BIG BROTHER IS LISTENING TO YOU: DIGITAL EAVESDROPPING IN THE ADVERTISING INDUSTRY

DACIA GREEN[†]

ABSTRACT

In the Digital Age, information is more accessible than ever. Unfortunately, that accessibility has come at the expense of privacy. Now, more and more personal information is in the hands of corporations and governments, for uses not known to the average consumer. Although these entities have long been able to keep tabs on individuals, with the advent of virtual assistants and "always-listening" technologies, the ease by which a third party may extract information from a consumer has only increased.

The stark reality is that lawmakers have left the American public behind. While other countries have enacted consumer privacy protections, the United States has no satisfactory legal framework in place to curb data collection by greedy businesses or to regulate how those companies may use and protect consumer data. This Article contemplates one use of that data: digital advertising. Inspired by stories of suspiciously well-targeted advertisements appearing on social media websites, this Article additionally questions whether companies have been honest about their collection of audio data. To address the potential harms consumers may suffer as a result of this deficient privacy protection, this Article proposes a framework wherein companies must acquire users' consent and the government must ensure that businesses do not use consumer information for harmful purposes.

INTRODUCTION

"Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment."[1]

[†] Duke University School of Law, J.D. May 2018; B.A. in Economics & History, Vanderbilt University, May 2015. I would like to thank Professor Rebecca Rich for her guidance, the editors of *Duke Law & Technology Review* for their tireless work, and all of the people with whom I have had many conversations about this topic for months.

[1] GEORGE ORWELL, NINETEEN EIGHTY-FOUR 5 (1949).

Three decades late, George Orwell's *Nineteen Eighty-Four* has turned from dystopian prediction to ingenious depiction. While not every ominous detail accurately describes modern society, Orwell's fiction approximates reality now more than ever. Orwell imagined a world in which the political party in power manipulated history, individual thought became an imprisonable offense, and technology was always listening. Propaganda wrangled with facts so much that literal opposites became synonyms: War became Peace, Freedom became Slavery, and Ignorance became Strength.[2] Citizens were routinely reminded that their thoughts were not their own, that their acts were not unseen. In almost every sense of the word, privacy ceased to exist.

In an age where political leaders manipulate the truth[3] and even government officials vocalize concerns of surveillance,[4] Orwell's story seems disturbingly familiar. Fears of constant surveillance induce us to identify our modern "Big Brother," the figure always watching. Like Orwell, many believe that Big Brother is the Government's moniker alone. While an ordinary citizen might have been called paranoid for covering his private web camera a few years ago, warnings from several sources[5] confirm that the Government can use our own video technologies to monitor us. But who else might be always watching—or always listening?

---

[2] *See id.* at 6.

[3] *See* Michiko Kakutani, *Why '1984' Is a 2017 Must-Read*, N.Y. TIMES, (Jan. 26, 2017), https://www.nytimes.com/2017/01/26/books/why-1984-is-a-2017-must-read.html?mcubz=1 (describing parallels between Orwell's novel and "today's 'post-truth' era").

[4] Edward Snowden, a former Central Intelligence Agency (CIA) employee, leaked several documents disclosing global surveillance in 2013. Barton Gellman, *Edward Snowden, After Months of NSA Revelations, Says His Mission Is Accomplished*, WASH. POST (Dec. 23, 2013), https://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html?noredirect=on&utm_term=.e06833c4a1c7. Similarly, Former Director of the Federal Bureau of Investigations (FBI), James Comey, admitted to placing tape over his personal computer's webcam to ward off potential hackers. Martin Kaste, *Why the FBI Director Puts Tape Over His Webcam*, NAT'L PUB. RADIO (Apr. 8, 2016, 4:43 PM), https://www.npr.org/sections/thetwo-way/2016/04/08/473548674/why-the-fbi-director-puts-tape-over-his-webcam.

[5] *See* Kim Zetter, *How to Keep the NSA from Spying Through Your Webcam*, WIRED (Mar. 13, 2014, 6:30 AM), https://www.wired.com/2014/03/webcams-mics/. Snowden is one such source. In 2014, Snowden leaked that the National Security Agency (NSA), a federal intelligence agency, can use a plug-in to spy on people through their computer cameras. *Id.*

Big Brother is not the only "big" thing we have to worry about now. Businesses know more about their customers than ever before thanks to immense data sets known as "Big Data." Big Data, which is "data that exceeds the processing capacity of conventional database systems,"[6] enables businesses to understand and predict consumers' habits in various areas, from their dating preferences to their shopping habits. Armed with information many consumers are unaware they have even provided, many businesses then attempt to influence consumers' decisions through advertisements targeted at specific individuals.[7] The massiveness of the data collected, and the value in collecting as much data about every consumer as possible,[8] points to an unsettling conclusion: Big Brother is no longer just the government. Big Brother is a corporation.

Neither tracking consumers nor advertising based on data collected are new phenomena. However, the Internet has made it possible for businesses to conduct both of these activities on an unprecedented scale. The Internet enables businesses to induce customers to try new products with more success than they previously had.[9] Since businesses are able to share the data they collected with other businesses, or even with the government, the number of ways Big Data can be used is virtually endless.

Many consumers are aware that companies collect *some* data. Websites like Facebook and Twitter allow their users to "opt-out" of behavioral, or interest-based advertisements.[10] Those users who wander

---

[6] Edd Wilder-James, *What is Big Data?*, O'REILLY (Jan. 11, 2012), https://www.oreilly.com/ideas/what-is-big-data. Although its name alludes to its size, Big Data is known for more than just the technical amount of data it conglomerates. *See infra* Part I.

[7] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all.

[8] Wilder-James, *supra* note 6 ("Big data analytics can reveal insights hidden previously by data too costly to process, such as peer influence among customers, revealed by analyzing shoppers' transactions, social, and geographical data.").

[9] *See e.g.*, HOWARD BEALES, NETWORKING ADVERT. INITIATIVE, THE VALUE OF BEHAVIORAL TARGETING 11–12 (2010), *available at* https://www.researchgate.net/profile/Howard_Beales/publication/265266107_The_Value_of_Behavioral_Targeting/links/599eceeea6fdcc500355d5af/The-Value-of-Behavioral-Targeting.pdf (finding that targeted advertising increases the rates at which online media participants "click through" delivered advertisements and increases the percentage of clicks that culminate in sales).

[10] *See How Can I Adjust How Ads Are Targeted to Me Based on My Activity Off of Facebook?*, FACEBOOK: HELP CENTER, https://www.facebook.com/help/568137493302217 (last visited Apr. 8, 2018);

into accounts' privacy settings thus know that their searches on other parts of the web can affect the advertisements they receive while using an unrelated website.[11] But even some seemingly informed consumers do not know just *how much* data is collected.

Similarly, not all consumers are aware of the source of that data. Many advertisements show consumers products or services that the consumer has recently researched. But oftentimes, the source of the data that leads to a particular advertisement being targeted at a consumer is not so easily identifiable. For example, an individual surfing the Internet on her smartphone could scroll through her Instagram application and suddenly receive an advertisement for a product she has merely talked about in person. Unwilling to reduce such an event to mere coincidence, the suspicious consumer might then wonder, "Is my phone listening to me?"[12]

This hypothetical Instagram user would not be the first person to report such a story. As one journalist notes, "The internet is rife with anecdotal stories about digital eavesdropping. Many people feel that conversations they've had within earshot of their phones have been used to tailor advertising."[13] Online forums, including the community website Reddit, are full of users sharing tales of advertisements appearing after in-

---

Your Privacy Controls for Personalized Ads, TWITTER: HELP CENTER, https://help.twitter.com/en/safety-and-security/privacy-controls-for-tailored-ads (last visited Apr. 24, 2018). Facebook and Twitter do not provide this feature out of their own benevolence. Rather, these companies allow users to opt-out of behavioral advertisements to adhere to the Self-Regulatory Principles for Online Behavioral Advertising, which were established by the Digital Advertising Alliance (DAA), a coalition of advertising and marketing companies based in the United States. *See* DIG. ADVERT. ALL., SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 1 (2009), *available at* http://digitaladvertisingalliance.org/sites/digital/files/DAA_files/seven-principles-07-01-09.pdf (detailing the self-regulatory principles). Membership in the DAA is not mandatory.

[11] *See How can I adjust how ads are targeted to me based on my activity off of Facebook?*, *supra* note 10.

[12] *See* Lee Koo, *Coincidence or Is My Phone Listening to Me?*, CNET: PHONES FORUM (May 13, 2016, 5:14 PM), https://www.cnet.com/forums/discussions/coincidence-or-is-my-phone-listening-to-me/ (claiming "ads being targeted at me for products or issues that I'm sure I had only spoken about – and have NOT Googled/searched for them on my PC or phone.").

[13] Simon Hill, *Is Your Smartphone Listening to Everything You Say? We Asked the Experts*, DIGITAL TRENDS (Jan. 15, 2017, 3:10 AM), https://www.digitaltrends.com/mobile/is-your-smartphone-listening-to-your-conversations/.

person conversations referencing the advertised products.[14] Although websites such as Facebook have denied that they listen to people's conversations,[15] the number of individuals with similar experiences keeps growing.[16]

With the development of voice assistants[17]—such as Apple's Siri, Amazon's Alexa, and Microsoft's Cortana, which are "always

---

[14] *See* Koo, *supra* note 12; *see also* Zoe Kleinman, *Is Your Smartphone Listening to You?*, BBC NEWS (Mar. 2, 2016), http://www.bbc.com/news/technology-35639549 (referencing stories appearing on Reddit); *see also* Neville, *Facebook iPhone Listening into our Conversations for Advertising TEST*, YOUTUBE (July 19, 2016), https://www.youtube.com/watch?v=U0SOxb_Lfps (a viral video—showing an experiment where a couple repeatedly talked about cat food around a smartphone to trigger advertisements on Facebook—posted in several Reddit threads that sparked thousands of comments in discussion).

[15] *See, e.g.*, *Facebook Does Not Use Your Phone's Microphone for Ads or News Feed Stories*, FACEBOOK: NEWSROOM (June 2, 2016), https://newsroom.fb.com/news/h/facebook-does-not-use-your-phones-microphone-for-ads-or-news-feed-stories/. However, considering that the FTC accused Facebook of making misrepresentations to users about consumer privacy in 2011, perhaps such statements should be taken with a grain of salt. *See* Press Release, Federal Trade Commission, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promise (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep (discussing the FTC's eight-count complaint against Facebook and a proposed settlement order to protect consumer privacy going forward).

[16] For more examples of people who suspect companies have been listening to their conversations, see Kleinman, *supra* note 14. Kleinman claims that she was speaking with her mother about a fatal motorcycle accident in which a family friend had been involved. *Id.* The next time Kleinman used the search engine on her phone, the deceased's name and a few other words about the accident populated in the suggested text underneath the search bar. *Id.* Kleinman shares a few similar stories, including one in which a friend's boyfriend complained of his very first migraine and the friend was then followed on Twitter by a migraine support group. *Id.*

[17] Khari Johnson, *Adobe Launches Voice Analytics for Siri, Alexa, and Other Intelligent Assistants*, VENTUREBEAT (June 29, 2017, 6:00 AM), https://venturebeat.com/2017/06/29/adobe-launches-voice-analytics-for-siri-alexa-and-other-intelligent-assistants/. As companies invest in intelligent assistants, they also invest in tools to track the performance of these voice-enabled assistants. *Id.* One tool, Adobe Analytics Cloud, combines data sets and tracks customers across devices. *Id.* This means that an individual's use of Siri on one device, such as her iPhone, can be connected to her use of Siri on her iPad or computer. It is not clear the extent of the data collected from the use of intelligent assistants, but these features necessarily involve the use of voice data.

listening"—the opportunities for businesses to eavesdrop on consumers have soared.[18] For instance, in 2015, Apple released an optional "Hey Siri" feature for its iPhones. Once enabled, a user could say "Hey Siri" at any time, regardless of whether the phone was plugged in, and trigger the phone's voice assistant.[19] According to Apple, "in no case is the device recording what the user says or sending that information to Apple before the feature is triggered."[20] However, these pre-installed voice assistants—and user-installed applications—may record audio data without the user's knowledge or involvement.[21]

If Facebook's and Apple's denials are to be believed, what else could explain the stories above and found all over the internet? The fact that some advertisements follow conversations related to the products advertised could be a result of pure coincidence. But there are too many examples for coincidence to be the only answer. Alternatively, the algorithms that advertisers rely on could just be *that* good. While smartphones are present for a lot of face-to-face conversations, their presence allows them to collect more than just audio information. With the right features enabled, phones can also collect geophysical information, information on the types of products a user typically shops for online, and information on posts or pages a user frequently interacts with on social media.[22] Any of that information could lead an algorithm to deduce that a

---

[18] Manufacturers of "always listening" technologies might not use data to deliver their own targeted advertisements to consumers. *See* discussion *infra* Part III. However, because these always listening technologies are now built into smart devices, other businesses could program user-downloaded applications to use those technologies for their own purposes and gain. *See* discussion *infra* pp. 7–8 and accompanying notes.

[19] Matthew Panzarino, *Apple Addresses Privacy Questions About 'Hey Siri' and Live Photo Features*, TECHCRUNCH (Sept. 11, 2015), https://techcrunch.com/2015/09/11/apple-addresses-privacy-questions-about-hey-siri-and-live-photo-features/.

[20] *Id.*

[21] *See* J. D. Biersdorfer, *Protecting Personal Information From Virtual Assistants*, N.Y. TIMES (Jan. 27, 2016), https://www.nytimes.com/2016/01/28/technology/personaltech/protecting-personal-information-from-virtual-assistants.html ("When you use voice commands with an assistant program . . . your audio data may also be sent to the company's servers to process the request and improve speech recognition. Your browsing and search histories are probably collected, too. Companies often claim this is to provide more relevant results, but the data may also be used to help send more targeted advertisements your way.").

[22] *See* David Goldman, *Your Phone Company Is Selling Your Personal Data*, CNN MONEY (Nov. 1, 2011, 10:14 AM) http://money.cnn.com/2011/11/01/technology/verizon_att_sprint_tmobile_privacy/?iid=EL (claiming that four major wire carriers sell to third-party companies their customers' data, including

user is likely to respond positively to an advertisement for a particular product.[23]

Even if the algorithms are that impressive, "always listening" technologies are as well. As stated by Michelle De Mooy, the Director of the Center for Democracy and Technology's (CDT) Privacy and Data Project, "Smartphones are like small tracking devices . . . . We may not think of them like that because they're very personal devices—they travel with us, they sleep next to us. But they are in fact collectors of a vast amount of information including audio information."[24] In response to claims that smartphones could collect audio information without a user's knowledge, two cybersecurity experts built a prototype app to see how they could record audio from a device without asking for a user's permission.[25] The application, which violates Google's and Apple's Terms and Conditions,[26] listened through the microphone on a user's phone and then sent that data over the internet to the developers' listening server.[27] The app was able to record and transcribe everything that was said around the phone on which the app was installed.[28] Other apps can use a phone's

---

data on customers' location, web browsing history, personal data such as age and gender, and downloaded apps); Robert McMillan, *The Hidden Privacy Threat of ... Flashlight Apps?*, WIRED (Oct. 20, 2014, 6:30 AM), https://www.wired.com/2014/10/iphone-apps/ (revealing that some applications request data from users that is seemingly unrelated to the app's purpose); *see also* discussion on the use of big data in advertising *infra* Part I.

[23] Hosts of the ReplyAll podcast attempted to convince listeners that their phones were *not* listening. *#109 Is Facebook Spying on You?*, REPLY ALL (Nov. 2, 2017), https://www.gimletmedia.com/reply-all/109-facebook-spying. Despite the alternative explanations, none of the people who called into the show changed their opinions. *Id.* While this is not conclusive evidence that phones are listening to users, it does show that the difficulty in debunking these rumors, especially in the absence of regulation preventing the unauthorized collection of audio data.

[24] Hill, *supra* note 13.

[25] Kleinman, *supra* note 14. For technical information on the app, see Ken Munro, *Are Your Phones Listening to You*, PEN TEST PARTNERS (Mar. 2, 2016), https://www.pentestpartners.com/security-blog/are-your-phones-listening-to-you/.

[26] Operating system providers, such as Google and Apple, prohibit the undisclosed collection of user data by app developers, but the extent to which such policies are enforced and the ease in identifying infringing app are unclear. *See infra* Part III.A.

[27] Kleinman, *supra* note 14.

[28] *Id.*

microphone or camera with a user's consent, but without the user actively using the app.[29]

Additionally, the CDT alerted the Federal Trade Commission (FTC or "the Commission") and consumers of a technology which used audio beacons to track consumers across devices.[30] The technology was able to pick up on sounds emitted by an individual's television—sounds which were inaudible to that individual—and link that television and the phone on which the app was installed as belonging to the same person.[31] Although the software company behind the technology claimed that its service was not in use in the United States, the FTC issued a warning letter to app developers who were using the software, requesting that the developers notify consumers of the software's capabilities.[32] The letter also noted that, upon downloading and installing the developers' apps, no disclosures about the included audio beacon functionality appeared to the user.[33] Further, the letter stated that the apps asked users for microphone permissions, despite having no apparent need for those permissions.[34]

---

[29] For example, an app called Audio Aware can detect sounds of danger, such as screeching tires or sirens, through a smartphone's microphone and alert users who may be distracted or have auditory impairments. Rachel Metz, *App Listens for Danger When You're Note Paying Attention*, MIT TECH. REV. (Feb. 26, 2014), https://www.technologyreview.com/s/524971/app-listens-for-danger-when-youre-not-paying-attention/. The app compares external sounds to pre-recorded sounds and, when it detects a match, cancels audio playing on the user's smartphone and plays a version of the detected sound. *Id.* Another app, CrashAlert, uses depth cameras to show users objects outside of their peripheral view and alert them of obstacles while the users are using their devices. Juan David Hincapié-Ramos & Pourang Irani, *CrashAlert: Enhancing Peripheral Alertness for Eyes-Busy Mobile Interaction While Walking*, PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, 3385 (2013) *available at* http://hci.cs.umanitoba.ca/assets/publication_files/2013-CHI-Juan-CrashAlert.pdf. Although the CrashAlert prototype required a depth camera to be attached to a mobile device, smartphones may soon have built-in depth-sensing cameras, making apps like CrashAlert more convenient and easier to use. *See* Chaim Gartenberg, *Android Phones Will Probably Have Depth-Sensing IR Cameras Next Year*, VERGE (Aug. 15, 2017, 10:10 AM), https://www.theverge.com/circuitbreaker/2017/8/15/16150166/qualcomm-snapdragon-spectra-image-processor-android-phones-depth-sensing-ir-camera.

[30] Hill, *supra* note 13.

[31] *Id.*

[32] Press Release, Federal Trade Commission, FTC Issues Warning Letters to App Developers Using 'Silverpush' Code (Mar. 17, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code.

[33] *Id.*

[34] *Id.*

These examples reveal that devices are capable of collecting audio information from consumers, with and without consent.[35] Given that some apps have listening capabilities, advertisements could have more than just algorithmic explanations. The advertisements shown to a consumer could very well be influenced by audio data from phones.

If businesses do in fact listen to users, many of whom have no idea that they are even being recorded, consumers have more than just their privacy interests at stake. Targeted advertisements already raise civil rights concerns, as businesses may target vulnerable or marginalized groups in harmful ways. Big Data has been referred to as our generation's civil rights issue[36] and "one of the biggest public policy challenges of our time."[37] In February 2014, thirteen signatories, including the American Civil Liberties Union (ACLU), National Association for the Advancement of Colored People (NAACP), and several other civil rights organizations, released a set of principles calling for the government and businesses to "respect the values of equal opportunity and equal justice" in the development of new technologies.[38] These organizations pointed out the ways in which Big Data can be used to undermine existing anti-discrimination efforts. For example, Big Data can help businesses differentiate between potential hires,[39] engage in price discrimination for

---

[35] One concern that casts doubt on the "always listening" capabilities of phones pertains to battery and data usage. For a study evaluating the impact of these technologies on smartphones' batteries and the ability of phones to process large data sets, see NICHOLAS D. LANE ET. AL, DEEPEAR: ROBUST SMARTPHONE AUDIO SENSING IN UNCONSTRAINED ACOUSTIC ENVIRONMENTS USING DEEP LEARNING 283 (2015), *available at* http://niclane.org/pubs/ubicomp_deepear.pdf ("[W]e show that – even though training requires large-scale datasets and significant computational power – the energy and execution overhead of this approach is still feasible for mobile devices.").

[36] *See* Alistair Croll, *Big Data is Our Generation's Civil Rights Issue, and We Don't Know It*, SOLVE FOR INTERESTING (July 31, 2012, 12:40 PM), http://solveforinteresting.com/big-data-is-our-generations-civil-rights-issue-and-we-dont-know-it/ (arguing that the ability of Big Data to help marketers personalize marketing efforts based on race, gender, religion, and sexual orientation makes Big Data a civil rights issue).

[37] Joseph Jerome, *Big Data: Catalyst for a Privacy Conversation*, 48 IND. L. REV. 213, 218 (2014).

[38] CTR. FOR MEDIA JUSTICE, CIVIL RIGHTS PRINCIPLES FOR THE ERA OF BIG DATA 1 (2014), *available at* http://centerformediajustice.org/wp-content/uploads/2014/10/Civil-Rights-Principles-for-the-Era-of-Big-Data-FINAL.pdf. For specific examples depicting how Big Data implicates civil rights concerns, see *id.*

[39] *See* UPTURN, CIVIL RIGHTS, BIG DATA, AND OUR ALGORITHMIC FUTURE 15 (2014), *available at* https://bigdata.fairness.io/wp-content/uploads/2015/04/2015-04-20-Civil-Rights-Big-Data-and-Our-

insurance and loans,[40] and perpetuate systematic biases against protected classes.[41] A few months after these organizations released their initial set of principles, the White House commissioned a study that found "big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace."[42] Similarly, the CDT warns "automated systems can deny eligibility without providing an explanation or an opportunity to challenge the decision or the reasoning behind it. This

---

Algorithmic-Future-v1.2.pdf (describing a process by which businesses use algorithms to evaluate job applicants). Big Data can reveal information that affects hiring, such as whether a person depends on public transportation or how long a person has lived at his current address. *Id.* Many firms prefer people with shorter commutes because they are likely to stay at their jobs longer. *Id.* Big Data could create "systematic bias[es] against whole classes of people," especially given the racial makeup of different neighborhoods, and using that data in hiring algorithms can potentially violate principles of equal employment opportunity. *Id.*

[40] *See id.* at 6 ("[T]he deluge of "big data" allows for a new level of specificity in underwriting, changing how risk is allocated."). For example, devices can detect when drivers are driving at night and predict whether individuals are afflicted with certain life-threatening diseases, such as diabetes and certain forms of cancer. This allows for price differentiation, which could provide a benefit to the business, as well as the person. However, the use of such devices potentially undermines civil rights protections, because many low-income individuals, who are more likely to work at night, are racial minorities. Additionally, low-income neighborhoods are considered less healthy, so those living there will pay higher insurance costs.

[41] Many people are familiar with a field experiment conducted by the National Bureau of Economic Research (NBER) researchers in 2001 and 2002, which found that job applicants with white names were fifty percent more likely to receive a callback when applying for a job than applicants with African-American names. *See* David R. Francis, *Employer's Replies to Racial Names*, NAT'L BUREAU OF ECON. RES. DIG. (Sept. 2003), http://www.nber.org/digest/sep03/w9873.html. This racial bias can also be seen when black names are entered into an online search, as Latanya Sweeney, a computer science professor at Harvard University and former Chief Technologist at the FTC, observed. UPTURN, *supra* note 39, at 16. Sweeney found that searches containing African-American names were more likely to generate ads with "arrest" in the results than white names were. *Id.* This is because Google's Adsense service "automatically learns which ad combinations are most effective (and most profitable) by tracking how often users click on each ad. *Id.* These user behaviors, in aggregate, reflect the biases that currently exist across society." *Id.*

[42] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES, at iii (2014), available at https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf [hereinafter SEIZING OPPORTUNITIES].

opacity can leave people feeling helpless and discourage them from participating in critical institutions."[43]

The undisclosed collection of audio data engenders even more privacy concerns. If every room has a hidden figure—whether her name is Alexa, Siri, or Cortana—all sorts of personal information could be in the hands of profit-seeking businesses. For instance, noises in the data collected could reveal when individuals are eating, sleeping, or engaging in intimate acts. While businesses knowing more about their consumers has some advantages, too much knowledge gives businesses the power to influence consumers' behaviors without the consumers ever becoming aware that they are being used. Further, the capabilities of these technologies to match individuals to their devices can be applied to purposes beyond advertising. If governments want to take advantage of the now ubiquitous "always listening" technologies created by corporations, "[a]ny government interested in who you are meeting with could play a tone through the TV and effectively ping all the phones in the room, identifying the whole group."[44]

The Electronic Communications Privacy Act (ECPA)[45] protects citizens against some government intrusions, but unfortunately, no satisfactory legal framework exists to curb businesses' power over consumers as it relates to targeted advertising. Congress has ignored recommendations from the White House,[46] the FTC,[47] and other interested parties[48] to enact legislation. Instead of legislation, consumers must put

---

[43] *Digital Decisions*, CTR. FOR DEMOCRACY & TECH., https://cdt.org/issue/privacy-data/digital-decisions/ (last visited Apr. 8, 2018).

[44] Hill, *supra* note 13.

[45] Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (2012) (protecting private electronic communications from unauthorized government access).

[46] *See* SEIZING OPPORTUNITIES, *supra* note 42 (emphasizing the need for baseline privacy legislation).

[47] *See e.g.*, FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY iv (2014), *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [hereinafter DATA BROKERS] (recommending legislative action to improve transparency and choice in the data broker industry).

[48] Many of the groups who signed *Civil Rights Principles for the Era of Big Data* have actively advocated for increased consumer protections in the digital world. For example, the ACLU has dedicated a portion of its website to explaining to consumer online privacy, linking to blogs, reports, and press releases on the subject. *See Consumer Online Privacy*, AMER. C.L. UNION, https://www.aclu.org/issues/privacy-technology/internet-privacy/consumer-

their faith in the market and hope that businesses decide amongst themselves to keep consumers' privacy interests in mind.

While data collection and audio surveillance are also concerning when conducted by the government, this Article focuses on the private sector only. It also primarily focuses on just one application of the collected data: digital advertising. Part I explains how Big Data can be used in targeted advertisements and provides an overview of the benefits and harms of Big Data. Part II describes regulations on digital advertisers, highlighting the sectoral approach to data privacy in the United States. Part III reveals the ways in which the existing data protection regulations leave consumers unprotected from the unauthorized collection of audio data. This Part also discusses the privacy policies of companies who may either collect or facilitate the collection of audio data by third party app developers. In Part IV, this Article considers various proposals to protect consumers from intrusive advertisers. Arguing that the current self-regulatory scheme inadequately protects consumers, this Article seeks a solution that (1) requires companies to obtain informed consent from consumers before collecting and using audio data and (2) prohibits discriminatory or otherwise harmful digital advertising practices.

I. OVERVIEW OF BIG DATA AND DIGITAL ADVERTISING

Big Data is often characterized by three Vs: Volume, Variety, and Velocity.[49] Volume refers to the immense size of the data collected. Big Data analytics are able to process vast sets of information at once, allowing companies to make better predictions than they could using models with smaller data sets.[50] Variety refers to the diversity of the sources and types of data collected.[51] Companies, known as data brokers, collect information on nearly every consumer and every commercial transaction in the United States.[52] Data brokers collect data from a multitude of sources, including

---

online-privacy (last visited Apr. 8, 2018) (explaining the importance of enacting consumer protections.

[49] Wilder-James, *supra* note 6.

[50] *See id.* ("Having more data beats out having better models: simple bits of math can be unreasonably effective given large amounts of data. If you could run that forecast taking into account 300 factors rather than 6, could you predict demand better?").

[51] *Id.*

[52] DATA BROKERS, *supra* note 47. ("Of the nine data brokers, one data broker's database has information on 1.4 billion consumer transactions and over 700 billion aggregated data elements; another data broker's database covers one trillion dollars in consumer transactions; and yet another data broker adds three billion new records each month to its databases. Most importantly, data brokers hold a vast array of information on individual consumers. For example, one of the nine data brokers has 3000 data segments for nearly every U.S. consumer.").

government records, commercial databases, social media websites, mobile applications, and publicly available sources.[53] The data collected by these brokers could consist of "bankruptcy information, voting registration, consumer purchase data, web browsing activities, warranty registrations, and other details of consumers' every day interactions."[54] Although each data source may only provide a few bits of information, "data brokers can put all of these data elements together to form a more detailed composite of the consumer's life."[55] Finally, Big Data is also defined by its Velocity, or the speed at which data can be processed.[56]

Big Data has recently been characterized by another V: Value. Big Data inherently networks small pieces of information.[57] The relationality of the data gives businesses significant advantages: "[Big Data's] value comes from the patterns that can be derived by making connections between pieces of data, about an individual, about individuals in relation to others, about groups of people, or simply about the structure of information itself."[58] Big Data is also valuable because of its accessibility to a wide range of people, including academics, marketers, and governments.[59] However, the ease in which individuals can collect, share, and use data can present some challenges for data management. As two researchers from Microsoft note, "Data is increasingly digital air: the oxygen we breathe and the carbon dioxide we exhale. It can be a source of both sustenance and pollution."[60]

A. How Businesses Use Big Data for Advertising

Online behavioral advertising ("OBA") is one of the many applications of Big Data. The FTC defines OBA as "the tracking of a consumer's activities online – including the searches the consumer has conducted, the Web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer's interests." [61] Companies track consumers using information-gathering tools known as cookies, flash cookies, and beacons. These tracking tools provide

---

[53] *See id.*; *see also* SEIZING OPPORTUNITIES, *supra* note 42, at 8.
[54] DATA BROKERS, *supra* note 47.
[55] *Id.*
[56] Wilder-James, *supra* note 6.
[57] DANAH BOYD & KATE CRAWFORD, SIX PROVOCATIONS FOR BIG DATA 2 (Sept. 21, 2011), *available at* https://ssrn.com/abstract=1926431.
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] Press Release, Federal Trade Commission, FTC Staff Proposes Online Behavioral Advertising Privacy Principles (Dec. 20, 2007), https://www.ftc.gov/news-events/press-releases/2007/12/ftc-staff-proposes-online-behavioral-advertising-privacy.

marketers with information "used to improve market segmentation and target marketing to reach consumers on an individualized basis."[62]

There are two types of OBA: first-party behavioral advertising, which allows companies to track a user's activity on a single website, and third-party behavioral advertising, which allows companies to collect data across multiple and varied websites.[63] First-party behavioral advertising uses cookies, which are small text files that web servers store on the hard drives of those who access a given website,[64] to track a user's activity on a website. Cookies were initially intended to benefit users, especially while online shopping.[65] Because cookies enable websites to quickly identify repeat visitors, they can save the users time and can lead to more personalized future visits to the website.[66] Third-party behavioral advertising uses flash cookies and beacons to track users. Flash cookies link a user's activity on one website to that user's activity on another website.[67] Similarly, beacons[68] track a user across multiple websites and then transmit information on that user's interaction with a website to a third party via a cookie.[69] Third parties can use beacons to "retrieve files stored on a hard drive, record conversations through a computer microphone, or transmit images from a computer's video camera."[70]

Companies can also track individuals' activity offline. For example, they can collect information on an individual's recent purchases,

---

[62] Janice C. Sipor, et. al, *Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons*, 10 J. INTERNET COM. 1, 2 (2011).
[63] Steven C. Bennett, *Regulating Online Behavioral Advertising*, 44 J. MARSHALL L. REV. 899, 901 (2011).
[64] *See* Amir M. Hormozi, *Cookies and Privacy*, 32 EDP AUDIT, CONTROL, AND SECURITY NEWSL. 1, 1–2 (2005). The software engineer who developed cookies, Lou Montulli, defines a cookie as "a piece of data that is stored, then given to the client, stored by the client, and returned to the server each time the client returns." *Id.* at 1–2.
[65] *Id.* at 2–3.
[66] *Id.* at 1. For more info on the advantages and disadvantages of cookies, see *id.* For a discussion on the privacy and "dataveillance" downsides of cookies in social media, also see Jo Pierson & Rob Heyman, *Social Media and Cookies: Challenges for Online Privacy*, 13 INFO 30, 30 (2011) ("The positive aspects of cookies, unobtrusiveness and ease of use, are also the main challenges for user privacy. This technology can be disempowering because users are often hardly aware of its existence. In that way cookies can obfuscate the perceived context of personal data exposure.").
[67] Sipor et. al, *supra* note 62, at 4.
[68] A beacon is a "small, imperceptible graphic file, often transparent because it is the same color as the background." *Id.*
[69] *Id.* at 5.
[70] *Id.*

place of residence, model of car, and number of children.[71] One method of collecting information involves a retailer requesting email addresses from customers.[72] The retailer then shares that email address with a digital marketing firm or data broker.[73] The marketing firm then locates that customer using the email address provided.[74] If the customer has used her email address to log into a website with which the marketing firm has a relationship, the marketing firm will then be able to "tag the customer's computer with a tracker."[75] The retailer's website can then be personalized for individual customers. In fact, one marketing firm's documents revealed that high-paying customers could see a version of the retailer's website that showed more expensive products.[76] Marketing firms can also track individuals using their real names, a process known as "onboarding."[77] Onboarding allows companies to connect consumers' offline and online activity, increasing the amount of information on each consumer they can gather and use for profit.[78] Additionally, companies can track individuals across multiple devices.[79] Even an individual's television can give companies information they can then use in targeted advertising.[80] Becky White, former-Chairwoman of the FTC, remarked at

---

[71] Julia Angwin, *Why Online Tracking Is Getting Creepier*, PROPUBLICA (June 12, 2014), https://www.propublica.org/article/why-online-tracking-is-getting-creepier [hereinafter *Why Online Tracking Is Getting Creepier*].

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] For more information on tracking, see Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J. (July 30, 2010), https://www.wsj.com/articles/SB10001424052748703940904575395073512989404 (explaining how companies capture data based on an individual's internet activity and use that data to create individual consumer profiles).

[79] To track individuals across multiple devices, companies use a combination of deterministic and probabilistic techniques. FED. TRADE COMM'N, FTC CROSS-DEVICE TRACKING WORKSHOP, SEGMENT 1 TRANSCRIPT 3 (2015), *available at* https://www.ftc.gov/system/files/documents/videos/cross-device-tracking-part-1/ftc_cross-device_tracking_workshop_-_transcript_segment_1.pdf. ("Deterministic linking is based on information a consumer provides to a website or service, such as when they log on to a social network or email account. Probabilistic models work more passively by making inferences based on information the user has no control over, such as shared IP addresses or location information, when two devices are consistently used together in the same household.").

[80] Then-Policy Director of the FTC's Office of Technology Research and Investigation, Justin Brookman, hinted at a workshop: "There are advertising

a workshop on cross-device tracking, "[w]hile tracking itself is not new, the ways in which data is collected, compiled, stored, and analyzed certainly is."[81]

Using the large quantities of information gathered from these tracking tools, companies build mathematically complex models known as algorithms.[82] Algorithms analyze the information collected on an individual user, including that user's online activity, and deduce that user's inclinations.[83] Through algorithms, private businesses, government organizations, and educational institutions learn "massive patterns in human behavior."[84] Further, businesses can use the algorithms to target advertisements to individuals. The more information businesses know about consumers, the better the algorithms can predict which ads will be successful when shown to an individual consumer.

---

companies that listen to—that use Bluetooth or microphones to listen to physical beacons or TV advertisements." *Id.* at 12–13.

[81] *Id.* at 4.

[82] The CDT explains algorithms as follows:

> In its most basic form, an algorithm is a set of step-by-step instructions—a recipe—'that leads its user to a particular answer or output based on the information at hand.' Applying its recipe, an algorithm can calculate a prediction, a characterization, or an inferred attribute, which can then be used as the basis for a decision. This basic concept can be deployed with varying degrees of sophistication, powered by the huge amounts of data and computing power available in the modern world. Algorithms take large amounts of information and categorize it based on whatever criteria the author has chosen.

Digital Decisions, *supra* note 43 (emphasis omitted). Another author defines algorithms as "predictive audience models [able to discern] the particular pattern in user profiles and user transactions that are most indicative of a positive response to the ads." John Sinclair, *Advertising and Media in the Age of the Algorithm*, 10 INT'L J. COMM. 3521, 3528 (2016) (quoting Xuhui Shao, *It's the Algorithm, Stupid*, CLICKZ (Mar. 14 2011), https://www.clickz.com/its-the-algorithm-stupid/52513/).

[83] Joanna Penn, Note, *Behavioral Advertising: The Cryptic Hunter and Gatherer of the Internet*, 64 FED. COMM. L.J. 599 (2012). Algorithms collect two types of information. The first is personally identifiable information (PII), which is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual." *Id.* at 604. PII includes "names, email addresses, credit card numbers, and other distinguishable bits of data." *Id.* The second type of information collected is non-personally identifiable information (non-PII), which is "anonymous data that, without more specific data added to it, cannot identify a specific person." *Id.*

[84] Boyd & Crawford, *supra* note 57.

Some businesses have come under fire for knowing too much. For example, retail giant Target, like many other businesses, collects information on customers in an attempt to shape their shopping habits.[85] After learning that customers are most likely to change their shopping preferences following a major life event, such as pregnancy or a job change, Target's statisticians developed an algorithm to identify potentially pregnant shoppers.[86] The algorithm assigned each female shopper a "pregnancy prediction" score, which Target then used to send these shoppers coupons timed according to the stage of pregnancy they were likely to be in.[87] Unfortunately, one recipient of Target's maternity advertisements was a teenage girl whose father accused Target of encouraging his daughter to get pregnant.[88] A few days after confronting Target, the father apologized, as the retailer had accurately guessed that his daughter was already pregnant.[89]

The Target story illustrates how Big Data enables businesses to know more about us and our lives than we know ourselves. Once they have obtained the information, these businesses deliver targeted ("Target-ed?") advertisements to consumers' mailboxes or, alternatively, to their inboxes. Additionally, these advertisements can show up on the webpages consumers visit. Digital advertising has become quite an effective and profitable enterprise, as indicated by the fact that it is "the fastest-growing sector of advertising expenditure in the United States."[90]

B. Advantages of Big Data

Businesses like Big Data because of the benefits that result from the ability of Big Data analytics to predict future outcomes. This ability allows businesses to make better decisions in the present, especially as those decisions pertain to marketing and advertising.[91] But Big Data does not benefit businesses alone. The digital advertising and marketing that Big Data enables "effectively subsidize many free goods on the Internet, fueling an entire industry in software and computer apps."[92] Big Data has other economic advantages as well; for instance, companies can use Big

---

[85] Duhigg, *supra* note 7.
[86] *Id.*
[87] *Id.*
[88] *Id.*
[89] *Id.*
[90] Sinclair, *supra* note 82, at 3530. For a study measuring the effectiveness of behavioral targeting, see Jun Yun et al., *How Much Can Behavioral Targeting Help Online Advertising?*, PROCEEDINGS OF THE 18TH INTERNATIONAL CONFERENCE ON WORLD WIDE WEB 261 (2009).
[91] Dennis D. Hirsch, *That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority*, 103 KY. L.J. 345, 349–50 (2015).
[92] SEIZING OPPORTUNITIES, *supra* note 42, at 50.

Data to estimate demand,[93] monitor the maintenance of equipment,[94] and predict stock market performance.[95]

Big Data can also benefit individuals. Data analytics can reveal which individuals are more likely to develop medical conditions, such as diabetes or other diseases, and identify infections early.[96] This allows medical providers to treat conditions early and save lives.[97] Big Data can also save money: the analytics can identify potential acts of reimbursement fraud before the government pays claims, preventing the government and taxpayers from getting swindled.[98] Big Data analytics can determine which students are likely to need additional help in school and help supply those students with the appropriate educational tools to succeed. [99] Additionally, individuals can benefit from Big Data as consumers. Predictive analytics make it possible for businesses to show individual consumers the types of products and services those consumers want to see.

C. Consumers' Invasion of Privacy

Yet big is not always better. Big Data arouses concerns about how much companies know about consumers and about what companies may do with that information. In the story above, Target revealed a teenager's pregnancy to her father without her consent. It is not hard to imagine what might have happened had the teen's father been abusive and reacted violently to the news of her pregnancy. Companies' use of individuals' sensitive information for financial gain can result in privacy harms, economic harms, and even physical.

Additionally, the amount of information businesses collect on individuals is just plain creepy. A few years ago, a female user of Tinder, an online dating service, requested the company's personal data on her.[100] The woman received over 800 pages of information known as "secondary implicit disclosed information."[101] The pages contained over 1700

---

[93] John Podesta, *Findings of the Big Data and Privacy Working Group Review*, WHITE HOUSE: BLOG (May 1, 2014, 1:15 PM), https://obamawhitehouse.archives.gov/blog/2014/05/01/findings-big-data-and-privacy-working-group-review.

[94] *Id.*

[95] Hirsch, *supra* note 91, at 350.

[96] *See id.*; *see also* Podesta, *supra* note 95.

[97] Hirsch, *supra* note 91, at 350. Podesta, *supra* note 95.

[98] Podesta, *supra* note 95.

[99] Hirsch, *supra* note 91, at 350.

[100] Judith Duportail, *I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets*, THE GUARDIAN (Sept. 26, 2017, 2:10 AM), https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold.

[101] *Id.*

messages she had sent to her romantic matches since 2013, information on the pages she had liked on Facebook, her education, and the age range of men in which she was interested.[102] Every time this woman swiped on a potential match, she unknowingly entered another data point in Tinder's file on her. Professor Allessandro Acquisti explained to the woman:

> Tinder knows much more about you when studying your behaviour on the app. It knows how often you connect and at which times; the percentage of white men, black men, Asian men you have matched; which kinds of people are interested in you; which words you use the most; how much time people spend on your picture before swiping you, and so on. Personal data is the fuel of the economy. Consumers' data is being traded and transacted for the purpose of advertising.[103]

While Tinder's privacy policy states that users' data can be used to deliver targeted advertisements, plenty of Tinder's 50 million-plus users are likely unaware of the fact that every one of their digital acts can turn into data. Further, Tinder is just one of many apps a person could have on his smartphone. A 2017 study found that the average person uses thirty apps per month, or about nine apps per day.[104] If each app has the same amount of information on each person as Tinder had, that's 24,000 pages of information companies could have on each individual who regularly uses their apps. In case that isn't alarming enough, consider how much personal information someone who uses Tinder (which catalogs, as one example, every conversation users have on its app), OkCupid (which has learned intimate details, including how its users like to have sex, whether they have problems achieving orgasm, and how often they masturbate),[105] and Uber (which has admittedly collected data on users' one-night-stands)[106] has shared with data collectors. These datasets can be purchased by any

---

[102] *Id.*

[103] *Id.*

[104] Sarah Perez, *Report: Smartphone Owners Are Using 9 Apps Per Day, 30 Per Month*, TECHCRUNCH (May 4, 2017), https://techcrunch.com/2017/05/04/report-smartphone-owners-are-using-9-apps-per-day-30-per-month/.

[105] *10 Charts About Sex*, OKCUPID BLOG (Apr. 19, 2011), https://theblog.okcupid.com/10-charts-about-sex-47e30d9716b0. OkCupid has collected this information by analyzing some users' answers to match questions and by observing others' activity on the dating platform. *Id.*

[106] Derrick Harris, *The One-Night Stand, Quantified and Visualized by Uber*, GIGAOM (Mar. 6, 2012, 4:05 PM), https://gigaom.com/2012/03/26/uber-one-night-stands/.

business—including a potential employer[107]—seeking to learn more about an individual.

Because businesses do not have to reveal what they do with the information they collect, or how much information they have, consumers can suffer injuries to their privacy. The woman from the above story had the right to request her data, and Tinder had the duty to oblige, thanks to data protection laws in the European Union.[108] Users in the United States have no such rights, so they have no way of knowing how much information companies have on them. While the fact that these users have consented to the collection and use of their data might mitigate the privacy injuries, there is no way that consumers can give informed consent without actually knowing what information they have "shared" with businesses. Similarly, because consumers cannot opt out of having certain information collected if they use certain services, the collection of such sensitive information can also amount to an unwarranted intrusion.

D. Discrimination in Targeted Advertising

Big Data also makes price discrimination possible. While price discrimination is not inherently bad, the ability to identify users based on certain characteristics enables companies to charge consumers for products and services based on their exact willingness to pay, which could lead to companies exploiting vulnerable groups of people.[109]

Big Data can undermine civil rights protections if businesses use algorithms to target advertisements in discriminatory ways. It also can make intentional forms of discrimination harder to identify, as there is often a lack of transparency as it pertains to data analysis. Further, algorithms can use certain factors, such as where a person lives or their interests, as proxies for race, gender, or other protected classifications. As the Obama Administration warned in 2014, "[j]ust as neighborhoods can serve as a proxy for racial or ethnic identity, . . . big data technologies

---

[107] Several companies use Big Data for employee recruitment, training, promotion, and discharge. *See generally* DARRELL S. GAY & ABIGAIL M. LOWIN, BIG DATA IN EMPLOYMENT LAW: WHAT EMPLOYERS AND LEGAL COUNSEL NEED TO KNOW (2017), available at https://www.americanbar.org/content/dam/aba/events/labor_law/2017/11/conference/papers/Gay-Paper%20on%20Big%20Data%20%20for%20ABA%20LEL%20Conference.authcheckdam.PDF (discussing the uses of Big Data in the recruitment context).

[108] *See* Olivia Solon, *New Europe Law Makes It Easy to Find Out What Your Boss Has Said About You*, GUARDIAN (Apr. 24, 2018, 2:00 AM), https://www.theguardian.com/technology/2018/apr/23/europe-gdpr-data-law-employer-employee (explaining the right of anyone in Europe to request access to data companies have on them).

[109] *See* Jerome, *supra* note 37, at 218–19.

could be used to 'digitally redline' unwanted groups, either as customers, employees, tenants, or recipients of credit."[110] Unintentional forms of discrimination can also occur if the data on which the algorithms are based is biased or incomplete.[111]

Even when it is clear that advertisements intentionally discriminate against whole classes of people, the websites on which these advertisements appear do not always filter out such ads. For example, many marketers advertise on Facebook. Facebook, which has over two billion users, keeps track of every time a user likes a post, updates her status, and adds her favorite movies and books to her profile.[112] All of this becomes valuable data for Facebook. Users further add data to Facebook's collection every time they log onto an app owned by Facebook, such as Instagram.[113] Additionally, every time a user logs into Facebook on a separate app not owned by Facebook, Facebook gains more information on the user's preferences and interests.[114] Facebook also purchases some

---

[110] SEIZING OPPORTUNITIES, *supra* note 42, at 53. But, the report also noted that "[t]he same algorithmic and data mining technologies that enable discrimination could also help groups enforce their rights by identifying and empirically confirming instances of discrimination and characterizing the harms they caused." *Id.*

[111] *See* Jerome, *supra* note 37, at 221–22. For a discussion on how incomplete or biased data leads to discriminatory models, see generally Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016). The authors explain:

> (1) If data mining treats cases in which prejudice has played some role as valid examples to learn from, that rule may simply reproduce the prejudice involved in these earlier cases; or (2) if data mining draws inferences from a biased sample of the population, any decision that rests on these inferences may systematically disadvantage those who are under-or [*sic*] overrepresented in the dataset.

Id. at 681.

[112] Julia Angwin et. al, *Breaking the Black Box: What Facebook Knows About You*, PROPUBLICA (Sept. 28, 2016). https://www.propublica.org/article/breaking-the-black-box-what-facebook-knows-about-you [hereinafter *Breaking the Black Box*].

[113] *Id.*

[114] *See Your Ad Preferences*, FACEBOOK, https://www.facebook.com/ads/preferences/?entry_product=ad_settings_screen (last visited Apr. 24, 2018) (listing advertisers whose websites or apps—which use Facebook technology—a logged-in user has accessed). Unlike with Tinder, Facebook shows users the types of categories they are sorted in. *See id.* (listing a logged-in user's categories under the "Your Information" section). However, Facebook does not reveal the specific sources of data that contribute to those categories. *See id.* Also note that, while this information is technically available, users must first know to look for it and how to access it (and must be logged into Facebook to see). *See id.*

data, including data "about its users' mortgages, car ownership and shopping habits from some of the biggest commercial data brokers."[115] Facebook uses this data to sell marketers the opportunity to target advertisements "to increasingly specific groups of people."[116] Facebook has over 1,300 categories in which it places users for the purposes of targeting advertisements.[117] These categories include "everything from people whose property size is less than .26 acres to households with exactly seven credit cards."[118] Facebook also has an "Ethnic Affinity" category, which categorizes users according to their affinity for minority ethnic groups.[119] One group of journalists investigating Facebook's advertising scheme discovered over 52,000 different attributes that Facebook uses to place its users into categories.[120] Marketers who use Facebook's services can show advertisements to —or hide them from— certain groups, based on these categories.[121]

Facebook's advertising policies prohibit advertisers from targeted ads based on protected classes.[122] But the social media company does not always enforce these policies to the best of its ability. In 2016, ProPublica, an investigative journalist company, bought ads on Facebook using Facebook's housing category to target users who were likely to be shopping for houses.[123] ProPublica then targeted the ads to exclude users

---

[115] *Breaking the Black Box*, *supra* note 112. Facebook informs users that it gets information from a variety of sources, but it does not inform users that those sources include the wealth of data "obtained from commercial data brokers about users' offline lives." Julia Angwin et. al, *Facebook Doesn't Tell Users Everything It Really Knows About Them*, PROPUBLICA, (Dec. 27, 2016, 9:00 AM), https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them. [hereinafter *Facebook Doesn't Tell*]. When asked about this non-disclosure, Facebook told journalists "that users can discern the use of third-party data if they know where to look. Each time an ad appears using such data, . . . users can click a button on the ad revealing that fact." *Id.* However, "[u]sers can still not see what specific information about their lives is being used." *Id.*

[116] *Breaking the Black Box*, *supra* note 112.

[117] *Id.*

[118] *Id.*

[119] *Facebook Doesn't Tell*, *supra* note 115.

[120] *Id.*

[121] *Breaking the Black Box*, *supra* note 112.

[122] *Advertising Policies*, FACEBOOK, https://www.facebook.com/policies/ads/ (last visited Apr. 8, 2018) ("Ads must not discriminate or encourage discrimination against people based on personal attributes such as race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, medical, or genetic condition.").

[123] Julia Angwin & Terry Parris Jr., *Facebook Lets Advertisers Exclude Users by Race*, PROPUBLICA, (Oct. 28, 2016, 1:00 PM),

with "an 'affinity' for African-Americans, Asian-Americans, and Hispanics."[124] Within fifteen minutes of placing the order, Facebook had approved the ad.[125] After ProPublica published an article informing readers of what they had been allowed to do using Facebook's services, Facebook received a lot of criticism and a demand from Congress to stop allowing advertisers to exclude certain ethnic groups.[126] Facebook soon after announced a new policy enforcing its prohibitions of discriminatory ads in February 2017.[127] However, when ProPublica re-conducted its experiment in November 2017, this time purchasing dozens of discriminatory ads in the housing category, each one was again approved within minutes.[128]

ProPublica also discovered that Facebook allows advertisers to connect to users interested in white supremacy and anti-Semitism.[129] While the ability to identify white supremacists could certainly be valuable for those interested in ending bigotry, Facebook's categories are not being used for that purpose. Rather, they are being used to sell advertising space, essentially giving advertisers the tools to sell hate speech by connecting them with individuals interested in hateful causes. Although statutes such as the Fair Housing Act of 1968 and the Civil Rights Act of 1964 prohibit discrimination in certain contexts, privacy laws in the United States do not effectively protect citizens from the dangers associated with collecting data for the purposes of perpetuating systematic biases and prejudices.

---

https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race [hereinafter *Exclude Users by Race*].

[124] *Id.*

[125] *Id.*

[126] Julia Angwin, *Facebook Says It Will Stop Allowing Some Advertisers to Exclude Users by Race*, PROPUBLICA (Nov. 11, 2016, 10:00 AM), https://www.propublica.org/article/facebook-to-stop-allowing-some-advertisers-to-exclude-users-by-race.

[127] *Improving Enforcement and Promoting Diversity: Updates to Ads Policies and Tools*, FACEBOOK: NEWSROOM (Feb. 8, 2017), https://newsroom.fb.com/news/2017/02/improving-enforcement-and-promoting-diversity-updates-to-ads-policies-and-tools/.

[128] Julia Angwin et. al, *Facebook (Still) Letting Housing Advertisers Exclude Users by Race*, PROPUBLICA (Nov. 21, 2017, 1:23 PM), https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin.

[129] *Facebook Enabled Ads Targeting Anti-Semites*, NAT'L PUB. RADIO (Sept. 15, 2017, 5:06 AM), https://www.npr.org/2017/09/15/551163392/facebook-enabled-ads-targeting-anti-semites.

II. DATA PRIVACY IN THE UNITED STATES

Modern data privacy law originates from the works of Alan Westin,[130] who defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[131] In *Olmstead v. United States*, Justice Brandeis produced another definition. He characterized privacy as simply "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[132]

The Constitution does not explicitly recognize a right to privacy. However, the Supreme Court has found that the First and Fourth Amendments implicitly guarantee the right to privacy against the government.[133] But this right does not protect citizens against intrusions in the private sector.

Congress has made some strides to provide a right to protect citizens from the use of personal information in the private sector. Rather than provide overarching protections, the existing regulations enacted by Congress target specific sectors. For example, Congress passed the Computer Fraud and Abuse Act (CFAA), the federal anti-hacking law, in 1984.[134] Congress also passed the Children's Online Privacy Protection Act (COPPA) in 1998 to protect the privacy of children under the age of thirteen.[135] Other sector-specific statutes include the Fair Credit Reporting

---

[130] Erin Corken, *The Changing Expectation of Privacy: Keeping Up with the Millennial Generation and Looking Toward the Future*, 42 N. KY. L. REV 287, 289 (2015); *see also*, Margalit Fox, *Alan F. Westin, Who Transformed Privacy Debate Before the Web Era, Dies at 83*, N.Y. TIMES (Feb. 22, 2013), http://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-privacy-dies-at-83.html ("Through his work — notably his book "Privacy and Freedom," . . . Mr. Westin was considered to have created, almost single-handedly, the modern field of privacy law.").

[131] ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967). *Privacy and Freedom* was Westin's response to developing surveillance technologies—most notably, wire-tapping—and growing concerns for the future uses of those technologies.

[132] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[133] U.S. CONST. amend. I; U.S. CONST. amend. IV. The Court recognized the right to privacy in *Griswold v. Connecticut*, 381 U.S. 479, 484–85 (1965) (finding the right to privacy emanates from the penumbra of the Bill of Rights).

[134] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012).

[135] Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–06 (2012) (prohibiting the collection of personal information from children without parental consent).

Act[136] and the Gramm Leach-Bliley Act,[137] which protect consumers' financial information. These statutes reflect Congress's effort to respond to privacy concerns in individual sectors of the economy, especially in the now-digital world.

However, no comprehensive federal privacy regulation currently controls the private sector. Despite urging from the Obama Administration[138] and several other groups interested in data protection,[139] Congress has not implemented baseline privacy legislation.[140] This lack of regulation stands in stark contrast to privacy regulation in the European Union, which has an expansive data protection scheme that requires

---

[136] Fair Credit Reporting Act, 15 U.S.C.§ 1681(2012) (requiring consumer consent before providing credit reports to employers or prospective employers).

[137] Gramm Leach-Bliley Act, 15 U.S.C. §§ 6801–10 (2012) (requiring financial institutions to provide notice to consumers and opt-out options for disclosure of personal data to third parties).

[138] WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 36 (2012), available at https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf. [hereinafter CONSUMER DATA PRIVACY IN A NETWORKED WORLD] ("The Administration encourages Congress to follow a similar path with baseline consumer data privacy legislation. It is important that a baseline statute provide a level playing field for companies, a consistent set of expectations for consumers, and greater clarity and transparency in the basis for FTC enforcement actions.").

[139] *See, e.g.*, Natasha Duarte, *Feds and States Must Work Together on Consumer Privacy*, CTR. FOR DEMOCRACY & TECH. (June 14, 2017), https://cdt.org/blog/feds-and-states-must-work-together-on-consumer-privacy/. ("The U.S. needs a good federal solution to protect consumer privacy, and that solution can include limited preemption to prevent genuine conflicts between federal and state law.").

[140] Although Congress has not yet passed data protection regulation, the Balancing the Rights of Web Surfers Equally and Responsibly (BROWSER) Act was introduced in May 2017. BROWSER Act of 2017, H.R. 2520, 115th Cong. (2017). The BROWSER ACT "authorizes the Federal Trade Commission to enforce information privacy protections that require broadband internet access services and certain websites or mobile applications providing subscription, account, purchase, or search engine services to allow users to opt-in or opt-out of the use, disclosure, or access to their user information depending on the sensitivity of the information." CONG. RES. SERV., SUMMARY: H.R.2520, *available at* https://www.congress.gov/bill/115th-congress/house-bill/2520. The CDT criticized this bill for its overly broad state preemption, which would "reverse a long tradition of state leadership and cooperation in consumer privacy protection." Duarte, *supra* note 139. As of this writing, the bill has not been passed in either the House or Senate.

databases to register with governmental data protection agencies.[141] While the European Union has moved towards enhancing consumer protections, the United States has fallen behind.

A. Fair Information Practice Principles and Federal Privacy Initiatives

After the publication of Westin's works, the Department of Health, Education, and Welfare established the Secretary's Advisory Committee on Automated Personal Data Systems.[142] Charged with protecting the privacy of data maintained by both private and public sector organizations, the Committee issued a report, *Records, Computers, and the Rights of Citizens*, which put forward a set of principles addressing information privacy.[143] These principles, known as fair information practice principles ("FIPPs") "established a framework for both the public and private sectors to implement procedures governing the collection, use, and disclosure of personal information."[144] FIPPs are often reflected in American privacy laws and have been internationally recognized.[145]

The FIPPS originally consisted of four elements: Notice, Choice, Access, and Security. The Notice Principle, also known as the Awareness or Collection Principle, stated that individuals should be given notice before their information is collected.[146] The Choice Principle, or the Consent Principle, states that individuals should be allowed to choose whether to opt-in or opt-out of the use of the information collected from them.[147] The Access Principle, also called the Participation Principle, states that individuals must be able to view and verify the accuracy of the collected information.[148] Lastly, the Security Principle, also known as the Integrity Principle, states that the collectors of information must ensure that the data collected is accurate and secure.[149]

Congress implemented the original four FIPPS when it enacted the Privacy Act of 1974, which was the first piece of legislation that regulated personal information specifically.[150] The Privacy Act governed

---

[141] *Session 4: Consumer Privacy*, HARV. UNIV., https://cyber.harvard.edu/olds/ecommerce/privacytext.html (last visited Apr. 8, 2018).
[142] Robert Gellman, *Fair Information Practices: A Basic History* 2 (2017), *available at* https://bobgellman.com/rg-docs/rg-FIPshistory.pdf.
[143] *Id.*; Corken, *supra* note 130, at 290.
[144] *See* Jerome, *supra* note 37, at 228.
[145] Gellman, *supra* note 142, at 1.
[146] Corken, *supra* note 130, at 290.
[147] *Id.*
[148] *Id.*
[149] *Id.*
[150] *Id.*; Jerome, *supra* note 37, at 228.

the collection, maintenance, use, and dissemination of personal information by federal agencies.[151]

In 1998, the FTC issued a report wherein it added a fifth principle, the Enforcement Principle.[152] Also known as the Redress Principle, this FIPP identified three mechanisms to enforce the other four core principles: self-regulation, private remedies, and government enforcement.[153] For a self-regulatory regime to be effective, the FTC stated that compliance mechanisms and "appropriate means of recourse by injured parties" were both necessary.[154] The other two enforcement alternatives would require specific legislative action.[155]

FIPPs have been expanded both globally and domestically. [156] In 2008, the Privacy Office of the Department of Homeland Security put forth a version of FIPPs with eight principles: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing.[157] The Organisation for Economic Co-operation and Development (OECD), an intergovernmental economic organization with thirty-five member countries including the United States, also expanded and adopted the FIPPs.[158]

The Obama Administration incorporated the FIPPS and urged Congress to provide stronger consumer protections. The Administration released the Consumer Privacy Bill of Rights, which included seven principles.[159] The Administration called for Congress to grant the FTC direct enforcement authority of the Consumer Privacy Bill of Rights and for Congress to enact privacy legislation protecting consumers.[160] In January 2014, the Administration subsequently conducted a comprehensive review of Big Data, recognizing the public policy issue that data privacy was becoming.[161] The review consisted of a public survey which asked people about their data privacy concerns and whether they

---

[151] Corken, *supra* note 130, at 290; Jerome, *supra* note 37, at 229.
[152] FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 10–11 (June 1998) [hereinafter REPORT TO CONGRESS].
[153] *Id.*
[154] *Id.* at 10.
[155] *Id.* at 11.
[156] Gellman, *supra* note 142, at 1.
[157] *Id.* at 21–22.
[158] Corken, *supra* note 130, at 291–92 (explaining the OECD's eight principles).
[159] CONSUMER DATA PRIVACY IN A NETWORKED WORLD, *supra* note 138. For comparison of the Consumer Privacy Bill of Rights to other statements of FIPPs, including the OECD guidelines, see *id.* at 49–52.
[160] *Id.* at 36.
[161] Jerome, *supra* note 37, at 217–18.

trusted institutions to protect and use their data responsibly.[162] One particular question raised by the review asked "whether the 'notice and consent' framework, in which a user grants permission for a service to collect and use information about them, still allows us to meaningfully control our privacy as data about is increasingly used and reused in ways that could not have been anticipated when it was collected."[163] A majority of the respondents were strongly concerned about the use and collection of data, as well as proper oversight and transparency for data practices.[164] Unfortunately, this review did not generate Congressional action, and the questions it raised remain unanswered.

B. Self-Regulation in the Digital Advertising Industry

For entities that do not fall under the umbrella of a specific sectoral law, self-regulation has been the primary method of privacy protection. The FTC is charged with enforcing the Federal Trade Commission Act (FTCA) and a number of additional statutes,[165] including the sector-specific statutes referenced above. The FTCA protects consumers from unfair or deceptive practices across various sectors of the economy.[166] The FTC also recommends legislation to Congress and publishes self-regulatory principles which it encourages the private sector to adopt.[167] The Commission has the additional responsibility of regulating online privacy.

---

[162] Corken, *supra* note 130, at 310.

[163] Podesta, *supra* note 95. Although the Administration warned of the possible inappropriate uses of Big Data, this Article would be remiss if it did not note that the Obama campaign took advantage of Big Data itself. Lois Beckett, *Everything We Know (So Far) About Obama's Big Data Tactics*, PROPUBLICA (Nov. 28, 2012, 10:45 AM), https://www.propublica.org/article/everything-we-know-so-far-about-obamas-big-data-operation. The campaign used cookies to advertise to people who had previously visited the campaign website and to determine television-watching habits for certain groups of potential voters in order to decide where to place its television ads. It would also be remiss of this Article to not mention that both national political parties have targeted advertisements in this manner. Lois Beckett, *How Microsoft and Yahoo Are Selling Politicians Access to You*, PROPUBLICA (June 11, 2012, 11:45 AM), https://www.propublica.org/article/how-microsoft-and-yahoo-are-selling-politicians-access-to-you.

[164] SEIZING OPPORTUNITIES, *supra* note 42, at 79. Over 24,000 people responded to the survey, but "this process was a means of gathering public input and should not be considered a statistically representative survey of attitudes about data privacy." *Id.*

[165] The FTC enforces the sector-specific statutes referenced *supra* pp. 21–22.

[166] Federal Trade Commission Act, 15 U.S.C. § 43 (2012).

[167] Bennett, *supra* note 63, at 907–08.

1. The Commission's Self-Regulatory Principles

The FTC created a set of Self-Regulatory Principles, revised in 2009, to guide companies engaged in behavioral advertising.[168] The scope of these four principles is quite limited. First, the principles do not apply to all non-advertising behavioral targeting. The FTC chose to exclude other types of behavioral targeting from the scope of these principles due to its lack of information on the uses of data in non-advertising contexts.[169] Thus, "the principles do not address any of the privacy risks associated with consumer profiling for purposes other than behavioral advertising." Second, the principles do not apply to "first party" targeting—behavioral advertising by and on one website[170]—because such targeting "is more likely to be consistent with consumer expectations, and less likely to lead to consumer harm, than other forms of behavioral advertising."[171] Likewise, the principles do not apply to contextual advertising, which occurs when an advertisement is displayed on a webpage simply based on the content of that webpage.[172] This exclusion results from the FTC staff's belief that contextual advertisements are likely to be less invasive than other behavioral advertisements.[173]

2. The Federal Trade Commission's 2012 Report

In 2012, the FTC further revised its privacy framework and recommended that Congress enact legislation protecting consumers from the unauthorized collection and use of their data.[174] The report promoted three baseline principles. First, the FTC believed that companies should

---

[168] Dustin D. Berger, *Balancing Consumer Privacy with Behavior Targeting*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 3, 43 (2011). The four principles are: Transparency and Consumer Control; Reasonable Security, and Limited Data Retention, for Consumer Data; Affirmative Express Consent for Material Changes to Existing Privacy Promises; and Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising. FED. TRADE COMM'N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 46–47 (Feb. 2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf [hereinafter SELF-REGULATORY PRINCIPLES].

[169] Berger, *supra* note 168, at 44.

[170] SELF-REGULATORY PRINCIPLES, *supra* note 168, at iii.

[171] *Id.*

[172] Berger, *supra* note 168, at 44.

[173] SELF-REGULATORY PRINCIPLES, *supra* note 168, at iii.

[174] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE at iv, vii (Mar. 2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter PROTECTING CONSUMER PRIVACY].

"promote consumer privacy throughout their organizations and at every stage of the development of their products and services."[175] Second, companies should simplify consumer choice. That is, companies should not be required to obtain consumer consent before collecting and using data as long as those practices are consistent with the context of the transaction or the consumers' relationship with the company.[176] However, companies should be required to obtain affirmative express consent if they want to (1) use consumer data in a manner that materially differs from the manner in which the data was first collected or (2) collect sensitive data.[177] The last baseline principle stated that companies should increase transparency when collecting and using data. This principle called for privacy notices provided to consumers, reasonable access to data collected, and the expansion of efforts to educate consumers about data privacy practice in the commercial context.[178]

As part of the report, the Commission decided to focus on five major policymaking efforts: the implementation of a Do Not Track[179] function on websites; improved privacy protections from companies providing mobile services; the increase in transparency and control of data brokers' collection and use of consumer information; a discussion on privacy concerns related to the comprehensive tracking of large platform providers, such as Internet Service Providers ("ISPs"), operating systems, and browsers; and the promotion of enforceable self-regulatory codes.[180] Unfortunately, the Commission's efforts did not lead to legislation protecting data privacy. However, the Commission did foster discussions and encourage the creation of various privacy initiatives by private parties.[181]

---

[175] *Id.* at vii.
[176] *Id.*
[177] *Id.* at viii.
[178] *Id.*
[179] "Do Not Track" is a policy that allows web users to opt-out of cross-site tracking. *See* SEIZING OPPORTUNITIES, *supra* note 42, at 42–43 (explaining challenges with "Do Not Track").
[180] *Id.* at iv–vii.
[181] *See* FED. TRADE COMM'N, MOBILE POLICY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 20–21 (Feb. 2013), *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (discussing various "Do Not Track" initiatives implemented by private companies, including Apple, and calling the development of further mechanisms).

3. Mobile Policy Disclosures

The FTC hosted a panel discussion on mobile privacy in May 2012, with the goal of finding ways to "build trust through transparency."[182] The FTC used the insights and information shared at this discussion, along with its prior work and written submissions to inform the report on Mobile Policy Disclosures it released in 2013. The Report, which focuses on transparency, "offers several suggestions for the major participants in the mobile ecosystem as they work to improve mobile privacy disclosures."[183]

The FTC made several recommendations pertaining to the collection and use of data. For example, the FTC recommended that platforms, or operating systems providers, obtain affirmative express consent from consumers before allowing apps to access sensitive data, like a user's geolocation.[184] Platforms were also encouraged to develop icons for apps to communicate to users when the app was transmitting user data.[185] Additionally, the FTC encouraged platforms to consider providing consumers with information about the extent to which the platform reviews apps and conducts compliance checks once the apps were placed in app stores.[186]

The Mobile Policy Disclosures also contained recommendations for app developers and advertisers. These recommendations encouraged truthful disclosures to consumers and the obtainment of affirmative expressive consent before collecting or using sensitive data.[187]

Unfortunately, without Congress's enactment of a statute pertaining to mobile disclosures, the FTC's recommendations are little more than suggestions. Failure to comply with the recommendations will not result in criminal or civil action, so businesses do not legally have to disclose whether and how they collect data from consumers.

III. AUDIO DATA AND DIGITAL EAVESDROPPING

From individuals oversharing with businesses to companies taking advantage of vulnerable groups to the lack of transparency around the collection and use of data, the privacy concerns provoked by the collection of large datasets in general are also provoked by the collection

---

[182] *Id.* at 1.
[183] *Id.* at i.
[184] *Id.* at i.–ii.
[185] *Id.*
[186] *Id.*
[187] *Id.* at ii–iii.

of audio data in particular. Data carries the potential to reveal sensitive information about users, and audio data only exacerbates that potential.

Consumer privacy legislation should focus not only on the content of the data collected, but also the source of that data. As described earlier, many people have become suspicious that businesses are listening to their private conversations in order to target advertisements. Many consumers own at least one "always listening" technology, such as an iPhone with the "Hey Siri" feature enabled. These technologies are capable of collection, recording, and using audio data. In a Q&A with the online newspaper, TechCrunch, Apple explained how its "always on" technology works:

> [A]udio from the microphone is continuously compared against the model, or pattern, of your personal way of saying 'Hey Siri' that you recorded during setup of the feature. Hey Siri requires a match to both the 'general' Hey Siri model (how your iPhone thinks the words sound) and the 'personalized' model of how *you* say it. This is to prevent other people's voices from triggering your phone's Hey Siri feature by accident.
>
> Until that match happens, *no audio is ever sent off of your iPhone*. All of that listening and processing happens locally.
>
> The "listening" audio, which will be continuously overwritten, will be used to improve Siri's response time in instances where the user activates Siri," says Apple. The keyword there being 'activates Siri.' Until you activate it, the patterns are matched locally, and the buffer of sound being monitored (from what I [the author of the article] understand, just a few seconds) is being erased, un-sent and un-used — and unable to be retrieved at any point in the future.[188]

Once Siri has been triggered, the audio information is then sent to Apple and associated with the user's device.[189] The user has technically "approved" Apple's use of this data by requesting Siri to respond to a query.[190] Apple claims "in no case is the device recording what the user says or sending that information *to Apple* before the ['Hey Siri'] feature is triggered."[191]

Apple's statement that no data is recorded or sent before the match is made still leaves users exposed to the unauthorized collection of their audio data. While Apple may not collect the data, a company who has developed an application compatible with Apple's operating system could.

---

[188] Panzarino, *supra* note 19.
[189] *Id.*
[190] *Id.*
[191] *Id.* (emphasis added).

And just as Apple has obtained a minimal level of "consent" for *some* use of the data, so have these developers.

For example, a user, enticed by the relatively new "Live" feature on social media apps like Facebook, could decide to share a video with the friends and family with whom she has online relationships. Before she can record this video using her smartphone, she must enable microphone and video permissions on the Facebook app. Because the permissions align exactly with what the user wants her technology to do, she accepts. Unless the user goes back into her settings and disables the microphone permissions, Facebook remains able to access her audio data.

The user in the above example has consented to Facebook's use of that specific audio data in her video, but has not consented to the use of *all* audio data that could possibly be collected. Yet, because the user has an "always on" technology, Facebook could potentially collect audio data even when the user is not currently activating the recording features of her app. Further, Facebook could store that audio data and use it to deliver advertisements specifically targeted at that user.

"Always on" technologies demonstrate the ability of technology to constantly collect and respond to audio data. While it seems intuitive that the same technologies would be regulated similarly, the previous sections have shown that self-regulation in place in the United States does not sufficiently limit companies' ability to use technologies to collect information from unwitting consumers. With the federal government's lack of involvement, little incentive exists for operating system providers, app developers, and social media websites to follow the self-regulatory principles protecting consumers' privacy.

A. Operating System Providers' Policies for App Developers

Although app developers are capable of collecting audio data with users' informed consent, operating system providers' policies may inhibit the data collection. The following subsections briefly examine the policies of three of the biggest companies with operating systems and voice assistants—Google, Apple, and Microsoft. Through their individual privacy policies, these companies either state that (1) the data collected and recorded by their voice assistants is not used or shared with third parties or (2) neglect to mention explicitly if and how the audio data is used.

1. Google

Google, the developer of the operating system on Android smartphones, frequently rolls out changes to its virtual assistant—Google

Assistant.[192] Like many other virtual assistants, Google Assistant can respond to audio data.[193] A user may trigger the Assistant by using a "Hey Google" or "OK, Google" command. [194] Because of the ability to trigger the Assistant solely with audio, Google Assistant is another "always on" technology. However, Google claims that it "categorically does not use what it calls 'utterances' – the background sounds before a person says, "OK Google" to activate voice recognition" for advertising or other purposes.[195]

Google also collects information from users of its other services. Google uses this information—which includes a user's name, address, credit card number, device information, location information, and information on how an individual uses Google's services (including websites that use Google's advertising services)—learn about its users and to deliver advertisements.[196]

Google's content policy for app developers prohibits developers from collecting information without the user's knowledge.[197] Developers must be transparent about how they collect, use, and share data.[198] Apps that violate this rule are removed from the Google Play store. Yet, the content policy does not contain any guidelines to determine what level of consumer awareness qualifies as "knowledge." Google also requires developers to "[r]equest permissions in context where possible" so that users may understand why the developer needs access to the data.[199] Developers should not request access to information that is unnecessary to utilize features of the app.[200] It is unclear how or if Google enforces these provisions of its privacy policy. Because Google does not build into its

---

[192] *See* Julian Chokkatu, *EverythingYou Need to Know About Google Assistant*, DIGITAL TRENDS (Apr. 11, 2018, 8:16 AM), https://www.digitaltrends.com/mobile/google-assistant/.

[193] *Id.* Google also has a voice search feature. A user who has conducted a voice search can find a list of audio recordings and listen to them. However, these audio recordings are the result of actual searches, which means that user is presumably aware that Google is listening to her audio.

[194] Chokkatu, *supra* note 192.

[195] Kleinman, *supra* note 14.

[196] *Privacy Policy*, GOOGLE (Dec. 18, 2017), https://www.google.com/policies/privacy/.

[197] *Id.*; *Privacy, Security, and Deception: User Data*, GOOGLE PLAY: DEVELOPER POLICY CENTER, https://play.google.com/about/privacy-security-deception/privacy-shield/ (last visited Apr. 24, 2018).

[198] *Privacy, Security, and Deception: User Data*, *supra* note 197.

[199] *Privacy, Security, and Deception: Permissions*, GOOGLE PLAY: DEVELOPER POLICY CENTER, https://play.google.com/about/privacy-security-deception/permissions/ (last visited Apr. 24, 2018).

[200] *Id.*

software measures to force developers to ask for permission before collecting audio data, Google could very well be ignorant to its developers' malfeasances.

2. Apple

Apple requires app developers to follow a policy to "Support User Privacy."[201] Apple instructs developers to review applicable "guidelines from government or industry sources"[202]—like the FTC's report on mobile privacy and the European Union's Data Protection Commissioner's Opinion on data protection for mobile apps.[203] Developers must also request permission to access "sensitive user or device data" at the time the application needs the data, and may only request the minimum amount of data needed to accomplish a given task.[204] The developer must be transparent with how the data will be used and give the user control over the data. As with Google, it is unclear what enforcement mechanisms Apple has implemented.

Apple's policy seems to prohibit the collection of audio data without the user's knowledge. However, Apple's app developers could potentially write apps that obtain microphone data without asking for permission from the device owner. Additionally, app developers could seek permissions to collect data for an initial, legitimate use and their subsequent collections of data for other uses will most likely not be discovered.

3. Microsoft

Microsoft, which owns Bing and the virtual assistant Cortana, admits that it collects data from consumers who use its services, including the voice services offered by Cortana.[205] Microsoft further contends that it uses the data collected to help show relevant ads for its products and products offered by third parties.[206] However, Microsoft claims to not use

---

[201] *App Programming Guide for iOS*, APPLE.COM, https://developer.apple.com/library/content/documentation/iPhone/Conceptual/iPhoneOSProgrammingGuide/ExpectedAppBehaviors/ExpectedAppBehaviors.html#//apple_ref/doc/uid/TP40007072-CH3-SW6 (last visited Apr. 24, 2018).
[202] *Id.*
[203] *See generally Opinion 02/2013 of the Art. 29 Data Protection Working Party on Apps on Smart Devices* (Feb. 27, 2013).
[204] *App Programming Guide for iOS*, *supra* note 201.
[205] Microsoft Privacy Statement, MICROSOFT, https://privacy.microsoft.com/en-us/privacystatement (last visited Apr. 24, 2018). ("Microsoft collects data to operate effectively and provide you the best experiences with our products. You provide some of this data directly . . . .").
[206] *Id.*

information from users' emails, chats, video calls or voicemails, or other personal files to target advertisements to users.[207]

B. Social Media Advertising Policies

Before the soon-to-effective European Union General Data Protection Regulation (GDPR)[208] loomed over their executives' heads, social media websites also left some questions unanswered in their policies. The sites all indicated in their advertising policies that they use data collected to target advertisements to users,[209] but none of these policies detailed the full extent of the sources of that data.[210] Several websites recently updated their privacy policies to comply with the GDPR by its effective date of May 25, 2018, and thus increased the specificity of the potential uses of consumer data.[211] For instance, Facebook previously stated that it "collect[s] information from or about the computers, phones, or other devices where you [presumably, a user of Facebook's services] install or access our Services, depending on the permissions you've granted."[212] In the corresponding section for its new privacy policy, Facebook states "we collect information from and about the computers, phones, connected TVs and other web-connected devices you use that integrate with our Products, and we combine this information across different devices you use" and significantly expands the examples of information obtained from users' devices.[213] Still, neither disclosure addresses whether the broad "information" includes audio information. Facebook has denied the use of audio data in behavioral advertisements

---

[207] *Id.*

[208] *See generally EU GDPR Portal*, EUGDPR.ORG, https://www.eugdpr.org (last visited Apr. 24, 2018).

[209] See *Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/ (last visited Apr. 24, 2018); *How Does Instagram Decide Which Ads to Show Me?*, INSTAGRAM, https://help.instagram.com/173081309564229 (last visited Apr. 24, 2018; *Twitter Privacy Policy*, TWITTER, https://twitter.com/privacy?lang=en (last visited Apr. 24, 2018).

[210] *See id.* (using phrases like "such as" and "can include" to provide a non-exhaustive list of possible sources of data). While it might be overly time-consuming and unreasonable for websites to provide a list of *all* potential sources of data, the ambiguity created by the non-exhaustive language could be resolved by statements listing which potential sources are *not* used to collect data.

[211] *See Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy /update (last visited Apr. 24, 2018) [hereinafter *New Data Policy*]; *Twitter Privacy Policy*, TWITTER, https://twitter.com/privacy?lang=en#update (last visited Apr. 24, 2018) (effective as of May 25, 2018).

[212] *Data Policy*, *supra* note 209.

[213] *New Data Policy*, *supra* note 211.

on other mediums,[214] but has yet to be fully transparent with consumers about its data collection processes.

IV. MEANS OF PROTECTING CONSUMERS AGAINST DIGITAL EAVESDROPPING

Although no company has admitted to the unauthorized collection of audio data, "always listening" technologies do have the capabilities of recording and analyzing audio data without a user's consent. Instead of just taking companies at their word, we should assume that at least some of these for-profit companies are opportunistic enough to take advantage of those technological capabilities.[215]

As stated above, the unauthorized collection of audio data essentially invokes two main concerns. First, consumers have not consented to the collection of the audio. Second, audio data can be used to perpetuate discrimination in advertising. Audio data can reveal all sorts of information about people—such as their dialect or place of origin, place of employment, sexual orientation, gender, or secrets they only feel comfortable sharing with their closest friends—of which ill-intentioned businesses could take advantage. A measure restricting the collection of audio data should acknowledge these two concerns, as well as promote

---

[214] Facebook's Vice President of Product, Ads and Pages, Rob Goldman tweeted: "I run ads product at Facebook. We don't - and have never - used your microphone for ads. Just not true." Rob Goldman (@robjective), TWITTER (Oct. 26, 2017, 1:39 PM), https://twitter.com/robjective/status/923620196010434560. Facebook also released its own short denial:

> Facebook does not use your phone's microphone to inform ads or to change what you see in News Feed. Some recent articles have suggested that we must be listening to people's conversations in order to show them relevant ads. This is not true. We show ads based on people's interests and other profile information – not what you're talking out loud about. We only access your microphone if you have given our app permission and if you are actively using a specific feature that requires audio. This might include recording a video or using an optional feature we introduced two years ago to include music or other audio in your status updates.

Facebook Does Not Use Your Phone's Microphone for Ads or News Feed Stories, *supra* note 15. Heed the same warning given *supra* note 15.

[215] Note: this assumption should be made only when the companies' privacy policies do not explicitly prohibit the collection and use of audio data. Other legal means of recourse would exist if companies were continually violating their own privacy policies, and most companies would not knowingly put themselves at such risk.

fair information practice principles.[216] Further, a national approach should be taken, as a framework with state-specific protections would mean that consumers are not protected equally across the board.

A. The "Do Nothing" Approach

The first way Congress can regulate audio data collection is by simply doing nothing. This does not mean that no regulations will be crafted; it just means that Congress will continue to stay out of it. Rather than have lawmakers with no technical knowledge trying to anticipate and respond to technological developments, Congress can trust businesses to protect consumers' interests. Those businesses can create their own guidelines for operators and app developers to follow. Individuals who feel as if they have been harmed by the businesses' practices can use other means of legal recourse to rectify those injuries.[217] Or consumers who want to avoid being harmed altogether can choose to disengage from the technology. The market will police businesses' harmful practices and will lead them to enact appropriate protections eventually.

Unfortunately, the current market-based policing mechanism inadequately protects consumers. For the mechanism to work, businesses must be transparent about the ways in which they collect and use audio data.[218] Otherwise, individuals cannot appropriately value their personal information, as is necessary in a market.[219] Further, this solution does not address the realities of disengagement. Technology is practically inescapable in modern society; nearly every adult owns a smart device that is capable of recording audio, which means even if a consumer decides to not have his own "always listening" device, he could still have several people in his life whose devices could collect audio information when around him. Also, it is likely that companies will continue to prioritize their own financial interests over consumers' interests if not regulated.

B. The "Consent Approach"

Instead of doing nothing, Congress could create a regulation giving consumers the ability to opt-in or opt-out of audio data collection. While some businesses give consumers the ability to opt-out of targeted

---

[216] Note: the solutions do not endorse one particular set of FIPPs. Rather, they include elements of various principles, most notably the principle pertaining to notice or transparency, choice, and collection limitations.

[217] Such a consumer could potentially claim torts like invasion of privacy, false light or false publicity, or misappropriation, but these torts were not developed to remedy injuries caused by the collection of data. *See* James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 30 (2003).

[218] *Id.* at 62.

[219] *Id.*

advertising, consumers often are not able to opt out of the underlying data collection itself.[220] Even if consumers do not receive targeted ads, businesses could still collect information, including audio information, and could use that data for other purposes.

An opt-in solution would require an app developer to ask a user for permission every time it wanted to access the users' microphone. This solution could empower consumers, but it could also be time-consuming and inefficient. With an opt-out solution, on the other hand, businesses could collect and use data with users' implied consent. For this solution to effectively prevent potential privacy harms, consumers would need to be informed of the data collection processes and would require greater transparency from companies.[221] Additionally, measure preventing companies from circumventing opt-out requirements would need to be created.[222]

A statute similar to the BROWSER Act, which allows consumers to opt-in to the collection of sensitive information and to opt-out of the collection of non-sensitive information, could be an effective solution.[223] However, unlike the BROWSER Act, the statute should not preempt state-

---

[220] *See* FED. TRADE COMM'N, FTC CROSS-DEVICE TRACKING WORKSHOP, SEGMENT 1 TRANSCRIPT (2015), *available at* https://www.ftc.gov/system/files/documents/videos/cross-device-tracking-part-1/ftc_cross-device_tracking_workshop_-_transcript_segment_1.pdf. (quoting then-Chairwoman of the FTC Edith Ramirez).

[221] The European Union proves it is possible to have informed consumers and transparency from companies. The European Data Protection Directive adopted an opt-out system for the installation of cookies. *See* Ignacio N. Cofone, *The Way the Cookie Crumbles: Online Tracking Meets Behavioral Economics*, 25 INT'L J.L. INFO. TECH. 38, 40–41 (2017). Additionally, many companies offer European consumers tools that increase the users' control over their information. *See* CTR. FOR DEMOCRACY & TECH., Re: Informational Injury Workshop P175413, (Oct. 27, 2017), *available at* https://cdt.org/files/2017/10/2017-1027-CDT-FTC-Informational-Injury-Comments.pdf (referencing data protection in the European Union).

[222] Companies have been able to ignore users' requests to opt-out of data collection. For example, a company called AddThis was able to track individual's website activity across various websites, from WhiteHouse.gov to Pornhub.com, without the website owner's awareness. This technology is hard to block and can't be prevented "by using standard Web browser privacy settings or using anti-tracking tools." Julia Angwin, *Meet the Online Tracking Device That is Virtually Impossible to Block*, PROPUBLICA (July 21, 2014, 9:00 AM), https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block.

[223] BROWSER Act of 2017, H.R. 2520, 115th Cong. (2017).

mandated consumer privacy protections broadly, as that would undo the protections created by proactive states like California.[224]

C. The "Ill Purpose Approach"

Congress could also enact legislation that requires stronger enforcement of anti-discrimination laws. Companies using audio data for ill purposes would be prohibited from displaying advertisements. However, one challenge would be identifying which party should bear the burden of enforcement: operators, application developers, or a government agency like the FTC. Monitoring advertisements on every website could be costly and cumbersome for any of these parties, but application developers are probably best suited for the task since the advertisements would appear on their webpages. Further, companies that collect the data used for advertising purposes themselves—like Facebook which classifies its users based on the data—could be legally prohibited from collecting data for discriminatory uses. However, the companies would need to be transparent about their data collection and data use practices. Such a regulation would probably not target audio data alone, as distinguishing the sources of the exact data used for discriminatory purposes would make the law difficult to enforce.

CONCLUSION

Lawmakers should take some combination of the "Consent Approach" and the "Ill Purpose Approach" to protect consumers from digital eavesdroppers. The legislation should seek to balance consumers' privacy concerns with their desires for businesses to take their preferences into account. As described throughout this Article, technology has immense capabilities to help, but also to harm. Big Data gives businesses an unprecedented amount of knowledge about consumers, enabling them to predict and shape consumers' behavior. But knowledge is power.

---

[224] California has enacted (and attempted to enact) several acts that protect the privacy interests of its citizens. For example, in 2003, California became the first state to require companies that collect personally identifiable information to provide privacy policies when it enacted the California Online Privacy Protection Act (CalOPPA) (2003). California Online Privacy Protection Act, Cal. Bus. & Prof. Code §§ 22575–22579 (2003). In 2013, state legislatures introduced a bill known as the Right to Know Act, which would give California residents the right to access data collected from them by companies whose services they were using. AB-1291, Reg. Sess. (Cal. 2013) This bill did not pass, but California has remained an advocate for consumer privacy rights. *See, e.g.*, Kamala D. Harris, Cal. Dep't of Justice, Privacy on the Go: Recommendations for the Mobile Ecosystem (2013), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf (offering recommendations to help app developers protect consumer privacy).

Without limitations on the exercise of this power, innovation can start to plague, rather than progress, society.