesswire.com/news/home/20150625005699/en/ (providing examples of developers integrating Alexa voice technology into their devices). *See* Romin Irani, *How to Get Started With Amazon's Alexa Skills Kit*, PROGRAMMABLEWEB (Aug. 2, 2016), https://www.programmableweb.com/news/how-to-get-started-amazons-alexa-skills-kit/how-to/2016/08/02.

[39] *See* Ankit Chawla, *CES 2018's Big Trend: A Voice Assistant in Every Corner of Your House*, GADGETS360 (Jan. 13, 2018), https://gadgets.ndtv.com/apps/features/ces-2018-voice-assistants-alexa-google-assistant-siri-cortana-roku-1799563.

track food expiration dates, and order groceries right from the kitchen.[40] Genesis, a division of Hyundai, was the first automaker to introduce Alexa-based connectivity to a car and has drawn awareness to its brand as a result.[41] Even the bathroom is becoming connected through Alexa-integrated mirrors, bathtubs, and toilets.[42]

C. PRIVACY CONCERNS RAISED BY DIGITAL ASSISTANTS

With the predicted widespread adoption of voice assistants, consumers can be tracked in nearly all aspects of their daily existence. Passive data-capture through smart devices typically found in the home (e.g., laptops, televisions, and toys) can lead to data collection about the most private aspects of individuals' lives, including data about a user's daily behavior patterns.[43] The incorporation of voice assistants into products such as cars, headphones, and smartwatches furthers this data collection by following users throughout almost all activities and enabling access to all kinds of information about the user.

Although voice assistants generally alert users when they are recording, this is not always the case. Scenarios where consumers are unaware that they are being recorded are plentiful, from defective devices that are always on, to innocent-looking connected items such as faucets.[44]

---

[40] Sean Buckley, *Amazon's Alexa Assistant is Coming to LG Refrigerators*, ENGADGET (Jan. 4, 2017), https://www.engadget.com/2017/01/04/LG-refrigerator-with-amazons-alexia/; see also Samsung *Family Hub Refrigerator*, SAMSUNG, https://www.samsung.com/us/explore/family-hub-refrigerator/refrigerator/.

[41] David Undercoffler, *Amazon Rolls out Alexa-Based Connectivity in Hyundai's Genesis*, ADVERTISING AGE (Aug. 18, 2016),

http://adage.com/article/digital/amazon-introduces-alexa-based-connectivity-hyundai-genesis/305504/.

[42] *See, e.g.*, *Verdera Voice Lighted Mirror with Amazon Alexa*, KOHLER,

https://www.us.kohler.com/us/Verdera-Voice-Lighted-Mirror-with-Amazon-Alexa/content/CNT131300006.htm (describing the "first-to-market bathroom lighted mirror available to consumers that has Amazon Alexa embedded").

[43] Christi Olson, *Just Say It: The Future of Search is Voice and Personal Digital Assistants*, CAMPAIGN (Apr. 25, 2016), https://www.campaignlive.co.uk/article/just-say-it-future-search-voice-personal-digital-assistants/1392459 ("Today's digital assistants are going beyond voice input, and are evolving to understand user intent and behaviors through available data . . .").

[44] *See, e.g.*, CONSUMER WATCHDOG, GOOGLE, AMAZON PATENT FILINGS REVEAL DIGITAL HOME ASSISTANT PRIVACY PROBLEMS 9, http://www.consumerwatchdog.org/sites/default/files/2017-12/Digital%20Assistants%20and%20Privacy.pdf (discussing that a bug in the Google Home Mini had randomly activated and recorded conversations despite the lack of users' commands to activate the device). *See also, e.g.*, Rich Brown & Molly Price, *Speak, Shower and Shave: Kohler Brings Smarts to Your Bathroom*, CNET (Jan. 5, 2018), https://www.cnet.com/news/speak-

For example, a Google Home Mini secretly recorded conversations without the user's knowledge, despite the wake word never being spoken.[45]

Furthermore, data collection is not always apparent to consumers because they may be unaware of the presence of voice assistants or may not expect persistent recording of conversations. Speech recognition services embedded in televisions and toys can be invisible and raise the question of whether consumers have adequately consented to recording.[46] For example, in 2012, hackers were able to gain access to users' Samsung Smart TVs and remotely turn on the built-in camera and microphone, surreptitiously listening to users without their knowledge.[47] Additionally, in 2015, Samsung warned users that "[s]ince the television is always listening for [their] voice[s] . . . every word is being captured and sent over the Internet."[48] However, even if a device owner is aware of the recording, a guest may lack such notice, which could violate that guest's reasonable expectation of privacy.[49] The devices are also not foolproof and sometimes will interpret words—that sound similar to the wake word—as commands to begin listening and recording. In one recent example, voice assistants all

---

shower-and-shave-kohler-brings-smarts-to-your-bathroom/ ("You can use an app or your voice to dispense a precise about of water from the Sensate faucet.").

[45] Samuel Burke, *Google Admits its New Smart Speaker was Eavesdropping on Users*, CNN (Oct. 11, 2017), http://money.cnn.com/2017/10/11/technology/google-home-mini-security-flaw/index.html. Google has since stated that the bug causing this issue was fixed.

[46] *See, e.g.*, Caitlin Hu, *Mattel's New "Hello Barbie" Records Kids' Voices and Sends the Intel Back to Corporate*, QUARTZ (Mar. 15, 2015), https://qz.com/362891/new-hello-barbie-records-kids-voices-and-sends-the-intel-back-to-mattel/ ("Pressing a button on [Barbie's] belt prompts the toy . . . to ask a question, and then record the response with an embedded microphone and transmits to cloud servers.").

[47] *See* Erica Fink & Laurie Segall, *Your TV Might be Watching You*, CNN (Aug. 1, 2013), http://money.cnn.com/2013/08/01/technology/security/tv-hack/index.html ("In the case of Samsung Smart TVs, iSEC researchers found that they could tap into the TV's Web browser with ease... [giving] hackers access to all the functions controlled by the browser.").

[48] David Goldman, *Your Samsung TV is Eavesdropping on Your Private Conversations*, CNN (Feb. 10, 2015), http://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/ ("You can opt-out of the SmartTV voice recognition feature.... But even if you opt out, your voice commands will still be captured. The SmartTV has a set of pre-programmed commands that it recognizes even if you opt out of voice recognition. Samsung will collect the text of those pre-programmed voice commands (though not your voice itself) and analyze how much you're using certain commands.") (noting that message quoted in the paragraph above was displayed briefly on the television and that the televisions continued to track users and collect data despite users opt-out selections).

[49] *See, e.g.*, CAL. PEN. CODE § 632(a) (explaining that California requires all parties to consent to the recording of a confidential communication).

over the United States were triggered to record conversations when a news reporter on television said the trigger word.[50]

Additionally, even when the device does not record audio data, it is unclear whether it tracks and collects text data based on its continuous passive listening.[51] Moving past the issue of surreptitious recording, voice assistants also collect other forms of consumer information, such as Internet searches and credit history information.[52] This data collection allows companies to compile and analyze the information to make eerily personal inferences about users that they might otherwise want to keep private, such as determining that a user is likely pregnant.[53]

In addition, consumers might be unclear about whether voice assistants are capable of only speech recognition or also voice recognition. While speech recognition involves the simple translation of voice to text, voice recognition involves using the consumer's unique voiceprint to identify the individual.[54] Furthermore, some digital assistants can analyze a user's voiceprint, the voice of an individual which, similar to a fingerprint, is unique.[55] Apple is developing this type of biometric tracing with voice recognition skills.[56] Facebook has gone even further and is currently

---

[50] Andrew Liptak, *Amazon's Alexa Started Ordering People Dollhouses after Hearing its Name on TV*, THE VERGE (Jan. 7, 2017), http://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse (explaining that this recent occurrence highlighted risks which may have been previously unanticipated but could result in widespread harm to consumers); *see* Goldman, *supra* note 48.

[51] For example, Samsung TVs microphones continued to collect text translations of users' commands, although they had stopped collecting audio recordings. Goldman, *supra* note 48.

[52] *Amazon Privacy Notice*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=468496

[53] *See, e.g.*, Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012,), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#517bc8e36668 (discussing how a father found out his daughter was pregnant based on Target coupons for baby items sent to his daughter).

[54] Lawrence Thompson, *Key Differences Between Speech Recognition and Voice Recognition*, STREETDIRECTORY, http://www.streetdirectory.com/travel_guide/139545/technology/key_differences_between_speech_recognition_and_voice_recognition.html ("While speech recognition is the process of converting speech to digital data, voice recognition is aimed toward identifying the person who is speaking.").

[55] *See, e.g.*, *Alexa FAQ*, *supra* note 19 ("Alexa uses recordings of your voice to create an acoustic profile of your voice characteristics. Alexa stores your voice profile in the Cloud and uses it to recognize you when you speak to Alexa. This allows Alexa to call you by name and personalize your experience.").

[56] *See* Shara Tibken, *Apple's Echo Rival Could See You with Built-In Camera*, CNET (May 27, 2016), https://www.cnet.com/news/apples-echo-rival-could-see-you-with-built-in-camera-

working on a digital assistant armed with both voice and face recognition skills.[57] For such biometric information, there are special privacy concerns related to breaches.[58] If such sensitive information is compromised by, for example, hacking, publishing, or sale to third parties, consumers cannot recover or replace it.

Even if voice assistants record only when prompted to do so by a user, what happens to the recording and data remains unclear. The information may be kept by the company and analyzed to improve product recommendations, but it can theoretically also be sold to third parties or even distributed freely over the web without users' consent or knowledge. Without strict laws prohibiting such behavior, or some sort of legal protection for users, this unsettling situation is not improbable. A review of privacy policies quickly demonstrates how little they protect and reveals how vague wording can render them meaningless.[59] In addition, hackers could publicly reveal private recordings, or text transcripts of those recordings.[60]

---

amazon-siri-facial-recognition/ ("The device would be 'self aware' and detect who is in the room using facial recognition technology. That would let the device automatically pull up a person's preferences, such as the music and lighting they like . . . ").

[57] *See* Mark Gurman & Ian King, *Apple Stepping up Plans for Amazon Echo-Style Smart-Home Device*, BLOOMBERG (Sep. 23, 2016), https://www.bloomberg.com/news/articles/2016-09-23/apple-said-to-step-up-plans-for-echo-style-smart-home-device-itfnod11 ("The device also has the ability to use facial recognition to identify users in real time. In addition, the virtual assistant can adapt how it behaves by sensing the user's mental state.")..

[58] Biometric information is regulated under some federal statutes, such as HIPAA. 45 C.F.R. § 164.514 (specifically including "[b]iometric identifiers, including finger and voice prints" in its scope.). In addition, some state statutes also regulate biometric information and limit its use in certain cases, such as commercial transactions. *See, e,g.*, Illinois Biometric Information Privacy Act, 740 ILL. COMP. STAT. ANN. 14/15 (sub-section (b) of the Illinois statute requires a person to be informed before any private entity collects that person's biometric information); TEX. BUS. & COM. CODE § 503.001 (same); FLA. STAT. § 1002.222 (agencies or institutions cannot collect or keep a student's, parent's, or student's sibling's biometric information).

[59] For example, many privacy policies state that they can collect information the user "provides" or "shares," without specifying what this term includes. Only examples of the type of information are listed, leaving the reader to wonder what the boundaries of the collection are and what type of information is not collected. *See, e.g.*, Eric Boughman, *Is There an Echo in Here? What You Need To Consider About Privacy Protection*, FORBES (Sept. 18, 2017), https://www.forbes.com/sites/forbeslegalcouncil/2017/09/18/is-there-an-echo-in-here-what-you-need-to-consider-about-privacy-protection/#588745bf38fd ("[A]s disclosed by Alexa's terms of use, if you access third-party services and apps through Alexa, Amazon (naturally) shares the content of your requests with those third parties. Amazon further discloses that data you provide may be stored on foreign servers. As such, U.S. Fourth Amendment protections may not apply.").

[60] *See, e.g.*, Andy Greenberg, *A Hacker Turned an Amazon Echo Into a "Wiretap"* WIRED (Aug. 1, 2017, 3:30 PM), https://www.wired.com/story/amazon-echo-wiretap-hack/ ("With just a few minutes of hands-on time, a hacker could turn an Echo into a personal eavesdropping microphone without leaving any physical trace.").

The important question has been raised regarding whether collected data about a user may later be used in harmful ways by third parties or government agents.[61] A recent case involved a request for an individuals' voice recordings collected by Amazon Alexa, showing that there is already interest in obtaining access to this information and signaling that such future requests may become common.[62] Insufficient regulations on access to this personal data could result in constant monitoring and could have a chilling effect on society.

Although voice assistants provide numerous benefits to consumers and create previously unheard-of opportunities, they also pose many risks and open the possibility that future generations will have no understanding of privacy.[63] The sense of security that one feels at home in one's bedroom may be overridden by voice assistants that are constantly on and listening to every word. Consumers must be wary of their privacy and actively strive to control the collection and use of their personal information.

Uniquely personal conversations are in danger of becoming the property of corporations interested in providing personalized ads and product recommendations.[64] Although some consumers will appreciate this personalization, users must necessarily be provided with more thorough and meaningful protections and understand what happens to their data in a world of always-on devices. Information might never be made private again once it is disclosed and becomes public knowledge.

But see Moynihan, *supra* note 27 ("The audio zipping from your home to Amazon and Google's data centers is encrypted, so even if your home network is compromised, it's unlikely that the gadgets can be used as listening devices. A bigger risk is someone getting hold of your Amazon or Google password and seeing a log of your interactions online.").

[61] *E.g.*, Jedidiah Bracy, *This Pacemaker Just Incriminated its Owner*, INT'L. ASS'N. OF PRIVACY PROF'LS (Feb. 7, 2017), https://iapp.org/news/a/this-pacemaker-just-incriminated-its-owner/ ("In its case against him, law enforcement obtained a warrant for all of the electronic data produced by his pacemaker — the data included his heart rate, pacer demand, and cardiac rhythms before, during, and after the time of the fire.").

[62] Christopher Mele, *Bid for Access to Amazon Echo Audio in Murder Case Raises Privacy Concerns*, N.Y. TIMES (Dec. 28, 2016), https://www.nytimes.com/2016/12/28/business/amazon-echo-murder-case-arkansas.html. The case was eventually dropped for unknown reasons.

[63] *See* Gregory L. White & Philip G. Zimbardo, *The Effects of Threat of Surveillance and Actual Surveillance on Expressed Opinions Toward Marijuana*, 111 J. SOC. PSYCHOL. 49, 59 (1980) (finding that "threat of surveillance exerts a powerful influence over behavior, beliefs, and feelings.").

[64] *See* Tom Smith, *Voice Assistants, Search and the Future of Advertising*, MARKETINGTECH (Sep. 4, 2017), https://www.marketingtechnews.net/news/2017/sep/04/voice-assistants-search-and-future-advertising/ ("consumers may be slightly reticent when it comes to inviting advertisers and brands into this personal space.").

While data collection through voice assistants is increasing in quantity because of growth in adoption rates, companies are using consumer data to create individual consumer profiles. Some of these companies that combine various sources of data, called data brokers, store billions of data elements on nearly every U.S. consumer.[65] Such a vast amount of data—spanning nearly all aspects of individuals' day-to-day lives based on these individuals' interaction with smart devices—has never before been available.[66]

"Big data" refers to the combination of nearly ubiquitous data collection and its use to make inferences and predictions.[67] Companies are no longer limited to collecting behavioral data from one device;[68] they can collect data from both connected devices and offline activities, such as credit card purchases—ultimately resulting in aggregated databases.[69] Consumers can be tracked across their connected devices, regardless of whether they provide personal information through a particular device.[70]

---

[65] Paul Boutin, *The Secretive World of Selling Data About You*, NEWSWEEK (May 30, 2016), http://www.newsweek.com/secretive-world-selling-data-about-you-464789

("[D]ata brokers are serving a growing clientele eager to know a person's ethnicity, spending habits, sexual orientation, and specific illnesses such as HIV, diabetes, depression or substance abuse. This information may be found directly in data broker records, or, increasingly, it may be predicted from other data. It's practically impossible for anyone to find all the information being passed around about themselves, or to correct it. As shady as it might sound, the entire industry is completely legal.").

[66] *See, e.g., id.* ("In the 1950s, credit agencies began creating scores on potential lenders that included factors, such as race, that were later banned by federal regulation.").

[67] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 2–3 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [hereinafter "WHITE HOUSE BIG DATA REPORT"].

[68] Justin Brookman et al., *Cross-Device Tracking: Measurement and Disclosures*, PROCEEDINGS ON PRIVACY ENHANCING TECH. 133, 134 (2017) https://petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf ("Originally, online behavioral data collection was limited to connecting users across multiples websites on one device. Today, advertising technology companies are finding ways to track users across devices as well. Consumers interact with more devices — and smarter devices — than ever before, including computers, smartphones, smart TVs and Blu-Ray players, gaming platforms, and Internet of Things devices.").

[69] WHITE HOUSE BIG DATA REPORT, *supra* note 67, at 5 ("The sources and formats of data continue to grow in variety and complexity. A partial list of sources includes the public web; social media; mobile applications; federal, state and local records and databases; commercial databases that aggregate individual data from a spectrum of commercial transactions and public records; geospatial data; surveys; and traditional offline documents scanned by optical character recognition into electronic form.").

[70] *See id.* ("Personal location data can come from GPS chips, cell-tower triangulation of mobile devices, mapping of wireless networks, and in-person payments.").

Even seemingly innocuous data can be used to infer personal details about consumers' daily activities.[71] Analysis and inferences through such data could be almost instantaneous.[72] This type of technology is still in its early stages, and various other privacy risks may be difficult to anticipate.

Lack of regulation of data collected through voice-controlled devices could cause significant problems by neglecting vast amounts of data already generated by consumers, which can then be used to harm these consumers.[73] In the words of one author, "[i]t's like willingly bugging your own home and hoping no one tunes in."[74]

III. EXISTING PRIVACY REGULATION

A. WHAT IS PRIVACY?

First, it is important to define just what the right to privacy means. Scholars have debated the concept of privacy for generations and continued disagreement still lingers over its scope and value; it remains an elusive term with no single definition.[75] Discussion of privacy as a legal right, as opposed to a moral right, began with the famous articulation of privacy as "the right to be let alone."[76] Since then, privacy has been posited to include, among other things, control over: "information about oneself," "freedom from surveillance," "freedom of thought," and "one's reputation."[77]

---

[71] MANAR SAFI ET AL., INFERENCE OF USER DEMOGRAPHICS AND HABITS FROM SEEMINGLY BENIGN SMARTPHONE SENSORS 1 (Oct. 3, 2016) https://www.ftc.gov/system/files/documents/public_comments/2016/10/00073-129193.pdf (discussing the use of unrestricted sensor data to "infer private details about the user, such as their daily schedules, income levels, and relationship status").

[72] WHITE HOUSE BIG DATA REPORT, *supra* note 67, at 5.

[73] Janna Anderson & Lee Raine, *The Internet of Things Will Thrive by 2025*, PEW RESEARCH CTR. (May 14, 2014), http://www.pewinternet.org/2014/05/14/internet-of-things/.

[74] Alex Cranz, *Amazon's Alexa is Not Even Remotely Secure and I Really Don't Care,* GIZMODO (Mar. 15, 2016), http://gizmodo.com/alexa-is-not-even-remotely-secure-and-really-i-dont-car-1764761117.

[75] Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1088–89, 1125 (2002) [hereinafter *Conceptualizing Privacy*].

[76] *See generally* William Prosser, *Privacy,* 48 Cal. L. Rev. 383, 389 (1960) (identifying four interests protected by privacy that laid the foundation for the four privacy torts widely used by states today: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) publicity placing another in false light; and (4) appropriation of another's name or likeness.). Another foundational article is Samuel Warren & Louis Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193-220, 193 (1890) (arguing that there is an individual right to privacy which is protected by the common law).

[77] *Conceptualizing Privacy*, *supra* note 75, at 1088.

Information privacy law has adopted the view of privacy as the right to control "the collection, use and disclosure of personal information."[78] This Note defines the right to privacy as the right to control the collection and dissemination of information about oneself.[79]

B. EXISTING REGULATION

The United States does not recognize a general fundamental right to privacy, and the Constitution does not explicitly mention privacy.[80] Consumer information in the U.S. is regulated by a fragmented system which applies different laws based on the industry and context of the information.[81] This sectoral approach, which applies various laws to each segment of the economy, contrasts with omnibus regulation adopted by many industrialized countries, which applies various laws largely without regard to the industry or the context.[82]

Various federal statutory laws in the U.S. address different privacy concerns. For example, the Children's Online Privacy Protection Act ("COPPA") governs data collected from children under the age of thirteen.[83] The Gramm-Leach-Bliley Act ("GLBA") regulates the collection and use of personal data by financial institutions.[84] The Fair Credit Reporting Act ("FCRA") addresses financial information relating to consumer credit.[85] The Health Insurance Portability and Accountability Act ("HIPPA") protects the privacy of health records.[86]

---

[78] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATIONAL PRIVACY LAW 2 (5th ed. 2015).

[79] *See* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 436 (1980).

[80] Despite this, an implied constitutional right to privacy has been found in certain areas. SOLOVE & SCHWARTZ, *supra* note 78, at # [2. Constitutional Law]. *But see* Charter of Fundamental Rights of the European Union, art. 8, 2012 O.J. (C 326) 391, 397 (explaining that, in sharp contrast, the European Union recognizes a basic right to privacy for all citizens; the Charter of Fundamental Rights of the European Union states, "everyone has the right to the protection of personal data concerning him or her.").

[81] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 586–87 (2014) [hereinafter *FTC and New Common Law of Privacy*].

[82] *Id.* at 604, 676.

[83] *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2012).

[84] *See* Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801–6809 (2012).

[85] *See* 15 U.S.C. § 1681b (2012).

[86] *See* 42 U.S.C. §§ 1320d-1 (2012).

1. FTC Regulation

The Federal Trade Commission ("FTC"), "an independent U.S. law enforcement agency charged with protecting consumers and enhancing competition across broad sectors of the economy,"[87] steps in to fill gaps in statutory protections. The FTC uses its broad authority to restrict "unfair or deceptive acts or practices" to protect consumer privacy.[88] Unlike the federal statutory laws, the FTC is not limited to specific sectors of the economy and its authority applies to most companies acting in commerce.[89] In addition, the FTC has the authority to enforce certain privacy laws, including those of COPPA,[90] HIPPA,[91] and Privacy Shield.[92] Armed with authority to enforce specific privacy laws and authority to regulate companies which fall outside sectoral regulation, the FTC is an important player in the U.S. privacy law landscape.[93]

The FTC's consumer protection authority derives from Section 5(a) of the Federal Trade Commission Act of 1914 ("FTC Act"), which prohibits "unfair or deceptive acts or practices in or affecting commerce."[94] "Unfair" acts or practices are those that "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or

---

[87] *About the FTC*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc [hereinafter *About the FTC*].

[88] 15 U.S.C. § 45(a)(1) (2012).

[89] Solove & Hartzog, *supra* note 81, at 609.

[90] FEDERAL TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2017 1 (https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf) [hereinafter *Privacy & Security Update: 2017*].

[91] U.S. DEP'T OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS., SHARING CONSUMER HEALTH INFORMATION?, 1 (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0219_sharing-health-info-hipaa-ftcact.pdf.

[92] *Privacy & Data Security Update: 2017*, *supra* note 90, at 6.

[93] Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. Rev. 2230, 2236 (2015) ("Today, the FTC [is] the broadest and most powerful data protection agency in the United States. No other agency has such a broad scope of power over so many different industries . . . [T]he FTC's scope covers nearly any for-profit entity that handles personal data. Except for a few small industry carve-outs, nearly every industry is subject to FTC enforcement power . . . .") [hereinafter *FTC Data Protection*].

[94] 15 U.S.C. § 45(a). Although the FTC's scope is not limited by industry, a few specific ones are carved out, including banks and air carriers. 15 U.S.C. § 45(a)(1).

to competition."[95] "Deceptive" acts or practices are those that involve a material misrepresentation, omission, or other practice that is likely to mislead a consumer acting reasonably under the circumstances.[96] This authority to regulate broad categories of unfair and deceptive acts is expansive and legislative history supports the conclusion this is intentionally so.[97] This wide-reaching authority allows the FTC to adapt to changing markets and take on the challenges presented by rapidly changing technology.

Certain elements must be present for an act to be deemed unfair or deceptive. To determine whether an act is unfair, three factors are considered: (1) substantial injury to consumers, (2) countervailing benefits to consumers or to competition, and (3) whether consumers can reasonably avoid injury.[98] This three-part test calls for a balancing of costs and benefits. *FTC v. Wyndham Worldwide Corporation* further clarified that although "unfairness claims generally involve actual and contemplated harms, they may also be brought on the basis of likely rather than actual injury. . . . and the FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs."[99]

On the other hand, to determine whether an act is deceptive, three different factors are considered: (1) existence of a misrepresentation or act, (2) which is likely to mislead a reasonable consumer, and (3) the act is material.[100] An act is material if it is "likely to affect the consumer's conduct or decision with regard to a product or service."[101] If the answer to this basic question is yes, then "the practice is material, and consumer injury is likely, because consumers are likely to have chosen differently but for the deception."[102] Materiality is also presumed in cases in which an express or

---

[95] 15 U.S.C § 45(n). *See also* FEDERAL TRADE COMM'N, *FTC Policy Statement on Unfairness*, December 17, 1980, https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness ("Unjustified consumer injury is the primary focus of the FTC Act . . . . By itself it can be sufficient to warrant a finding of unfairness.").

[96] FEDERAL TRADE COMM'N, *FTC Policy Statement on Deception*, October 14, 1983, https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf [hereinafter FTC Policy Statement on Deception].

[97] *FTC Data Protection*, *supra* note 93, at 2246–47. *See also Privacy & Security Update: 2017*, *supra* note 90, at 1 ("This broad authority allows the Commission to address a wide array of practices affecting consumers, including those that emerge with the development of new technologies and business models.").

[98] 15 U.S.C. § 45(n).

[99] FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 246 (3d Cir. 2015).

[100] FTC Policy Statement on Deception, *supra* note 96, at 1–2.

[101] *Id.* at 1.

[102] *Id.*

implied statement exists, but only if such statement goes to the central character of the product or services.[103]

In contrast with unfairness analysis, deception analysis does not require that actual injury occur, and risk of consumer harm alone is sufficient.[104] Furthermore, if there is a material misleading statement which is false, deception analysis presumes that prohibiting such a statement will result in a net benefit to consumers, and a further cost-benefit analysis to determine alternative courses of action is not necessary.[105] Deception is considered so harmful to consumer decision-making and to the functioning of the marketplace that no countervailing benefits are presumed, rendering a cost-benefit analysis unnecessary in such cases.[106]

2. FTC's Goals

FTC's overarching goal in regulating is to ensure that innovation is maximized while also "protect[ing] consumers' personal information and ensur[ing] that they have the confidence to take advantage of the many benefits of the ever-changing marketplace."[107] This difficult task requires balancing consumers' interest in protecting the privacy of personal information and business interests in utilizing information to drive innovation and competition.[108] As stated by the FTC, this involves "[w]orking to protect consumers by preventing anticompetitive, deceptive, and unfair business practices, enhancing informed consumer choice and public understanding of the competitive process, and accomplishing this without unduly burdening legitimate business activity."[109]

The FTC's use of its toolkit is guided by a reasonableness standard, with its enforcement largely based on industry standards and consumer expectations.[110] As a result of its reliance on standards developed by the free market, many of the enforcement cases brought by the FTC have involved

---

[103] *Id.* at 5.

[104] *See id.*; *see also* FTC Policy Statement on Unfairness, *supra* note 95.

[105] FTC Policy Statement on Deception, *supra* note 96, at 1–2.

[106] *Id.* at 5.

[107] *Protecting Consumer Privacy*, FEDERAL TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy (last visited Mar. 26, 2017) [hereinafter *Protecting Consumer Privacy*].

[108] The FTC states its vision as "A vibrant economy characterized by vigorous competition and consumer access to accurate information." *About the FTC*, *supra* note 87.

[109] *Id.*

[110] Solove & Hartzog, *supra* note 81, at 661.

business practices that have deviated significantly from industry norms.[111] The FTC also looks to the industry in producing reports and setting forth guidance for companies.[112] These reports examine industry trends and provide guidelines for businesses by recommending certain privacy and data security practices.[113] The FTC's publications, including reports, educational materials, and press releases, provide insight into what the FTC believes to be reasonable practices.[114] As such, businesses often review these publications to guide their privacy and data security measures.[115]

C. CURRENT PRIVACY REGULATION IS INADEQUATE

As mentioned above, no specific federal laws apply to data collected by digital voice assistants and regulation of this vast data falls mainly to the FTC. The FTC uses its broad Section 5 unfairness and deception authority to regulate voice assistant data by enforcing the promises made in the applicable privacy policies of such devices. Additionally, because COPPA applies to data regardless of the industry, instead of looking to whether the information was collected from a child under the age of thirteen, COPPA

---

[111] *See FTC Data Protection*, *supra* note 93, at 2269–70.

[112] *What We Do*, FEDERAL TRADE COMM'N, https://www.ftc.gov/about-ftc/what-we-do ("The FTC develops policy and research tools through hearings, workshops, and conferences. We collaborate with law enforcement partners across the country and around the world to advance our crucial consumer protection and competition missions. And beyond our borders, we cooperate with international agencies and organizations to protect consumers in the global marketplace."). *See also Reports*, FEDERAL TRADE COMM'N, https://www.ftc.gov/policy/reports ("The FTC produces a number of reports that examine antitrust and consumer protection trends.").

[113] *FTC and the New Common Law of Privacy*, *supra* note 81, at 625–26. *See also Commission and Staff Reports*, FEDERAL TRADE COMM'N, https://www.ftc.gov/policy/reports/policy-reports/commission-and-staff-reports (showing a listing of FTC reports).

[114] *FTC and the New Common Law of Privacy*, *supra* note 81, at 625–26.

[115] *Id.* at 626 ("The FTC materials do not have the same force and effect of a settlement; they are merely statements by the FTC about how it interprets its regulatory authority and Section 5, and how it might choose to enforce in the future. The FTC might change course or not enforce in that manner. The FTC might attempt an enforcement but be challenged by a company in court. Thus, FTC materials do not appear to be as strongly precedential as settlements, but they create incentives for companies to comply, and thus serve as a softer kind of rule."). *See also id.*, at 585–86 (discussing that businesses "parse and analyze the FTC's settlement agreements, reports, and activities" to help ensure compliance with privacy law) ("Those involved with helping businesses comply with privacy law—from chief privacy officers to inside counsel to outside counsel—parse and analyze the FTC's settlement agreements, reports, and activities as if they were pronouncements by the Chairman of the Federal Reserve. Thus, in practice, FTC privacy jurisprudence has become the broadest and most influential regulating force on information privacy in the United States—more so than nearly any privacy statute or common law tort.").

also applies to voice assistant data in some cases.[116] Although a few state laws apply to voice assistant data, this Note concentrates on FTC regulation of such technology.

III. FTC FLAWS & FIXES

A. FTC REGULATION SHORTCOMINGS

Although the FTC has attempted to use its toolkit to protect consumer privacy, steps taken thus far have proven insufficient in a world of increasingly connected devices and immense amounts of sensitive data. The FTC's goal to maximize innovation and ensure consumer confidence in the marketplace[117] has been far from realized considering the present world of vast data. To the contrary, consumers have expressed discontent with current privacy protections and surveys show they lack notice, feel powerless to protect their privacy, and have increasingly lost trust in the market.[118]

Voice assistants pose additional challenges to effective privacy regulation because they continuously listen to everything. Numerous cases involving such voice-enabled devices reveal that consumers are not adequately protected. For example, "Hello Barbie," a doll with a built-in microphone, recorded children without consent and then used this data to analyze preferences and send targeted advertising.[119] Similarly, Internet connected toys My Friend Cayla and i-Que Intelligent Robot recorded children without consent and collected personal information including children's names and locations.[120] Google secretly installed software that

---

[116] *See FTC Provides Additional Guidance on COPPA and Voice Recordings*, FEDERAL TRADE COMM'N (Oct. 23, 2017), https://www.ftc.gov/news-events/press-releases/2017/10/ftc-provides-additional-guidance-coppa-voice-recordings.

[117] *Protecting Consumer Privacy*, *supra* note 107 (stating its goal to "balance the privacy interests of consumers with innovation that relies on information to develop beneficial new products and services").

[121] *See* Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security, and Surveillance*, PEW RESEARCH CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

[119] Iain Thomson, *Hello Barbie: Hang on, this Wi-Fi Doll Records Your Child's Voice? What Could Possibly Go Wrong?*, THE REGISTER (Feb. 19, 2015), http://www.theregister.co.uk/2015/02/19/hello_barbie/.

[120] *See* Complaint and Request for Investigation, Injunction, and Other Relief, Electronic Privacy Information Center, Dec 6, 2016, https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf.

activated microphones on computers, allowing it to eavesdrop on conversations.[121] Samsung SmartTVs also were factory-configured with voice recognition software that recorded a user's every word and sent this information to a third party.[122] Unfortunately, these instances of voice recognition, enabling devices to eavesdrop on and record unknowing consumers, are neither isolated nor uncommon.[123]

Existing FTC regulation does not adequately address such intrusions and its actions do not promote consumer interests. None of the cases discussed above resulted in any action by the FTC against the eavesdroppers.[124] However, even when the FTC does take enforcement actions to protect privacy, its actions may not lead to increased privacy protections for consumers. This discrepancy between the intended effect of specific FTC regulation and the actual outcome can be seen through a closer look at two recent enforcement actions. Both actions concerned the surreptitious collection of personal data and fairly represent most FTC enforcement actions.

An enforcement action was brought against Lenovo, Inc., one of the world's largest computer manufacturers, for unfair and deceptive practices.[125] The action involved Lenovo's sale of laptops preloaded with ad software that tracked user activity continuously and collected sensitive information, including Social Security numbers and financial account information.[126] Lenovo sold around 750,000 laptops preinstalled with this malware, which secretly collected the information without consumer notice

---

[121] Samuel Gibbs, *Google Eavesdropping Tool Installed on Computers Without Permission*, THE GUARDIAN (Jun. 23, 2015), https://www.theguardian.com/technology/2015/jun/23/google-eavesdropping-tool-installed-computers-without-permission.

[122] David Goldman, *Your Samsung TV is Eavesdropping on your Private Conversations*, CNN (Feb. 10, 2015), http://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/index.html; *In the Matter of Samsung Electronics Co. Ltd., Complaint, Request for Investigation, Injunction, and Other Relief*, ELECTRONIC PRIVACY INFORMATION CTR., Feb. 24, 2015, https://www.epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf.

[123] *See generally* Complaint, U.S. v. VTech Electronics Limited, (N.D. Ill. Jan. 8, 2018), (No. 1:18-cv-114), https://www.ftc.gov/system/files/documents/cases/vtech_file_stamped_complaint_w_exs_1-8-18.pdf (discussing a complaint arising under COPPA and the FTC Act); T.C. Sottek, *The Xbox One Will Always be Listening to You, in Your Own Home (Update)*, THE VERGE (May 21, 2013), https://www.theverge.com/2013/5/21/4352596/the-xbox-one-is-always-listening ("The new Xbox will always be listening to you, even when it's turned off.").

[124] It is possible that the FTC has investigated these cases but has not taken any public action.

[125] Complaint at 7, In the Matter of Lenovo Inc., No. C-4636, https://www.ftc.gov/system/files/documents/cases/1523134_lenovo_united_states_complaint.pdf.

[126] *Id.* at 2.

or consent and created a serious security risk of unauthorized access to personal information.[127] The FTC settled the case, with Lenovo agreeing that it would refrain from making misrepresentations about the software, obtain consumers' affirmative express consent before preinstalling software and offer an opt-out option, implement a security program to assess vulnerabilities, and undergo periodic third party security assessments.[128]

In another recent case, the FTC brought an action for unfair and deceptive conduct against Vizio, Inc.,[129] one of the world's largest smart television manufacturers.[130] Vizio sold over 11 million televisions with pre-installed software that collected second-by-second viewing data about consumers without their knowledge or consent, including information collected from their cable boxes and even through airwaves.[131] This information was then sold to third parties and compiled into a large database of consumers' information, such as their sex, income, and marital status.[132] This action ended in a stipulated court order, with the FTC imposing penalties almost identical to those against Lenovo, including a prohibition on future misrepresentations, affirmative consent before future data collection and an option to revoke consent, deletion of improperly collected data, and implementation of a data privacy program with periodic third party audits.[133] As a condition of the settlement, Vizio agreed to pay a monetary penalty of $2.2 million.[134]

Both cases are fair and representative examples of actions that the FTC has brought: egregious privacy violations that are offensive to any conception of consumer protection. Both involved the pervasive collection of sensitive and intimate information about consumers who had no reason

---

[127] *Id.* at 3.

[128] Order at 6–8, In the Matter of Lenovo Inc. Order, No. C-4636, https://www.ftc.gov/system/files/documents/cases/152_3134_c4636_lenovo_united_states_decision_and_order.pdf [hereinafter *Lenovo* Order].

[129] Complaint at 1, Federal Trade Commission v. Vizio Inc., (D.N.J. Feb. 13, 2017) (No. 2:17-cv-00758-SRC-CLW, 2017 WL 7000553), https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf [hereinafter *Vizio* Complaint].

[130] *VIZIO Licenses Digital TV Patent Portfolio to SONY*, VIZIO, https://www.vizio.com/news/VIZIOLicensesDigitalTVPatentPortfoliotoSONY.

[131] *Vizio* Complaint, *supra* note 130, at 4, 8–9.

[132] *Id.* at 5–6.

[133] Stipulated Order at 3, 5, 7, Federal Trade Commission v. Vizio Inc., (D.N.J. Feb. 13, 2017) (No. 2:17-cv-00758-SRC-CLW, 2017 WL 7000553), https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf [hereinafter *Vizio* Order].

[134] *Id.* at 8–9.

to suspect their information was vulnerable to collection by concealed software or invisible tracking technology in a laptop or television. Yet the companies appeared to escape mostly unscathed—the most burdensome conditions of the settlements included periodic reporting requirements, establishment of a privacy program, and compliance monitoring.[135] Vizio was additionally subjected to a monetary penalty, but this number is laughable considering that Vizio not only profited from the sale of 11 million televisions but also sold licenses, on a per television basis, for the personal information of about 11 million consumers.[136] While it is difficult to estimate the profit gained from license sales, the $2.2 million penalty was likely a trivial price to pay in relation to the transaction's total revenues.[137]

Although these enforcement actions are necessary to stop unscrupulous consumer data collection without notice or consent, they are a long shot from the FTC's mission of protecting consumers' personal information. Once data is collected, consumer privacy has already been violated and FTC action only prohibits further violations. In addition to this, the large number of recent data breaches also demonstrates the shortcomings of privacy protections. Notably, 57 million driver and rider account information was stolen from Uber,[138] 1 billion and 500 million Yahoo accounts were hacked on separate occasions,[139] and the personal information of about 143 million consumers was compromised in an Equifax data breach.[140]

This Note argues that the FTC does not adequately protect privacy because its regulation suffers from various procedural flaws. Although enforcement under Section 5 of the FTC Act requires careful analysis of the elements of unfairness and deception, such an analysis is missing or inapposite in many cases. Further, the dual mission of protecting consumers while promoting competition creates additional factors that must be considered each time the FTC undertakes enforcement. Such an analysis requires consideration of factors such as consumer preferences and

---

[135] *See Lenovo* Order, *supra* note 129; *Vizio* Order, *supra* note 152.

[136] *Vizio* Complaint, *supra* note 130.

[137] Solove & Hartzog, *supra* note 81, at 605 (explaining that the FTC is limited in the amount of penalty it can enforce).

[138] Mike Isaac, et al., *Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data*, N.Y. TIMES (Nov. 21, 2017), https://www.nytimes.com/2017/11/21/technology/uber-hack.html.

[139] Vindu Goel & Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.

[140] Tara Siegel Bernard, et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

expectations, an understanding of the current competition landscape, and a grasp of the current state of information privacy, among other factors. However, the FTC often acts without adequately evaluating all the relevant facts or balancing its two goals. Absent careful consideration and analysis of these factors, regulation is unlikely to result in efficient or optimal outcomes.

B. PROPOSED REGULATION

This Note argues that the FTC must properly consider and weigh the relevant factors to result in more effective privacy protections while maximizing innovation. Enforcement actions must be reasonably calculated to meet the FTC's goals. This Note examines issues in current regulation and sets forth proposed changes. First, the FTC should evaluate the market at the time of regulation and account for any existing economic incentives. It should further tailor enforcement to correct any existing market failures and aim to restore effective competition. Second, the FTC should move toward ex-ante rather than ex-post regulation. Instead of allowing the industry to create inefficient norms, it should lead the industry to use standards that balance countervailing interests. In addition, instead of stepping-in only when privacy has been violated, it should proactively act to prevent harm. Third, the FTC should move away from unprincipled actions and carefully analyze the factors and effects of such actions when regulating. In determining how to regulate, it should consider both short-term and long-term costs and effects of the action.

Adopting these proposals will allow the FTC to use calculated actions to achieve its desired changes in the marketplace. Undertaking a careful analysis—before bringing enforcement actions, setting forth guidelines, or taking any other actions—will help lead to more efficient outcomes. This is necessary in the current market because of the immense amount of increasingly personal consumer data. To keep up with quickly changing technology, FTC regulation must be more efficient and effective. The anticipated widespread adoption of technology such as digital voice assistants highlights the issues with the current regulation of data privacy and suggests that stronger protections are necessary. These assistants are anticipated to be in every home, and businesses are already taking steps to incorporate them into their offices. In the sections below, this Note discusses why current FTC regulation must be changed and what effect those changes would have on consumer privacy and competition.

1. Evaluating the Market

This Note argues that when regulating businesses, the FTC often fails to account for marketplace factors and consider how its enforcement actions will play out in the existing economic landscape. Because of this oversight, its regulation has led to undesirable consequences for consumer privacy and the overall marketplace. Specifically, the FTC does not properly account for the incentives created by the marketplace and it does not consider how its regulation may affect these incentives. Regulatory actions do not operate in a vacuum, and factors such as economic or social incentives must be considered to understand the actual effect of such actions on the market. Further, any regulatory action carries with it the implication that such action was necessary because of some compelling reason to justify intervention in the market. Part of this reason is that the current market is inefficient and suffers from numerous market failures. Therefore, any FTC regulation must clearly set forth the reasons that justify its intervention and strive to correct the market failures that necessitated regulation. This Part discusses these proposals in more detail, identifying shortcomings of current regulation and explaining how the changes would lead to more desirable results in the marketplace.

a. Correct Market Failure

Properly functioning markets are efficient at allocating goods and services to their "highest and best uses" through the interaction of supply and demand.[141] However, specific conditions must be present for markets to function in this way. Market failure occurs when the market fails to allocate resources efficiently because of some problem in the market, such as asymmetric information, when there is not enough information to make an informed choice, or externalities: when one party's decisions affect a third party.[142]

FTC regulation is based in part on the ideal of self-regulation, which relies on the market to account for all factors and result in a favorable outcome.[143] However, to be self-regulating, the market must be an efficient market and be able to correct problems through the pull of supply and

---

[141] SUSAN E. DUDLEY & JERRY BRITO, REGULATION: A PRIMER 65 (2012), https://www.mercatus.org/system/files/RegulatoryPrimer_DudleyBrito_0.pdf.

[142] *See id.* at 12–14.

[143] *See* Solove & Hartzog, *supra* note 81, at 598.

demand.[144] Although imposing penalties when companies act unfairly or deceptively may be effective in some situations, the FTC should aim to correct marketplace defects and inequities in order to result in more meaningful privacy protections. Restoring market efficiency can result in less intervention by the FTC, as the market will be able to correct itself to reflect the most favorable outcomes and more long-lasting protections.

The FTC strives to create a "vibrant economy characterized by vigorous competition and consumer access to accurate information."[145] However, the current marketplace suffers from information failure as consumers are unaware of the scope and amount of personal information that companies collect and use. Voice assistants can collect information invisibly, including biometric data such as a user's voiceprint.[146] Cross-device tracking is complex, and the FTC itself has admitted that consumers are unaware of just how much personal information about them is collected.[147] Privacy policies are vague and do not generally clarify consumer confusion.[148] Consumers are deprived of the chance to consider their information privacy in making decisions in the marketplace if they do not know their televisions are listening to and recording every word, or that their children's toys are recording their conversations and targeting them for advertisements. An informed consumer would avoid such companies and demand from the marketplace stricter privacy protections, but an unaware consumer is unable to push the market in this way. Negative externalities also exist in the current market.[149] For example, companies can collect a large amount of personal consumer data and sell it for a profit, but

---

[144] *See, e.g.*, DUDLEY & BRITO, *supra* note 142, at 3 ("The USDA's Agricultural Marketing Service . . . . sets grade standards and purchases fruits and vegetables 'to correct supply and demand imbalances,' which keeps prices higher than they otherwise would be.").

[145] *About the FTC*, *supra* note 87.

[146] *See* 45 C.F.R. § 164.514 (specifically including "[b]iometric identifiers, including finger and voice prints" in its scope.).

[147] *See* Craig Timberg, *Brokers Use 'Billions of Data Points to Profile Americans*, WASH. POST (May 27, 2014) https://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19_story.html?utm_term=.6f4f79806926 ("The extent of consumer profiling today means that data brokers often know as much — or even more — about us than our family and friends," FTC Chairman Edith Ramirez said in a statement. "It's time to bring transparency and accountability to bear on this industry on behalf of consumers, many of whom are unaware that data brokers even exist.") (internal citations omitted).

[148] Boughman, *supra* note 59 ("[A]s disclosed by Alexa's terms of use, if you access third-party services and apps through Alexa, Amazon (naturally) shares the content of your requests with those third parties. Amazon further discloses that data you provide may be stored on foreign servers. As such, U.S. Fourth Amendment protections may not apply.").

[149] DUDLEY & BRITO, *supra* note 142, at 12, 78–80.

any resulting harm falls on the consumer if such information is used by identity thieves. This is a classic negative externality, where the company has no reason to consider the risks of data collection which fall on the consumer.

Data collection by a company, like pollution, results in a negative externality,[150] because the sale of data results in loss of consumer privacy, a cost not borne by the company. Companies collecting data generally do not bear the costs of privacy harms, therefore creating a negative externality.[151] For example, without regulation, a manufacturer emitting pollutants does not have to bear the cost of that pollution.[152] Because this cost is passed on to a third party, the manufacturer has little incentive to minimize pollution. Similarly, when a company sells data about an individual, the harm (i.e., loss of privacy) is borne not by that company but by the individual. Companies can use collected data to customize targeted advertisements or sell the data to data brokers, leading to increased profits.[153] Therefore, without regulation, the company has no incentive to minimize such harms, but it has strong economic incentives, in the form of increased revenue, to continue this practice. Just as manufacturers will pollute over the most efficient limit, companies will collect data over the most efficient limit as well. In addition, without regulation, companies that limit their data collection and sale are generally put in a worse position than competitors that do not limit this practice.

These marketplace failures can and should be addressed by the FTC. Information failure can be corrected by educating consumers by putting out more information and guides both online and in print.[154] Further, companies should be required to disclose the types of information they collect. Audio recordings and biometric voice data collection should be set forth in a clear fashion on voice assistants. Companies that have breached consumer privacy and inappropriately collected information should reach out to consumers over email or via their websites and alert consumers of the situation. Educated consumers can weigh all the factors in deciding whether

---

[150] *See id.*

[151] *Id.* at 12 (A negative externality occurs when a party making a decision does not bear the full cost of that decision, and harmful effects or costs are imposed on a third party.).

[152] *Id.* at 78–80.

[153] *See* Boutin, *supra* note 65.

[154] DUDLEY & BRITO, *supra* note 142, at 107–08 ("[S]ocial media and other Internet technologies lower the cost of group formation and collective action so that citizens will be better able to educate themselves about the regulations that affect them and to take action to make their voices heard.").

to give up certain privacy protections, therefore setting the supply and demand line at an acceptable level. Furthermore, negative externalities should be allocated to the company, requiring it to account for the imposed costs in its operations instead of ignoring costs. Even disclosure of data by an individual can act as a negative externality on other individuals' privacy.[155] For example, information collected by a digital assistant could include conversations between the device owner and another individual who was unaware of the recording, or household members' discussions that reveal intimate details about a neighbor or a friend. Collected information may also include data which could be generalized across a certain group of people and allow inferences about the group, revealing personal information at a high probability of accuracy.[156] Therefore, similar to clean air protections, privacy protections of such data could be viewed as a benefit to society.

b. Create Better Incentives and Stronger Deterrents

This Note argues that in taking any action to regulate privacy, the FTC should strive to change existing marketplace incentives to help achieve its desired outcome. For example, if economic considerations push companies to behave in ways that compromise consumer privacy, any FTC regulation should reshape incentives to push companies to be more privacy-conscious. A shortcoming of current FTC regulation is that it does not properly account for existing marketplace incentives and does not consider the real-world effect of its regulation. The FTC can more effectively regulate if it takes into account market incentives and takes steps to shift them in the desired direction.

First, the FTC must examine and understand the forces that shape the current market. Voice assistants are a good example. Since most current privacy laws do not reach companies that make voice assistants, [157]

---

[155] *See* Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J. L. POL'Y FOR INFO. SOC'Y 425, 429 (2011) ("The idea is that disclosure of information by some people can reveal information about other people, to their detriment."); Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 28 (2006) ("When a web site gathers and sells personal information about one of its users, . . . they cause that individual to lose a degree of privacy. This cost is borne by the user and is external to the business. It is a negative externality.") [hereinafter*Inner Environment*].

[156] WHITE HOUSE BIG DATA REPORT, *supra* note 67, at 7–8.

[157] *But see* Mark Harris, *Virtual Assistants Such as Amazon's Echo Break US Child Privacy Law, Experts Say*, THE GUARDIAN (May 26, 2016), https://www.theguardian.com/technology/2016/may/26/amazon-echo-virtual-assistant-child-privacy-law (companies that sell virtual assistant devices, like Amazon, are subject to COPPA).

companies can collect and use information largely without any restraints. The FTC does enforce privacy policies and can step in if a company fails to meet its own promises. Companies are guided by self-interest and selling consumer data is incredibly profitable.[158] Further, competitors may push companies that were originally privacy-conscious to lower protections and disclose sensitive consumer information to third parties. For example, feeling marketplace pressure, Amazon has stated that it may start disclosing voice assistant transcripts to third parties; its rival Google has already begun doing so.[159] Amazon may lose money if it continues to be more protective of consumer privacy and is therefore incentivized to disclose this information. However, Amazon and other companies may be driven by other incentives, such as building consumer trust and maintaining a good reputation, that lead them to remain privacy-conscious.[160] Yet companies must keep up with the fast pace of technology and are motivated to come up with new products and gain market share as quickly as possible. For example, car maker Genesis gained widespread publicity after becoming the first to integrate voice assistants into cars.[161] In an environment of stiff competition and great payoffs for companies that make it to the finish line first, any extra time spent on proper security measures may lead to lost profits because of late entry into the market.[162] Thus, absent baseline security guidelines that even out the playing field for companies and ensure that corners are not cut in ensuring data security, companies may lose profits

---

[158] *See The Value of Data 2015: Consequences for Insight, Innovation & Efficiency in the U.S. Economy*, DATA AND MKTG ASSOC., https://thedma.org/advocacy/data-driven-marketing-institute/value-of-data/ (discussing a finding that the "Data-Driven Marketing Economy (DDME) contributed nearly 1 million jobs to the United States in 2014 and added $202 billion in revenue to the U.S. economy.").

[159] Rob LeFebvre, *Amazon May Give Developers Your Private Alexa Transcripts*, ENGADGET (Jul. 12, 2017), https://www.engadget.com/2017/07/12/amazon-developers-private-alexa-transcripts/.

[160] Nick Ismail, *The Financial Impact of Data Breaches is Just the Beginning*, INFORMATION AGE (Jan. 8, 2018), http://www.information-age.com/data-breaches-financial-impact-123470254/ (stating that reputational damage is "[o]ne of the biggest impacts following a data breach").

[161] David Undercoffler, *Amazon Rolls out Alexa-Based Connectivity in Hyundai's Genesis*, ADVERTISING AGE (Aug. 18, 2016),

http://adage.com/article/digital/amazon-introduces-alexa-based-connectivity-hyundai-genesis/305504/.

[162] Yet the expense and delay might be worth it. *See* Heidi Maher, *Building a Business Case for a Data Privacy Program*, LAW.COM (Jan. 23, 2017), https://www.law.com/corpcounsel/almID/1202777417516/Building-a-Business-Case-for-a-Data-Privacy-Program-/ ("Even a modest breach of 30,000 records at a small business or startup can cost more than $4.6 million.").

if they spend extra time on protecting privacy.[163] Therefore, many economic incentives in the current market induce companies to be less cautious in their privacy and security measures. Companies do not have strong enough reasons to be more privacy-conscious unless countervailing forces shift these incentives.

Considering the foregoing factors, current FTC regulation is insufficient. The Vizio case (above) shows that enforcement actions do not sufficiently deter companies from harming consumer privacy. Even when monetary fines are imposed, they are generally small and companies may view them as the cost of doing business.[164] Also, fines may not prevent future companies from selling data for profit and paying the price later. Weighed against vast sums of money that companies make from collecting, using, and sharing data, the relatively small economic price of infringing individual privacy rights tends to push companies to maximize profit and engage in privacy-harming conduct.

In the absence of sufficient monetary disincentives or nonmonetary deterrents, companies will act in self-interest and continue to increase profits at the cost of consumer privacy. Although enforcement actions also impose other requirements on companies that have engaged in unfair or deceptive conduct—such as periodic reporting requirements and establishing privacy programs—these conditions do not sufficiently deter companies.[165] Although a more detailed analysis is required to evaluate the effects of these conditions, periodic reporting requirements that aim to prevent privacy breaches likely do not impose a substantial cost on companies.[166] The fact that all companies, regardless of the size or the

---

[163] *See, e.g.*, Steven Bellovin, *Security Costs Money. So – Who Pays?*, CIRCLEID (May 17, 2017), http://www.circleid.com/posts/20170517_security_costs_money_who_pays/ ("Computer security costs money. It costs more to develop secure software, and there's an ongoing maintenance cost to patch the remaining holes. Spending more time and money up front will likely result in lesser maintenance costs going forward, but too few companies do that.").

[164] *But see* David Ellis, *How Much Does a Data Breach Cost Your Organization?*, SECURITYMETRICS BLOG (Oct. 2016), http://blog.securitymetrics.com/2016/10/-how-much-does-a-data-breach-cost.htlm ("Some organizations believe dealing with a data breach might be better than dealing with the difficulties of [regulatory] compliance. Unfortunately, they don't realize how much damage a data breach can inflict on a business.").

[165] *See, e.g.*, Natasha Lomas, *Uber Agrees to 20 years of Privacy Audits to Settle FTC Data Mishandling Probe*, TECHCRUNCH (Aug. 15, 2017), https://techcrunch.com/2017/08/15/uber-agrees-to-20-years-of-privacy-audits-to-settle-ftc-data-mishandling-probe/.

[166] *See* Larry Ponemon, *The Cost of Privacy Safeguards*, TECHTARGET (Jan. 17, 2008), http://searchfinancialsecurity.techtarget.com/news/1294347/The-cost-of-privacy-safeguards (according to an IBM-sponsored study conducted by the Ponemon Institute, "[s]pending on privacy initiatives among the [44 U.S.-based multinational] organizations surveyed varied from approximately $500,000 to about $22 million annually.").

severity of the privacy breach committed and the size of the breaching company, are subject to the same or similar conditions in post-violation consent decrees also points to the fact that the punishments are not economically tailored to discourage unfair privacy practices. Further, establishing a privacy program should not be a "punishment" for companies that have already violated consumer privacy. Instead, it should be a baseline protection required of any company dealing with large amounts of personal consumer information. Settlement agreements or consent orders prohibit companies from acting unfairly or deceptively in the future, which is the equivalent of a slap on the wrist and a scolding. Because enforcement actions do not provide enough force to adequately deter companies from engaging in privacy violating conduct, companies might view the procedure of FTC settlements as a license to breach consumer privacy until the FTC catches them and orders them to stop.

Recently, the FTC brought an enforcement action against Nomi Technologies, a company that placed sensors in retail stores to track consumers and provide stores with consumer traffic data.[167] The action involved Nomi's privacy policy, which stated that consumers could opt out of being tracked by Nomi's website and from retailer stores.[168] However, Nomi allowed customers to opt out only via its website, and the FTC alleged that this practice was misleading.[169] The case was ultimately settled and Nomi entered into a 20-year consent order prohibiting Nomi from further misrepresenting consumers' privacy options.[170] Notably, although the FTC alleged that Nomi's failure to provide notice to consumers that they were being tracked was false or misleading,[171] the final order did not require Nomi to alert consumers of this fact going forward.[172]

This Nomi settlement highlights the inverted marketplace incentives that result from FTC actions. The FTC in this case attempted to protect privacy by making sure that companies follow through on keeping their promises regarding consumer privacy policies. However, as this example

---

[167] Complaint, In the Matter of Nomi Techs., Inc. (Aug. 28, 2015), 132-3251, 2015 WL 5304114 https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf [hereinafter Nomi Complaint].

[168] *Id.* at 2 (noting that the privacy policy stated that Nomi would "[a]lways allow consumers to opt out of Nomi 's service on its website as well as at any retailer using Nomi's technology.").

[169] Nomi Complaint, *supra* note 168, at 2–3.

[170] Decision and Order, In the Matter of Nomi Techs., Inc., 2015 WL 5304114 at *2, https://www.ftc.gov/system/files/documents/cases/150902nomitechdo.pdf [hereinafter Nomi Decision and Order].

[171] Nomi Complaint, *supra* note 168, at 3.

[172] *See* Nomi Decision and Order, *supra* note 171.

demonstrates, because the FTC did not require Nomi to institute a proper notice system alerting consumers of the tracking device, Nomi could comply with the settlement simply by taking out its promise to provide any opt-out mechanism at all. In this case, Nomi was not required to set forth a detailed privacy policy, provide notice, or offer opt-out choices.[173] Rather, Nomi was simply asked to stop acting in a false or misleading manner and subjected to some limited reporting requirements.[174]

This example makes clear that absent a proper reward and penalty system, incentives in the marketplace result in counterproductive outcomes. A company that takes the steps to post a privacy policy and offers an opt-out choice but is later punished because of these actions is likely to serve as a cautionary tale for other companies. Companies attempting to steer clear of an FTC enforcement action could simply refuse to offer any notice and choice at all, considering that any promises they make may be used against them. Thus, incentives shift in a way that harms customer privacy, as companies shy away from making any promises or allowing any opt-out choices.

To ensure stronger privacy protections, the FTC must change the existing incentives in the marketplace. The FTC should implement both stronger incentives to protect consumer information and stronger deterrents for privacy breaches, including: disgorgement of improper profits, deletion of improperly collected data, establishment of baseline protections, reputational risk, and responsibility for consumer data. Economic incentives which guide companies to collect, use, and sell consumer data because enforcement actions are not a sufficient deterrent.[175] Disgorgement of improper profits from unfairly or deceptively collected information would create a strong disincentive for this act. Although companies could greatly profit from consumer information, they would also face an equivalently significant risk in losing these profits if caught. Further, companies should be required to delete improperly collected data if it was obtained unfairly or deceptively. Companies would not be as willing to invest in collecting consumer data if there was a risk that this data would later be forcibly deleted. Thus, companies would have an increased incentive to be more privacy-conscious and ensure fair and truthful data collection.

Some reputational risk should be at stake for companies that violate consumer privacy. Companies are motivated to protect their reputations and

---

[173] *See id.*

[174] *Id.* at 2–3.

[175] *See, e.g.*, Lomas, *supra* note 166.

ensure consumer trust to drive business. Currently, companies are not required to admit any wrongdoing when they enter settlement agreements or consent orders.[176] Even when companies have acted unfairly or deceptively, reputational costs may not be incurred if consumers do not find out about it. The FTC should require companies to admit fault or publicly announce unfair or deceptive conduct because reputational risk can be a powerful incentive for companies to be conscious of consumer privacy and can strongly deter violations.[177] Although companies are necessarily concerned with monetary incentives, adding reputational risk will shift incentives so that a company acting in self-interest will be more inclined to protect consumer privacy. Companies will be less inclined to violate privacy, as a breach may result in damage to company goodwill, lead to consumer resentment, and result in lost profits.[178] Also, companies should be held responsible for how collected consumer data is later used. This will help counteract the competitive pressure to freely give out consumer information. For example, a company that shares transcripts or audio of conversations with a third party should require that the third party implement privacy protections and security measures before giving out such data. This small requirement of third parties will result in a company's more careful data sharing. Thus, these proposed changes would create incentives and disincentives in the market which lead companies to better protect privacy.

c. From Ex Post to Ex Ante

In light of the rapidly changing marketplace, increasing amounts of data, and higher risk of data breaches, the FTC should reconsider its use of an ex post approach to regulating privacy.[179] Although the industry develops quickly and consistently poses new challenges for privacy regulation, the FTC falls behind and steps in to correct harms only after they have already

---

[176] Brady Dale, *FTC Slaps the Wrist of Tax Prep Service After 8,800 Customers' Data Breached*, OBSERVER (Aug. 30, 2017), http://observer.com/2017/08/ftc-taxslayer/ ("Traditionally, when the FTC signs a consent agreement with a company, it doesn't admit nor deny wrongdoing. By entering into a consent order, the FTC is agreeing not to take the company to court for its failure to protect its members.").

[177] *See* Ismail, *supra* note 161.

[178] See *Latent Effects of the Recent Target Data Breach On The US Economy*, BRAVATEK, http://bravatek.com/latent-effects-of-the-recent-target-data-breach-on-the-us-economy/ (discussing that Target's data breach resulted in "business disruption costs," consumers' increased "uneasiness about using credit and debit cards," but arguing that "the cost that is perhaps hardest to quantify is the loss of business goodwill.").

[179] Solove & Hartzog, *supra* note 81, at 598.

occurred. This approach is unacceptable in the current marketplace of increasing data collection, which is poised to grow exponentially. To keep up with technology and increasing amounts of data, the FTC must take more firm strides towards its goal of protecting consumer privacy. By waiting until issues arise before it steps in, the FTC fails to take a stance or effect a change in consumer privacy. Clinging to its goal to allow the market to regulate itself and enforce industry standards, the FTC fails to see that current industry standards do not provide an adequate level of privacy protection. Further, existing conditions do not allow for a self-regulating free market.

In contrast with current regulation, which looks backwards to stop existing violations, the FTC should utilize its unique flexibility to look forward by preventing predictable harms. Section 5 regulation of unfair and deceptive practices is intentionally broad, and the FTC is tasked with utilizing this flexibility to "address a wide array of practices affecting consumers, including those that emerge with the development of new technologies and business models."[180] The FTC has a duty to use this authority to carry out its mandate of consumer protection in light of the increasing amount and increasing sensitivity of data in the market.

Instead of using industry standards to guide its actions, this Note argues that the FTC should step in and guide the market towards stronger privacy protections. Although reluctance to intervene in a free market or impose regulatory costs on companies is understandable, such action is necessary here. Current industry standards insufficiently protect privacy, and enforcing such standards does not promote consumers' interests. Industry standards are significantly shaped by self-interested companies which either did not consider privacy or do not have compelling reasons to protect consumer privacy. The current state of the industry reveals that consumers are unhappy with the state of privacy, feel that they do not have enough control over what information is collected, and feel that they do not know enough about the scope of data collection.[181] Privacy breaches are slowly becoming the norm, rather than the exception, as major companies

---

[180] *Privacy and Security Update: 2017*, *supra* note 90, at 1.

[181] Madden & Rainie, *supra* note 121.

including Yahoo,[182] Equifax,[183] and Uber[184] are being hacked, compromising information about millions of consumers. Enforcing industry standards when these are the industry norms only validates privacy-harming practices and normalizes such behavior.

Privacy policies are developed by the industry and are the norm for consumer privacy. However, such policies are intentionally vague, do not discuss the full scope of data collection and use, and avoid making any promises as any promises could be enforced against the company. Further, the FTC practice of bringing enforcement actions only against the most egregious offenders gives time for other privacy violations to become widespread.

Further, without setting meaningful boundaries for acceptable privacy policies, enforcing a company's own promises against itself simply pushes that company to act defensively and use self-preservation as the main driver behind its policy. Even when privacy policies are posted, companies have an incentive to be as vague as possible to avoid making any promises that could be used against the company later. On the other hand, companies may be incentivized to make broad statements encompassing all types of data collection and use, which minimizes the risk that a company will later be held liable for having overstepped any of its own privacy policy limits. Privacy policies are increasingly shorter and less detailed because of an attempt to make them simpler and easier to comprehend, but this results in vague policies which are unhelpful to consumers.[185] Studies consistently show that consumers are not sufficiently notified because they do not read privacy policies and even when they do, consumers do not understand them.[186] It is no wonder that a privacy policy in a self-regulatory system is unlikely to protect consumer privacy in any meaningful way.

---

[182] Selena Larson, *Every Single Yahoo Account was Hacked – 3 Billion in* All, CNN (Oct. 4, 2017), http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html.

[183] Seena Gressin, *The Equifax Data Breach: What to Do*, FTC (Sep. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

[184] Julia Carrie Wong, *Uber Concealed Massive Hack That Exposed Data of 57M Users and Drivers*, THE GUARDIAN (Nov. 22, 2017), https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack.

[185] Solove & Hartzog, *supra* note 81, at 674 ("Increasingly, privacy policies are shorter and much less detailed in an effort to make them quick to read and simple to understand. The problem is that these policies really do not say much.").

[186] *See, e.g.*, Florencia Marotta-Wurgler, *Does Contract Disclosure Work?*, 168 J. INST. THEO. ECON. 20, 94, 95 (2012).

Not only do such broad and vague privacy policies fail to adequately protect consumers, but they also impose increased regulatory costs on companies complying with privacy laws, with no offsetting benefit to consumers or the market. Research has consistently reported consumer dissatisfaction with privacy policies as they exist now.[187] Thus, the FTC's action taken towards its goal of preserving customer privacy while driving innovation is not effective unless it takes other steps to create boundaries.

Instead of following industry standards, the FTC should require that certain information be disclosed in privacy policies. For example, regarding voice-controlled digital assistants, a required disclosure should inform consumers about what information is collected during the listening state and what information is recorded, including whether the device is capable of voice identification or collects biometric voice prints. The FTC should set forth baseline standards of minimum requirements for disclosure. Privacy policies should be required of every company that collects and uses data. This would also give the FTC more teeth since its authority is based on enforcing promises but companies are not actually required to make any promises. Further, companies should be required to follow minimum security standards. Recent data breaches demonstrated that many companies' inadequate data protection measures. As data becomes increasingly personal and increasingly aggregated, more sensitive and detailed information could be disclosed by breaches. Once disclosed, injured parties cannot get the information back and consumer privacy cannot be restored to the state it was. Further, setting baseline standards will help companies understand their obligations and put all companies on a more level playing field regarding how much money and time to spend before releasing products.

Instead of punishing egregious privacy violators, the FTC should do more to prevent such violations ex ante. To this end, it can utilize its wide toolkit to create disincentives for privacy breaches and create rules and norms for privacy protections. The FTC's current enforcement actions are a necessary step, but they are not strong enough to deter companies from breaching privacy. Instead, the FTC should change the punishment for companies that breach privacy by increasing the risk of reputational harm to violators, requiring disgorgement of improper profits and deletion of

---

[187] *See, e.g.*, GINA PINGITORE, ET AL., MCGRAW HILL FINANCIAL: GLOBAL INSTITUTE CONSUMER CONCERNS ABOUT DATA PRIVACY RISING: WHAT CAN BUSINESS DO? (Oct. 29, 2013), http://www.jdpower.com/sites/default/files/Consumer_Concerns_Data_Privacy.pdf ("Results of this research show that consumers' concerns about data privacy and ownership have increased across the past three decades and remain high.").

improperly collected data, and increasing monetary penalties. Instead of imposing standard settlement provisions on all companies regardless of the type of privacy breach, the FTC should tailor each violator's settlement requirements based on the extent of the privacy harms and include provisions aimed at remedying that company's past behavior. Companies should also be required to disclose privacy breaches and educate consumers about their behavior. This would help slowly even out the informational asymmetry between consumers and companies. Such provisions in settlements would create stronger disincentives for companies and help prevent privacy violations, slowly shaping industry standards to become more privacy protective.

d. Fix the Flawed Analysis

Although the FTC has brought hundreds of privacy and data security cases, its regulation rarely includes an analysis of the relevant elements for each cause of action. Analysis requires insight into consumer preferences and expectations, an understanding of the current competition landscape, and a grasp of the current state of information privacy, among other considerations. The FTC should use these factors to help determine what actions will affect its two-fold goal.

The FTC must conduct a careful analysis of the balance between potential risks and benefits of any regulation.[188] This must include an analysis of any costs and benefits to consumers and companies, accounting for any effects on both privacy and innovation. Even if the FTC determines that the current state of affairs results in a marketplace that satisfactorily protects consumers and promotes innovation, an analysis must be conducted to support the decision to take or forego action. The decision to forego action is an action in itself which confirms that no regulation is necessary because the market is operating efficiently. Further, any future FTC reports should contain comprehensive discussions about the potential costs and benefits of the proposed guidelines and employ data to back up these claims.

---

[188] *See, e.g.*, U.S. ENVT'L. PROTECTION AGENCY OFFICE OF AIR AND RADIATION, THE BENEFITS AND COSTS OF THE CLEAN AIR ACT FROM 1990 TO 2020 1 (2011), https://www.epa.gov/sites/production/files/2015-07/documents/fullreport_rev_a.pdf ("Section 812 of the 1990 Clean Air Act Amendments established a requirement that EPA develop periodic reports that estimate the benefits and costs of the Clean Air Act (CAA). The main goal of these reports is to provide Congress and the public with comprehensive, up-to-date, peer-reviewed information on the Clean Air Act's social benefits and costs, including improvements in human health, welfare, and ecological resources, as well as the impact of CAA provisions on the US economy.") [hereinafter *Benefits and Costs of the Clean Air Act*].

The FTC currently employs a flawed process of regulation because it fails to perform an accurate cost-benefit analysis to determine how to effectively balance consumer protection and innovation. While in some of its actions the FTC sets forth relevant considerations for a cost-benefit analysis, it does not meaningfully evaluate the costs and benefits of both privacy and innovation. The FTC's limited use of this analysis contributes to the disparity between the goals of its enforcement and its actual effects on the market. This frequent lack of balancing also stems from the fact that the FTC has thus far brought enforcement cases involving the largest harms to consumers, such as in *Lenovo* and in *Vizio*, in which obvious inequities between the interests render such an analysis superfluous.

Further, a cost-benefit analysis is implied in the FTC's goal to protect consumers without stifling innovation. Thus far, FTC actions suggest a failure to consider relevant marketplace factors and adequately weigh competing interests. For example, a 2017 FTC staff report, *Cross-Device Tracking,* considers the issues raised by online advertisers' practice of tracking consumer activity across various connected devices and sets privacy guidelines.[189] Although the report takes a step in the right direction by identifying risks and benefits to both consumers and advertisers, it does not go on to evaluate how these interests weigh against each other.[190] Rather, the FTC simply pronounces recommendations without providing an explanation or support for this action. For instance, after the FTC asserts that it is trying to "keep pace with new technological developments"[191] it goes on to recommend that companies follow "longstanding privacy principles" set forth in 2009.[192] The FTC itself noted significant changes in consumer tracking since the 2009 privacy principles, including new, more pervasive and intrusive forms of tracking.[193] Despite this, the FTC did not evaluate whether its recommendations would benefit consumers or promote

---

[189] *See generally* FEDERAL TRADE COMM'N, CROSS-DEVICE TRACKING (2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf (concluding that consumers benefit from cross-device tracking but should be informed about and equipped to control tracking and recommending that entities provide transparency, consumer control, and heightened security over tracking and data collection) [hereinafter CROSS-DEVICE TRACKING REPORT].

[190] *Id.*

[191] *Id.* at i.

[192] *Id.* at ii.

[193] *See, e.g., id.* at 1–2 ("onboarding" occurs when "companies combine offline and online data to create detailed consumer profiles.")

innovation, and it also failed to consider any other possible courses of action.[194]

These privacy principles were largely carried over from its 2012 report, *Protecting Consumer Privacy in an Era of Rapid Change*.[195] This report outlined best practices for companies with the goal of increasing consumer protection and set forth guiding privacy principles, including "privacy by design,"[196] "simplified consumer choice,"[197] and "transparency."[198] The recommendations have been carried over to many subsequent reports, which have used these same principles as guidelines.[199] In addition, enforcement actions have also adopted these principles by implementing them into consent orders.[200]

The *2012 Privacy Report* itself is defective in that it fails to provide evidence to support the adopted framework and lacks analysis of whether these principles would benefit consumers while still promoting innovation. A major shortcoming in this report's analysis is that the FTC did not

---

[194] *See id.*

[195] FEDERAL TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter 2012 PRIVACY REPORT].

[196] *Id.* at 22, 24, 26–27, 29 ("Privacy by design" urges companies to incorporate privacy protections into products and services at every stage of their development, which includes creating reasonable security, setting reasonable limits to their data collection, implementing reasonable retention and disposal policies, and maintaining accuracy.").

[197] *Id.* at 38–39. ("Consumer choice" needs to be provided only when the use of the data is inconsistent "with the context of the transaction," inconsistent with the company's relationship with the consumer, or "specifically authorized by law.").

[198] *Id.* at 71 (finding notice to consumers should "be clearer, shorter, and more standardized," and consumers should have "reasonable access" to data maintained about them.").

[199] *See e.g.*, FEDERAL TRADE COMM'N, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD 37–44 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (recommending the adoption of the notice and choice model without providing any actual estimates of its costs or benefits) [hereinafter INTERNET OF THINGS REP.].

[200] *See, e.g.*, Stipulated Order for Permanent Injunction and Civil Penalty Judgment at 7–8, U.S. v. InMobi Pte. Ltd., (N.D. Cal. Jun. 22, 2016) (No. 3:16-cv-3474), https://www.ftc.gov/system/files/documents/cases/160622inmobistip.pdf; TERRELL MCSWEENY, COMMISSIONER, FED. TRADE COMM'N, REMARKS AT TECNATION 2016: UNITED STATES CHAMBER OF COMMERCE (Sept. 20, 2016), https://www.ftc.gov/system/files/documents/public_statements/985773/mcsweeny_-_tecnation_2016_9-20-16.pdf ("[InMobi] underscores the core principles that the FTC's privacy program is founded on: transparency, choice (including affirmative express consent before retroactive changes are made, meaningful choices around collection of sensitive information) and context (collection and use consistent with consumer expectation).").

consider other courses of action, and, similarly to its subsequent reports, the report was significantly influenced by public comments and discussions between stakeholders.[201]

Evidence does not sufficiently show that these principles have promoted consumer privacy. Despite the lack of support or a measured analysis of how and whether such guidelines impact consumers and companies, the FTC continues to advocate adopting these principles. Continued use and application of these principles as guidelines in subsequent reports creates a domino effect on future regulations. Although technology is constantly changing and becoming increasingly advanced, the FTC does not engage in meaningful analysis to determine whether these principles are still applicable or effective given these developments.[202]

Surveys of consumers find that they lack notice, feel powerless to protect their privacy, and are increasingly losing trust in markets.[203]

Effective privacy regulation must necessarily consider both the immediate and long-term costs and benefits of such regulation, as well as the regulation's potential future effects. Once proposed guidelines are adopted, the FTC must consider the future of the marketplace.[204] Despite some harms to innovation, such as slower development of new technologies, the risks to privacy are great. Without this analysis, consumers could end up living in a world dominated by innovative technologies that simplify all aspects of life yet lack any privacy protections to the extent that everything is open to the public eye. Although such an example is extreme, it reminds us of what we stand to lose at the cost of faster innovation.

---

[201] *See* 2012 PRIVACY REPORT, *supra* note 197, at 72 ("The final privacy framework set forth in this Report reflects the extensive record developed through the Commission's privacy roundtables as well as the over 450 public comments received in response to the proposed framework issued in December of 2010."); *id.* at 2 ("The roundtables brought together stakeholders representing diverse interests to evaluate whether the FTC's existing approach to protecting consumer privacy was adequate in light of 21st Century technologies and business models.").

[202] THOMAS M. LENARD & PAUL H. RUBIN, THE ANTITRUST SOURCE, THE FTC AND PRIVACY: WE DON'T NEED NO STINKING DATA, (Oct. 2012), http://www.americanbar.org/content/dam/aba/publishing/antitrust_source/oct12_lenard_10_22f.authcheckdam.pdf ("Because the Commission and Staff Reports provide virtually no new data or analysis, they are seriously deficient as a foundation for new policy recommendations . . . . Without such analysis, there is no way of knowing whether a particular regulatory action will improve or reduce consumer welfare.").

[203] Madden et al., *supra* note 137.

[204] *See, e.g.*, *Benefits and Costs of the Clean Air Act*, *supra* note 189, at 1–2 ("[T]his report incorporates a sophisticated economy-wide model to estimate effects of the CAAA on such measures as GDP, prices, and consumer welfare.").

The marketplace is quickly changing because of the rapid adoption of new technologies which are likely to shape consumer values and expectations. Just as the FTC's current principles need to be reevaluated and updated to keep up with these developments, any future framework will continuously require adjustment. The FTC must engage in regular periodic evaluations of how its actions affect the delicate balance between consumer protection and innovation. To move closer to its goal of a "vibrant economy characterized by vigorous competition and consumer access to accurate information,"[205] the FTC should monitor the market to ensure it is operating efficiently. This can be done through periodic assessments of market participants and conditions, specifically noting the existence of any undue influence on the market such as informational failure and negative externalities, among other factors.[206] This evaluation will guide the FTC in conducting a balancing test and determining when it should act to correct any imbalances in the market.

IV. CONCLUSION

The current privacy framework is overdue for modernization. The fast-paced adoption of innovative technologies, such as voice-controlled assistants, has resulted in increased efficiency and task simplification. However, voice-controlled devices and related technologies also highlight the shortcomings of current privacy protections and the urgent need to strengthen consumer protection. Never before has so much data been available. The exponential increase in data collection presents a pressing problem which needs to be addressed before an irreversible, substantial harm takes place. Any regulation must account for both sides of the argument and engage in a comprehensive analysis of the anticipated effects on both the market and consumer privacy protections. Until such regulation is enacted, the FTC should continue to act as the privacy protector of consumers. Importantly, any balancing of interests under this proposed amended privacy framework must include a consideration of the future costs and benefits. Research, data, and careful analysis must take place to fully embrace the power of FTC regulation.

---

[205] *About the FTC*, *supra* note 87.

[206] *See generally Guide to Antitrust Laws*, FEDERAL TRADE COMM'N, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws (noting that the FTC already employs similar analyses in connection with its antitrust authority).