Catholic University Journal of Law and Technology

Volume 27 | Issue 1 Article 8

2018

Alexa, Who Owns My Pillow Talk? Contracting, Collaterizing, and Monetizing Consumer Privacy Through Voice-Captured Personal Data

Anne Logsdon Smith
Catholic University of America (Student)

ALEXA, WHO OWNS MY PILLOW TALK? CONTRACTING, COLLATERALIZING, AND MONETIZING CONSUMER PRIVACY THROUGH VOICE-CAPTURED PERSONAL DATA

Anne Logsdon Smith[*]

Household voice-activated digital assistant devices, such as Amazon's Echo and Google's Home, have ushered in a new era of personal data collection from consumers. Personal data is easier than ever to obtain and virtually impossible to delete from the service provider once it's transmitted from the capturing device.[1] Since these devices' relatively recent emergence in the mass market in 2015, more than 39 million consumers have incorporated them into their homes, and subsequently, their intimate lives.[2] Digital assistant devices continue to grow rapidly in popularity.[3] The data these devices acquire funnels into virtual acres

[*] The author is a 2018 graduate of the Catholic University of America, Columbus School of Law and holds B.A. and M.P.S. degrees from Georgetown University. She is a licensed attorney in Maryland specializing in commercial transactions, bankruptcy, real estate, and creditor-debtor law. The author would like to thank Professor Veryl Miles for her valuable instruction in contract law, the Uniform Commercial Code, and secured transactions, as well as for her guidance in writing this note. The author also appreciates the hard work and thorough editing by the dedicated staff of *the Journal of Law and Technology*. Finally, the author is grateful to her husband for his support and feedback throughout the writing process.

1 Stacey Gray, *Always On: Privacy Implications of Microphone-Enabled Devices*, FUTURE OF PRIVACY FORUM, at 3 (Apr. 2016), https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf.

2 Sarah Perez, *39 million Americans now own a smart speaker, report claims*, TECHCRUNCH (Jan. 12, 2018), https://techcrunch.com/2018/01/12/39-million-americans-now-own-a-smart-speaker-report-claims.

3 Mike Jeffs, *OK Google, Siri, Alexa, Cortana; Can you tell me some stats on voice search?*, BRANDED (Jan. 8, 2018) (stating that technology experts predict 50% of all searches will be voice searches, about 30% of searches will be done without a screen, and there will be 21.4 million smart speakers in the U.S. by 2020).

upon acres of servers across the globe.[4]

Forget Bitcoin—data is the digital economy's most valuable currency.[5] Google and Facebook boast some of the largest repositories of personal data, because of the free use of their digital applications and messaging services.[6] Google and Facebook also control a majority of the global market in online advertising, with their business model built squarely upon unrestricted access to this personal data.[7] As "surveillance capitalism" fuels what is expected to be a $203 billion-plus industry in "Big Data" and business analytics by 2020, companies and governments are racing to collect and collateralize this prized asset.[8]

Companies have engaged in fierce legal battles over ownership, possession, and, in some cases, repossession of certain consumer data.[9] Consumers have challenged corporate behemoths by asserting rights to data they allegedly generated.[10] Recently, the federal government interceded in corporate

---

4 Michael Kanellos, *152,000 Smart Devices Every Minute in 2025: IDC Outlines The Future of Smart Things* (Mar. 3, 2016, 6:25 PM), https://www.forbes.com/sites/michaelkanellos/2016/03/03/152000-smart-devices-every-minute-in-2025-idc-outlines-the-future-of-smart-things/#f2332d24b63e (predicting that the aggregate amount of data obtained from devices as part of the "internet of things" and other smart devices will exceed 44 zettabytes by 2020).

5 *See* Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1373 (2017) (discussing how companies monetize data); *see also* Michelle Evans, *Why Data Is The Most Important Currency Used In Commerce Today*, FORBES (Mar. 12, 2018, 7:24 AM), https://www.forbes.com/sites/michelleevans1/2018/03/12/why-data-is-the-most-important-currency-used-in-commerce-today/#75592dc854eb (discussing how data facilitates the transactional relationship between consumers and companies); Lowell Fryman, *Business Glossaries and Metadata: The "Value" of our Data Consumers*, DATA ADMIN. NEWSLETTER (Sept. 1, 2016), http://tdan.com/business-glossaries-and-metadata-the-value-of-our-data-consumers/20286 (proposing that "data is the new currency, and its value is in its usage.").

6 Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley —and Won*, N.Y. TIMES (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html.

7 *Id.*

8 Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 75 (2015) (defining surveillance capitalism as the rationale behind behavioral data accumulation, extraction, and analysis for purposes of commoditization and prediction); Gil Press, *6 Predictions For The $203 Billion Big Data Analytics* Market, FORBES (Jan. 20, 2017, 9:27AM), https://www.forbes.com/sites/gilpress/2017/01/20/6-predictions-for-the-203-billion-big-data-analytics-market/#756bfced2083.

9 *See* Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 428 (2018) (discussing the collateralization of consumer data); *see, e.g.*, *Experian Says Competitor Is Infringing Its Trademarks*, 18 W.L. J. INTELLECTUAL PROP. 11, 11 (2011) (discussing Experian's complaint against Practical Marketing, Inc.).

10 *See* Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN ST. L. REV. 777, 789-90 (2016) (discussing limited protections afforded to consumers against companies); Francesa Fontana, *Lawsuits Against Facebook Over Data Privacy*

bankruptcies and mergers involving the potential transfer of personal consumer data.[11] Even financially stable companies pledge enormous assets of personal consumer data as collateral.[12] These events give rise to an important question of whether companies should be collateralizing—that is, pledging an asset to the lender as security in the event the borrower defaults on the loan—data they may not be authorized to sell.[13]

Courts and legislatures have attempted to develop contract law, property law, secured transactions law, and statutes that balance parties' rights and obligations with respect to data. Despite these efforts, judicial hurdles and limited interpretations have precluded remedies under these legal approaches.[14] In some cases, part of the challenge stems from incompatible results arising out of differing legal approaches.[15]

This comment introduces the dynamics of voice-captured data in the scheme of Big Data while examining the implications of its collection and use under various laws. Part I investigates the mechanics of data collection and transmission via voice-enabled devices, along with data's progressive dissemination into the stream of commerce. Part II probes the legal classification of voice-captured data, which eludes clear-cut categorization by virtue of its

---

Issues Are Piling Up, THESTREET (Mar. 27, 2018), https://www.thestreet.com/story/14536213/1/everyone-who-is-suing-facebook-for-cambridge-analytica.html (describing 16 pending lawsuits over breaches of user privacy related to Facebook); *see, e.g.*, Kaye Wiggins et al., *Google Sued Over Privacy on Behalf of 5 Million iPhone Users*, BLOOMBERG (Nov. 30, 2017, 8:18 AM), https://www.bloomberg.com/news/articles/2017-11-30/google-sued-over-data-claims-on-behalf-of-5-million-iphone-users (discussing U.K. consumers' claims that Google improperly misused their personal data).

11 Luis Salazar, *The most dangerous intersection–bankruptcy and consumer privacy*, PRIVACY ADVISOR (June 1, 2009), https://iapp.org/news/a/2009-06-bankruptcy-and-consumer-privacy.

12 Natasha Singer & Jeremy B. Merrill, *When a Company Is Put Up for Sale, in Many Cases, Your Personal Data Is, Too*, N.Y. TIMES (June 28, 2015), https://www.nytimes.com/2015/06/29/technology/when-a-company-goes-up-for-sale-in-many-cases-so-does-your-personal-data.html (discussing how prominent companies like Facebook and Apple provide policies that consumer data may be transferred if a merger or other transaction occurs in their terms of service).

13 Xuan-Thao N. Nguyen, *Collateralizing Privacy*, 78 TUL. L. REV. 553, 587-95 (2004).

14 Consumer Privacy Protection Act of 2017, S. 2124, 115th Cong. 1st Session (2017); *see, e.g.*, Carlsen v. GameStop, Inc., 833 F.3d 903, 911 (8th Cir. 2016) (holding that a website operator who allegedly disclosed personal user information did not breach a contract because the terms of use did not provide that the website would not disclose user information); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 968 (7th Cir. 2016) (holding that plaintiffs whose data was breached by the chain restaurant did not have a property right to their personally identifiable data); Apple, Inc. v Superior Court, 292 P.3d 883, 896 (Cal. 2013) (holding that merchant defendant was not prohibited from recording personal identification information of consumers for downloadable products).

15 *See* Nguyen, *supra* note 13, at 593-99 (discussing different governmental regulatory approaches of consumer privacy collateralization).

changeable form, ownership, and function. After evaluating voice-captured data's simultaneous character as original speech, personal information, and a sellable commodity, Part III will discuss the conflicting interests surrounding the use of voice-captured personal data and identify the weaknesses in the predominant legal frameworks through which the chain of ownership is currently analyzed.

Part IV proposes different ways of applying existing legal principles, as well as new federal legislation, to better align and distribute these interests among stakeholders of voice captured data. Property law's legal framework is well-suited to handle such data ownership since it allows shared ownership with multiple concurrent users of the same asset and recognizes public rights in private property.[16] Adjusting the process by which security interests in voice-captured data are created and enforced may help protect the data's integrity while minimizing unintended transfers that may harm consumers.[17] Ultimately, statutory relief may be the best method to protect and restore certain rights to consumers in their own voice-captured personal data.

I. COLLECTION AND USE OF VOICE CAPTURED PERSONAL DATA

A. What Are Voice-Activated Digital Assistant Devices, and How Do They Work?

A voice-activated digital assistant device, also known as a "voice assistant" or "smart speaker," is an "intelligent voice recognition and natural language understanding service that allows [users] to voice-enable any connected device that has a microphone and speaker."[18] Popular devices include the Amazon Echo (also called "Alexa") and Google Home.[19] These devices can perform a variety of tasks including answering questions, sending messages, playing audio books or music, paying bills, tracking packages, and controlling smart-home

---

16 *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2057–58 (2004) (discussing competing legal theories of treating personal data as property).

17 *See e.g.*,Danita Arrowood et. al., *Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 update)*, J. AM. HEALTH INFO. MGMT. ASS'N, 58-62 (2013) (illustrating the need for a process to secure dictated data in the healthcare sphere).

18 Kim Wetzel, *What is Alexa? It's Amazon's new virtual assistant*, DIGITAL TRENDS (May 11, 2018, 11:09 AM), https://www.digitaltrends.com/home/what-is-amazons-alexa-and-what-can-it-do.

19 *Id.*; Jenny McGrath, *Google Home review*, DIGITAL TRENDS (May 20, 2018, 08:00 AM), https://www.digitaltrends.com/smart-home-reviews/google-home-review.

appliances.[20]

Smart-speakers have been integrated into multiple forms of electronic devices, including televisions, phones, cars, cameras, and even lamps.[21] As novel as smart devices seem today, voice-enabled technology has been utilized in consumer technology for over two decades. For example, in 1992, the automobile industry debuted voice-activated, on-board GPS systems in cars.[22] In 2012, Samsung introduced their "Smart TV"; the first television with a smart speaker.[23] And finally, Microsoft launched Cortana on Windows 10 desktops and mobile devices in 2015.[24]

To enable the voice-assistant device to transmit queries and retrieve responses, the user must link it to a specified personal account, such as their Amazon or Apple account.[25] Google and Amazon have enabled their devices to distinguish between multiple users and associate their voice with their own personal account.[26] Google Home is capable of recognizing up to six users' voices and answering their queries based on their Google account.[27] While, Alexa can switch user accounts on demand.[28] Nevertheless, individuals who do not have an associated account with the device's company can still activate and generate recorded data to the server.[29]

---

20 Thuy Ong, *39 million Americans reportedly own a voice activated smart speaker*, THE VERGE (Jan. 15, 2018, 4:53 AM), https://www.theverge.com/2018/1/15/16892254/smart-speaker-ownership-google-amazon; Wetzel, *supra* note 18.

21 Chris Kelly, *Amazon integrates an improved Alexa throughout homes and in cars with new hardware*, MOBILE MARKETER (Sept. 21, 2018), https://www.mobilemarketer.com/news/amazon-integrates-an-improved-alexa-throughout-homes-and-in-cars-with-new-h/532882/; Wetzel, *supra* note 18.

22 *Know Everything About Satellite Navigation in Cars*, AUTOPORTAL (Jan. 13, 2015), https://autoportal.com/articles/know-everything-about-satellite-navigation-in-cars-2867.html (stating that Toyota debuted the voice assisted GPS navigation system in its 1992 Celsior model car).

23 *[Infographic] History of Samsung Smart TV*, SAMSUNG NEWSROOM (Apr. 21, 2015), https://news.samsung.com/global/infographic-history-of-samsung-smart-tv.

24 Jacob Kastrenakes, *Microsoft unveils Cortana for Windows 10*, THE VERGE, (Jan. 21, 2015), https://www.theverge.com/2015/1/21/7866741/cortana-windows-10-announced-microsoft.

25 Tim Moynihan, *ALEXA AND GOOGLE HOME RECORD WHAT YOU SAY, BUT WHAT HAPPENS TO THAT DATA?*, WIRED (Dec. 5, 2016, 9:00 AM), https://www.wired.com/2016/12/alexa-and-google-record-your-voice.

26 Rob LeFebvre, *Amazon's Alexa can recognize the voices of multiple users*, ENGADGET (Oct. 11, 2017), https://www.engadget.com/2017/10/11/amazon-alexa-multiple-users; Tess Townsend, *Google Home can now recognize different users by their voice*, RECODE (Apr. 20, 2017, 12:00 PM), https://www.recode.net/2017/4/20/15364120/google-home-multiple-accounts.

27 Townsend, *supra* note 26.

28 Taylor Martin, *How to set up and use multiple accounts on Amazon Echo*, CNET (Feb 21, 2016, 6:30 AM), https://www.cnet.com/how-to/how-to-set-up-and-use-multiple-accounts-on-amazon-echo.

29 James Stables, *Multiple Alexa accounts: How to create household profiles and use*

The device is programmed to respond to an activation word or an "awake word".[30] Once the activation word triggers the device, it sends a visual signal that it's ready to interact, such as a flash of light at the crown of the speaker.[31] The devices themselves have a relatively limited understanding of speech.[32] Without further assistance, the devices are only programmed to understand their respective wake words, and can only respond if connected to the Internet.[33] To instantly interact with users, the device is technically always listening and can remain in "awake" mode even when its signal does not indicate it is awake.[34] Users also report inadvertent activation of voice-activated devices.[35] Any voice within audible range of the device can activate it by pronouncing its awake word—this includes voices originating from electronic sources such as televisions and audio players.[36]

Once the device picks up the wake word, it begins recording the user's speech and the ensuing conversation.[37] The device wirelessly transmits the recorded speech to a remote server, then the remote server processes the query and sends back an appropriate response based on information it procures.[38] Operating as a control center, the remote servers can immediately transmit customized information from thousands of miles away to the comfort of a user's home.[39] Half of surveyed device owners reported using their device in a common room such as a living room, one-quarter reported using it in the bedroom, and the third

---

voice profiles, THE AMBIENT (July 27, 2018), https://www.the-ambient.com/how-to/multiple-alexa-accounts-voice-profiles-513.

30 Anne Pfeifle, *Alexa, What Should We Do About Our Privacy? Protecting Privacy for Users of Voice-Activated Devices*, 93 WASH. L. REV. 421, 421-22 (2018); Jon Martindale, *Cortana vs. Siri vs. Google Assistant*, DIGITAL TRENDS (Aug. 12, 2018), https://www.digitaltrends.com/computing/cortana-vs-siri-vs-google-now.

31 Moynihan, *supra* note 25; Wetzel, *supra* note 18; *see e.g.*, Taylor Martin, *What the light ring colors on Amazon Echo spea*kers mean, CNET (June 26, 2017, 3:37 PM), https://www.cnet.com/how-to/light-ring-colors-amazon-echo-alexa.

32 Moynihan, *supra* note 25.

33 *Id*.

34 *Id.*; *Are Google Home and Amazon Echo listening more than you realize?* CBS NEWS (Dec. 14, 2017, 7:45 AM), https://www.cbsnews.com/news/google-home-amazon-echo-patents-track-listen.

35 Ananya Bhattacharya, *Amazon's Alexa heard her name and tried to order up a ton of dollhouses*, QUARTZ (Jan. 7, 2017), https://qz.com/880541/amazons-amzn-alexa-accidentally-ordered-a-ton-of-dollhouses-across-san-diego.

36 *Id.*; Sara Chodosh, *How to keep your kid from ordering four pounds of cookies with Amazon's Alexa*, POPULAR SCI. (Jan. 6, 2017), https://www.popsci.com/how-to-stop-amazon-alexa-buying-things-you-dont-want.

37 Bhattacharya, *supra* note 36.

38 Moynihan, *supra* note 25.

39 *Id.*; Nick Statt, *Amazon may give app developers access to Alexa audio recordings*, THE VERGE (Jul 12, 2017, 2:51 PM), https://www.theverge.com/2017/7/12/15960596/amazon-alexa-echo-speaker-audio-recordings-developers-data.

most common room was the bathroom.[40]

B. What Happens to the Data Captured?

The physical device does not locally store the voice data it captures; instead the recordings are stored on Amazon or Google servers.[41] It captures this data even when the device is offline.[42] Google's device records a speaker's voice and other audio, including a few seconds of sound before the activation.[43] Users who have examined the recorded data, either via a separate app or by playing it back from the device, have discovered unexpectedly recorded voice data.[44] Users may delete some of the data on most devices, or may mute the device to prevent further recording.[45]

However, the recorded data transmitted to the remote servers remains in the companies' databases.[46] Amazon, Google, and Apple claim to use this data to enhance the systems' functionality, improve speech recognition, better understand voice commands, and provide a more customized user experience.[47] Microsoft allegedly set up fake apartments for the sole purpose of recording and analyzing speech patterns.[48]

While these companies may legitimately stockpile millions of users' conversations to analyze their voices and preferences as a means to improve the product, some groups have expressed concern over selling this data to third-parties.[49] With companies such as Amazon and Google continuously collecting

---

40 Dave Chaffey, *Consumer use of voice-controlled digital assistants / smart speakers*, SMART INSIGHTS (Jan. 15, 2018), https://www.smartinsights.com/digital-marketing-strategy/consumer-use-of-voice-controlled-digital-assistants-smart-speakers.

41 Mary Hanbury, *Amazon's Alexa keeps recordings of your voice – here's how to listen to them*, BUSINESS INSIDER (May 25, 2018, 11:56 AM), https://www.businessinsider.com/amazon-alexa-voice-recordings-how-to-access-them-2018-5.

42 Moynihan, *supra* note 25; Tim Collins, *Google and Amazon really DO want to spy on you: Patent reveals future versions of their voice assistants will record your conversations to sell you products*, DAILY MAIL (Dec.15, 2017, 10:28 AM), http://www.dailymail.co.uk/sciencetech/article-5182577/How-Google-Amazon-SPYING-you.html; Sharon Profis & Rick Broida, *Amazon Echo saves all your voice data. Here's how to delete it.*, CNET (May 31, 2018, 11:50 AM), https://www.cnet.com/how-to/amazon-echo-saves-all-your-voice-data-heres-how-to-delete-them/.

43 Collins, *supra* note 42.

44 *Id.*

45 *See generally* Todd Haselton, *Amazon stores every conversation you have with Alexa – here's how to delete them*, CNBC (Nov. 19, 2018, 1:59 PM), https://www.cnbc.com/2018/11/19/how-to-delete-amazon-alexa-conversations.html; Profis & Broida *supra* note 42; Moynihan, *supra* note 25.

46 Moynihan, *supra* note 25.

47 Collins, *supra* note 43; Statt, *supra* note 40; *This is how we protect your privacy*, APPLE, https://www.apple.com/privacy/approach-to-privacy (last visited Dec. 29, 2018).

48 Moynihan, *supra* note 25.

49 Kate Nicholson, *Experts caution against using digital assistants without knowing*

and storing data, these consumers' concerns regarding exploitation may be legitimate as companies push further into advertising.[50] As of July 2017, Amazon was considering selling this data to third parties.[51] Since the voice data is connected with the user's account and registered with the company, the company may sell voice data to interested third parties.[52] The data can include the user's Internet searches, shopping lists, entertainment preferences, app downloads, purchases, and general household habits.[53]

Consumer Watchdog, a California based advocacy group, studied patent applications filed for future smart devices.[54] It found Amazon's and Google's patent applications indicate that smart speakers are being designed to identify individuals by voice and locally build advertising profiles geared towards them without the wake word being spoken.[55] Amazon envisions the next wave of Alexa-enabled devices using information collected to build profiles on anyone in the room to sell them goods.[56] Google filed a patent application to use newer versions of Google Home to monitor and control everything from screen time and hygiene habits, to meal and travel schedules, and other activities.[57]

---

where your data goes, CBC NEWS (Dec. 14, 2017, 10:20 AM), https://www.cbc.ca/news/canada/manitoba/experts-caution-against-using-digital-assistants-without-knowing-where-your-data-goes-1.4447347; Jay Stanley, *The Privacy Threat From Always-On Microphone Like the Amazon Echo*, ACLU (Jan. 13, 2017, 10:15 AM), https://www.aclu.org/blog/privacy-technology/privacy-threat-always-microphones-amazon-echo.

50 Brian Dumaine, *It Might Get Loud: Inside Silicon Valley's Battle to Own Voice Tech*, FORTUNE (Oct. 24, 2018), http://fortune.com/longform/amazon-google-apple-voice-recognition/.

51 Kevin McLaughlin, *Facing New Rivals, Amazon May Open Up Alexa Data for Developers*, THE INFO. (July 12, 2017, 10:01 AM), https://www.theinformation.com/articles/facing-new-rivals-amazon-may-open-up-alexa-data-for-developers; Statt, *supra* note 40.

52 *Id*.

53 Maurice E. Stucke & Ariel Ezrachi, *How Digital Assistants Can Harm Our Economy, Privacy, and Democracy*, 32 BERKLEY TECH. L.J. 1239, 1242-43, 1246-47, 1251, 1255 (2017).

54 *Google, Amazon Patent Filings Reveal Digital Home Assistant Privacy Problems*, CONSUMER WATCHDOG, http://www.consumerwatchdog.org/report/home-invasion-google-amazon-patent-filings-reveal-digital-home-assistant-privacy-problems (last visited Dec. 18, 2018).

55 *Id*.

56 *Id*. (describing Amazon's pending patent application for an algorithm that would let future versions of the device identify statements of interest, such as "I love skiing," enabling the user to be monitored based on their interests and targeted for related advertising.).

57 *Id.*; Michael Hicks, *Amazon Echo and Google Home patents show the power they have to compromise your privacy*, TECHRADAR (Apr. 2, 2018), https://www.techradar.com/news/amazon-echo-and-google-home-patents-show-the-power-they-have-to-compromise-your-privacy ("Amazon's patent, titled 'Keyword determinations from conversational data', would have Echo use 'voice sniffer algorithms' to listen for triggering phrases indicating interest in a potential product and then would record and analyze that data for your personal

If this occurs, it may not be long before future versions of voice-enabled devices are used to sell products to consumers.[58] In fact, using surveillance to sell consumer products is nothing novel.[59] Facebook and Google routinely customize ads based on a user's browsing history and content posted.[60] But there is a distinction between sensing that your computer is spying on you when you actively browse the Internet and suspecting that your home smart speaker is silently assessing the content of your conversations.

A separate Google patent application describes how a device could use optical sensors to analyze such signals as speech volume, breathing rate, crying, coughing, and sneezing to categorize a user's mood or physical condition.[61] Used in conjunction with a voice-activated device, this data could be used to promote such products as medicines, and therapeutic aids.[62]

Besides using voice surveillance to sell consumers tailored products, the prices consumers are quoted for the same products may vary depending on the location of the household.[63] Online retailers already adjust prices, offers, and descriptions for products based on a customer's discoverable characteristics such as browsing history and geolocation.[64] Conversation data collected by voice-enabled devices about a speaker's perceived mood, urgency, or projected life decisions could provide retailers with even more psychographic ammunition, which could result in a dangerous new level of marketing persuasion.

---

interests and sell the data to "advertisers or content providers" for personalized ads.").

58 Kathryn McMahon, *Tell the Smart House to Mind its Own Business!: Maintaining Privacy and Security in the Era of Smart Devices*, 86 FORDHAM L. REV. 2511, 2520-21 (2018).

59 Confessore, *supra* note 6; *see also* Alexandra Suich, *Little Brother*, THE ECONOMIST (Sept. 11, 2014), https://www.economist.com/special-report/2014/09/11/little-brother (quoting Chris Babel of TRUSTe, an online privacy service provider, as saying, "A site is not one company any more. A site is tens of hundreds of companies all knowing where you are and what you're looking at.").

60 Laura J. Bowman, *Pulling Back the Curtain: Online Consumer Tracking*, 7 I/S J. OF L & POL'Y FOR INFO. SOC'Y 721, 748-50 (2012); Confessore, *supra* note 6.

61 Consumer Watchdog, *supra* note 54; *New Google Patent Could Turn Your Bathroom Mirror Into A Medical Device*, CBINSIGHTS (Jan. 5, 2018), https://www.cbinsights.com/research/google-patent-smart-home-medical-device.

62 *New Google Patent Could Turn Your Bathroom Mirror Into A Medical Device*, *supra* note 61.

63 Jennifer Valentino-DeVries et al., *Websites Vary Prices, Deals Based on Users' Information*, WALL ST. J., Dec. 24, 2012, at A1.

64 *Id*. (describing price variations based on IP address, smartphone location and physical location); Confessore, *supra* note 6 (describing retail websites that provide price information based on location).

C. What Is this Data Used for?

Consumers, whether they know it or not, routinely give companies massive amounts of data about their location, online search behavior, and purchasing habits via digital devices.[65] This data likely contains personally identifiable information (PII).[66] The National Institute of Standards and Technology (NIST) defines PII as:

> Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biomatic records; and (2) any other information that is linked to an individual, such as medical, educational, financial, and employment.[67]

This has important legal ramifications. Companies can only disseminate personal data by removing traceable PII.

Whenever individuals go online or use an Internet-enabled app, they may be unknowingly disseminating their information to multiple entities.[68] For instance, if a user shares their occasional enjoyment of alcoholic beverages on a dating website, then the dating website may sell this information to a marketing company.[69] The marketing company can mine that data for valuable elements, then categorize and sell it.[70] Metadata can be collected to provide additional

---

65 Melody Ucros, *10 Sneaky Ways Companies Are Collecting Data to Understand Customers*, MEDIUM (Jan 12, 2018), https://medium.com/@melodyucros/10-sneaky-ways-companies-are-collecting-data-to-understand-customers-be0b9089d54a (describing numerous ways that companies collect data on customer behavior, often without their knowledge).

66 Stephen E. Embry, *Developments in the rules governing Personal Identifiable Information may have unexpected consequences for lenders and other businesses*, LEXOLOGY (June 18, 2015), https://www.lexology.com/library/detail.aspx?g=41b7a141-deba-4101-847f-fdb7e0e62879 (noting that Radio Shack pioneered the collection of PII and when Radio Shack was sold, the buyer had to decide whether the customer data it collected would be included in that sale, and whether such a sale would violate the original customer privacy policy).

67 ERIKA MCCALLISTER ET AL., NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., 800-122, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) (2010), https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=904990.

68 Robert L. Mitchell, *Ad tracking: Is anything being done?*, COMPUTERWORLD (Apr. 2, 2014 7:30 AM), https://www.computerworld.com/article/2489106/data-privacy/ad-tracking—is-anything-being-done-.html.

69 Daniel Zwerdling, *Your Digital Trail: Private Company Access*, WYSO (Oct.1, 2013), http://www.wyso.org/post/your-digital-trail-private-company-access (describing third party companies who receive information about users and track their activity on specific websites).

70 Veronica K. McGregor et al., *Big Data and Consumer Financial Information*, BUS. L. TODAY (Nov. 2013), https://www.americanbar.org/content/dam/aba/publications/blt/2013/

attributes about the source of the data and other details about its history.[71] The aggregated data can then be categorized and repackaged before being offered to buyer entities.[72] Data brokers or data warehousing companies hold reams of accumulated data, amassing vast amounts of demographic, socioeconomic, psychographic, and even physiological data about consumers .[73] This data is disseminated by sale or license, to private and public entities.[74]

Consumer data purchasers claim to use the data for a number of purposes, including improving customer experiences and understanding consumer habits.[75] With the help of detailed data broker-built profiles, companies are able to make informed business decisions and create customer specific ads.[76] Increasingly, consumer data, treated as a valued commodity, has been collateralized to obtain capital or secure credit.[77]

11/big-data-financial-info-201311.pdf.

71 *What is metadata and why is it as important as the data itself?*, OPENDATASOFT (Aug. 25, 2016), https://www.opendatasoft.com/2016/08/25/what-is-metadata-and-why-is-it-important-data (providing an overview of what metadata is, its history, and how it provides context to interpret and analyze other data).

72 Steve Kroft, *THE DATA BROKERS: SELLING YOUR PERSONAL INFORMATION*, CBS NEWS (Mar. 9, 2014), https://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information (describing how data mined from the Internet is used to create and sell dossiers on individuals; habits and traits); McGregor et al., *supra* note 70 (showing that companies mine data to provide information about individuals such as social status, and that data can be used to determine more information about people, such as whether they are pregnant).

73 Kroft, *supra* note 72 (providing examples of data that is sold about an individual including "religion, political affiliations, user names, income, and family medical history" and information about particular diseases or conditions such as alcoholism, depression, psychiatric disorders, genetic problems and/or sexual orientation); *What Is Psychographics? Understanding The 'Dark Arts' Of Marketing That Brought Down Cambridge Analytica*, CBINSIGHTS (June 7, 2018), https://www.cbinsights.com/research/what-is-psychographics (distinguishing between demographics and psychographics and explaining how this information is gathered and used to tailor sales and increase clicks on ads).

74 David C. Vladeck, *Consumer Protection in an Era of Big Data Analytics*, 42 OHIO NORTHERN U.L. REV. 493, 497-98, 501-02 (2016).

75 Andrew McAfee & Erik Brynjolfsson, *Big Data: The Management Revolution*, HARV. BUS. REV. (Oct. 2012), https://hbr.org/2012/10/big-data-the-management-revolution (stating "In particular, companies in the top third of their industry in the use of data-driven decision making were, on average, 5% more productive and 6% more profitable than their competitors." While also noting that companies like Sears used analytics to rapidly improve the quality of its promotions to better give customers what they want.).

76 Lipman, *supra* note 10, at 779 (providing an example of retailer predicting customer pregnancy and strategically targeting ads at her).

77 Nguyen, *supra* note 13, at 566, 581 (describing databases used for marketing and as assets).

II. CLASSIFYING PERSONAL DATA

A. Consumer Data as an Intangible Asset

To probe who owns voice-captured personal data, it is helpful to first understand how data is classified as an intangible asset. An asset is defined as a resource, or "an item that is owned and has value."[78] Assets include "cash, inventory, equipment, real estate, accounts receivable, and good will [property, or] all the property of a person available for paying debts or for distribution."[79] Intangible assets are non-physical assets that have a useful life of more than one year and are often comprised of "all of the elements relating to a business enterprise that exist after the monetary and tangible assets have been identified."[80] Its existence depends on "the presence, or the expectation, of earnings."[81] Some intangible assets can be freely exchanged, while others cannot be separated from the business entity that owns them.[82] In addition to customer lists—which are comprised of data—common types of intangible assets include patents, copyrights, and licenses.[83]

A customer list generally arises by contract and can be a simple list with customers' contact information, or, a complex database with customers' transactional history, personal information, demographics, and preferences.[84] Businesses commonly lease or exchange their customer lists with other businesses. However, a customer list subject to confidentiality, or other agreement prohibiting its sale, lease, or exchange, cannot be separated from the original business entity.[85]

Other intangible assets include, copyrights and licenses. A copyright protects the rights of originators of creative works such as writings, songs, films, software code, website designs, marketing materials, and product renderings.[86]

---

78 *Asset*, BLACK'S LAW DICTIONARY 140 (10th ed. 2009).

79 *Id.*

80 *What Are Intangible Assets?*, APPRAISAL ECONOMICS, https://www.appraisaleconomics.com/intangible-assets-2 (last visited Dec. 18, 2018).

81 *Id.*

82 FINANCIAL ACCOUNTING STANDARDS BOARD, EITF ABSTRACTS: RECOGNITION OF CUSTOMER RELATIONSHIP INTANGIBLE ASSETS ACQUIRED IN A BUSINESS COMBINATION 1 (2008).

83 *What Are Intangible Assets?*, *supra* note 81.

84 FINANCIAL ACCOUNTING STANDARDS BOARD, *supra* note 82, at 2.

85 *Id.*

86 A copyright arises automatically when the creative work is put into tangible form and gives its author the exclusive right to publish, reproduce, perform, and produce derivatives from the work. While not required, registration with the USPTO provides notice to the public and the legal ability to enforce the copyright against infringement. *Copyright Basics*, UNITED STATES PATENT AND TRADEMARK OFFICE, https://www.uspto.gov/learning-and-

A license is a contract used to transfer an exclusive or non-exclusive right to use an owner's intellectual property to a third party in exchange for a fee or royalty.[87]

Whether held by a company or sold to a third party, personal voice data is characterized as intangible property because of its similarity to customer lists and relationships. If a company licenses this unaltered data, then the license itself is still classified as intangible property.[88] If a company alters or edits the data it collects, consolidates it with other data, and repackages it or gives it a proprietary structure, the data could become intellectual property, which remains classified as intangible property under the Uniform Commercial Code (UCC).[89] However, if a company combines recorded voice captured data with metadata and user account data, it may acquire characteristics of PII, which carries additional privacy rights.[90]

Notwithstanding its acceptance as a type of business property, consumer data is currently not recognized as personal property. The court in *In re Facebook Privacy Litigation* held that "personal information" was not property under the California's Unfair Competition Law for purposes of allowing consumers who provided personal data to bring a claim under the state's consumer protection law.[91] On appeal, the 9th Circuit affirmed the District Court's ruling that personal information does not constitute property under California's consumer protection law.[92] However, the court partially reversed the District Court by holding that the lost value of the sale of personal information fulfilled the damages requirement for breach of contract and fraud claims.[93]

B. Voice-Captured Data as Intellectual Property

Historically, consumer data is not readily classified as intellectual property. Whether voice-captured consumer data would fare better as intellectual property is worth examining, particularly in its form as recorded original speech. The primary categories of intellectual property are patents, copyrights, trademarks,

---

resources/ip-policy/copyright/copyright-basics (last visited Dec. 5, 2018).

87 *Licensing of Intellectual Property Rights; a Vital Component of the Business Strategy of Your SME*, WORLD INTELL. PROP. ORG., https://www.wipo.int/sme/en/ip_business/licensing/licensing.htm (last visited Dec. 18, 2018).

88 Sharon Finney & Kang Cheng, *The Tangle of Intangible Assets and Business Combinations*, CPA J. (Jan. 2016), https://www.cpajournal.com/2016/01/13/tangle-intangible-assets-business-combinations.

89 U.C.C. § 9-102(a)(42) (AM. LAW INST. & NAT'L CONF. OF COMM'N 2017); U.C.C. § 9-102(a)(45), U.C.C. § 9-102 cmt. 5(d) (AM. LAW INST. & NAT'L CONF. OF COMM'N 2017).

90 McCallister et al, *supra* note 67.

91 *In re* Facebook Privacy Litig., 791 F.Supp.2d 705, 714 (N.D. Cal. 2011).

92 Facebook Privacy Litig v. Facebook, Inc., 572 Fed. Appx. 494 (2014).

93 *Id*.

and trade secrets.[94]

The Supreme Court held that facts and compilations of facts, including electronic data, are not copyrightable because they lack originality.[95] Furthermore, databases do not qualify as patents or trade secrets since they do not require invention, nor are they considered business secrets.[96] Congress has "consistently declined to pass legislation that would protect databases as a new or *sui generis* form of intellectual property."[97] Federally protected intellectual property consists of industrial or creative material that has been granted a patent with the USPTO or as copyright with the Library of Congress.[98] If a company creates a new structure, design, or software to use or disseminate data, it may patent such product.

The Copyright Act defines sound recordings as "works that result from the fixation of a series of musical, spoken, or other sounds but not including sounds accompanying a motion picture or other audiovisual work."[99] This includes the sound of a person speaking if "the recording contains a sufficient amount of production authorship."[100] The U.S. Copyright Office states, "a sound recording typically includes the contributions of the parties whose performance is captured in the recording and the parties who captured and processed those sounds to make the final recording."[101]

---

94 *Intellectual Property*, BLACK'S LAW DICTIONARY (10th ed. 2009) (defining Intellectual Property as "a category of intangible rights protecting commercially valuable products of the human intellect . . . compromise[d] primarily [of] trademark, copyright, and patent rights, but also includes trade-secret rights, publicity rights, moral rights, and rights against unfair competition").

95 Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., Inc., 499 U.S. 340, 364 (1991).

96 Jane B. Baron, *Property as Control: The Case of Information*, 18 MICH. TELECOMM. & TECH. L. REV. 367, 396 n.160 (2012); 35 U.S.C. § 101 (2017) (discussing patents for inventions); 18 U.S.C. §1832(a) (1985).

97 Jane B. Baron, *Rescuing the Bundle-of-Rights Metaphor in Property Law*, 82 U. CIN. L. REV. 57, 98 (2014); *see* Daniel J. Gervais, *The Protection of Databases*, 82 CHI.-KENT L. REV. 1109, 1139-42 (2007).

98 *Copyright Law of the United States*, LIBRARY OF CONGRESS, https://www.copyright.gov/title17 (last visited Dec. 5, 2018) (addressing federally protected intellectual property); *General information concerning patents*, U.S. PATENT AND TRADEMARK OFFICE, https://www.uspto.gov/patents-getting-started/general-information-concerning-patents (last visited Dec. 5, 2018) (addressing federally protected intellectual property).

99 17 U.S.C. § 101 (2016).

100 U.S. COPYRIGHT OFFICE, COPYRIGHT REGISTRATION FOR SOUND RECORDINGS 1 (2017) (discussing types of sound recordings eligible for copyright protection); *see* 17 U.S.C. § 114 (discussing the scope of exclusive rights to sound recordings).

101 U.S. COPYRIGHT OFFICE, *supra* note 99, at 1; *see also* 17 U.S.C. § 101 (explaining that sound recordings are "works that result from the fixation of a series of musical, spoken, or other sounds, but not including the sounds accompanying a motion picture or other audiovisual work, regardless of the nature of the material objects, such as disks, tapes, or

The U.S. Copyright Office clarifies that "[s]hort sound recordings may lack a sufficient amount of authorship to warrant copyright protection, just as words and short textual phrases are not copyrightable. Sound recordings captured by purely mechanical means without originality of any kind also lack a sufficient amount of authorship to warrant copyright protection."[102] This gives rise to the question of how long and how original a string of speech must be in order to qualify as copyrightable.

Trade secrets are a type of intellectual property that were largely governed by state law until the Defend Trade Secrets Act of 2016.[103] Trade secrets include a formula, pattern, device or compilation of data that grants the user an advantage over competitors.[104] In order to protect a trade secret, a business must prove that it adds value to the company—that it is, in fact, a secret—and that appropriate measures have been taken within the company to safeguard the secret, such as wishing to keep its customers' data to use for their own business advantage. However, secrecy requirements are difficult to meet when databases are designed to be marketed and shared.[105]

Without federal statutory protection, original marks and writings still carry some common law protections.[106] Under some circumstances, the original speaker or performer may retain some degree of ownership of that speech if it is embedded in a medium.[107]

---

other phone records, in which they are embodied").

102 U.S. COPYRIGHT OFFICE, *supra* note 99, at 1-2.

103 18 U.S.C. § 1836(a-b) (2016); *see* S.R. REP. NO. 114-220 at 5 (2016) (discussing the shift to federal jurisdiction for theft of trade secret claims); *Trade Secrets Acts Compared to the USTA*, BECK REED RIDEN LLP (Aug. 8, 2018), https://www.faircompetitionlaw.com/wp-content/uploads/2018/08/Trade-Secret-50-State-Chart-20180808-UTSA-Comparison-Beck-Reed-Riden-2016-2018.pdf (discussing trade secret laws throughout the U.S. before the adoption of the federal statutes).

104 18 U.S.C. § 1839(3) (2016).

105 JULIE E. COHEN & WILLIAM M. MARTIAN, INFORMATION SYSTEMS AND THE ENVIRONMENT 48 (2001).

106 Feist Publ'ns, Inc., 499 U.S. at 344 (discussing the limited amount of originality required for protections); Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 471 (1984) (discussing the limitations to copyrights).

107 *See* 17 U.S.C. § 1101 (2016) (detailing the protections for anyone who produces sound recordings and music videos without the consent of the performer); *Are historical speeches public domain?*, NEWS MEDIA RIGHTS (June 28, 2017, 4:44 PM), https://www.newmediarights.org/business_models/artist/are_historical_speeches_public_domain.

III. RIGHTS AND PROTECTIONS FOR PERSONAL DATA IN EXISTING LEGAL FRAMEWORKS

A. Sources of Conflict amongst Stakeholders

Disputes can arise among consumers, primary data collectors and subsequent data purchasers. Disputes can also arise between creditors and debtors over data assets that have been collateralized, as well as between multiple creditors or successors in interest to the previous owners. Different legal frameworks may be used to resolve these disputes.[108] Stakeholders in voice-captured personal data include primary collectors, brokers, first-tier purchasers, second-tier purchasers, licensees, secured creditors, successors in interest, and the consumers themselves who generate the data.[109]

Voice-activated devices are a consumer good.[110] Consumer goods are governed largely by contract law and supplemented by statutes for consumer transactions. However, contract law is problematic because it can be limited in defining the scope and authority of the collection and use of data.[111] Additionally, contract law does not provide consumers with feasible remedies to pursue claims regarding voice-captured data rights.[112] There are limits in contract law, and even in statutes supplementing them, preventing consumers from adequately pursuing remedies for misuse of their personal data captured by

---

108 *See generally* Stacy-Ann Elvy, *Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond*, 44 HOFSTRA L. REV. 839, 842 (2016); *Successor in Interest*, MERRIAM-WEBSTER, https://www.merriam-webster.com/legal/successor%20in%20interest (last visited Dec. 5, 2018) (defining a successor in interest as "a successor to another's interest in property, especially a successor in ownership of a business that is carried on and controlled substantially as it was before the transfer.").

109 Karl Antle, *The Looming Battle over Customer Data*, CLEARINGHOUSE, https://www.theclearinghouse.org/banking-perspectives/2016/2016-q1-banking-perspectives/articles/the-looming-battle-over-customer-data (last visited Jan. 5, 2019); *see* David Knight, *Who owns the data from the IoT?*, NETWORK WORLD (Jan. 30, 2017, 4:00 AM), https://www.networkworld.com/article/3152837/internet-of-things/who-owns-the-data-from-the-iot.html; Kelly Shermach, *Data Mining: Where Legality and Ethics Rarely Meet*, E-COMMERCE TIMES (Aug. 25, 2006, 4:00 AM), https://www.ecommercetimes.com/story/52616.html?wlc=1245363355.

110 WILLIAM D. HAWKLAND ET AL., HAWKLAND UNIF. COM. CODE SERIES § 9-102:2 cmt. (Carl S. Bjerre ed., 1982).

111 Elvy, *supra* note 108, at 842.

112 Stacy-Ann Elvy, *Hybrid Transactions and the Internet of Things: Goods, Services, or Software?*, 74 WASH. & LEE L. REV. 77, 103 (2017); Michael Silvestro & John Black, *"Who Am I Talking To?" - The Regulation of Voice Data Collected by Connected Consumer Products*, BUS. L. TODAY (May 2016), https://www.skarzynski.com/siteFiles/files/ABA%20Voice%20Data%20Article.pdf (explaining how California's Connected Televisions statute is the first to regulate the collection and use of voice data through televisions, but voice recordings collected for other purposes are not explicitly regulated).

voice-enabled devices.[113]

Agreements between commercial entities governing data are largely removed from consumers.[114] Once transactions are taken out of the consumer sphere, there is less regulatory protection and government intervention, even when the transactions may involve something that significantly affects consumers. This is because commercial data brokers consider voice-captured data a commodity.[115] Commodities are governed by the law of commercial transactions, licensing, and secured transactions, rather than by federal consumer protection statutes.[116]

B. The Limitations of Contract Law

When consumers purchase voice-activated devices, and the device servicers provide consumers with content or services through the device, a relationship is formed between the two parties.[117] Contract law will generally dictate this relationship. Freedom of contract principles are prevalent in common law and likewise are incorporated throughout the entire UCC, subject to statutory limitations.[118]

Contracts between entities relating to sales and licensing of data are likely to be governed by common law rather than UCC Article 2, although other UCC articles may apply.[119] Common law, state statutes and federal law govern the transfer and licensing of property.[120]

1. The Consumer Purchase Transaction

The UCC and the common law of contracts govern the consumer's purchase of voice-activated devices from a company storing the user's data.[121] It is necessary to analyze whether the consumer transaction is primarily for the sale of goods or for the provision of services.[122] UCC Article 2 governs sales of

---

113 Jillisa Bronfman, *Weathering the Nest: Privacy Implications of Home Monitoring for the Aging American Population*, 14 DUKE L. & TECH. REV. 192, 216 (2015).

114 Elvy, supra note 108, at 843-44.

115 Kroft, *supra* note 72.

116 Elvy, *supra* note 112, at 80-82, 145, 151.

117 *Id.* at 92 n.54, 105, 145.

118 Charles Bunn, *Freedom of Contract Under the Uniform Commercial Code*, 2 B.C. INDUS. & COM. L. REV. 59, 59 (1960) (describing the freedom of contract doctrine and its incorporation in the U.C.C).

119 U.C.C. §§ 2-102, 2A-102 cmt. (illustrating what type of transactions are covered by Article 2 of the UCC, which does not include sales and licensing of data); RESTATEMENT (SECOND) OF CONSUMER CONTRACTS §1 cmt. 10 (AM. LAW. INST. 2017).

120 15 U.S.C. § 8112 (2018).

121 Elvy, *supra* note 108, at 840-42; *see* U.C.C. § 2-105 (defining goods as things that are moveable).

122 Elvy, *supra* note 112, at 105.

goods, while the common law of contracts governs services.[123] The UCC generally defines goods as "all things that are moveable."[124] Since devices are moveable, their sales would be covered by Article 2, of the UCC.[125]

Unlike sales of goods, contracts for services are covered by common law rather than by UCC Article 2.[126] However, Article 2 of the UCC may still cover the sale of goods even when the goods are bundled with services.[127] This is relevant when examining the device's more service-like functions such as performing household tasks, inquiries, and shopping.[128] The majority of jurisdictions approach these hybrid transactions using the "predominant purpose" test, which assesses whether the predominant purpose of the transaction was to purchase goods, with services being incidental, or vice-versa.[129] For the sale of goods to predominate in a given transaction, courts analyze factors such as whether the parties intended to enter into a contract for goods or services, the presence of any agreements and their titles, the nature of the seller's business, and the amounts charged for goods or services respectively.[130]

Courts apply common law or the UCC to analyze contract formation, performance, and warranties differently when the transaction is for goods or services.[131] Contract formation under traditional common law has more stringent requirements, especially contracts between merchants and non-merchants.[132] To sue under common law, privity of contract is required, unlike under the UCC, which provides remedies for indirect purchasers and even non-purchasers of goods.[133] The statute of limitations to file a claim under the UCC is one to four

---

123 U.C.C. § 2-102.

124 U.C.C. § 2-105.

125 Elvy, *supra* note 112, at 105-12.

126 U.C.C. §2-102; 1 E. ALLAN FARNSWORTH, FARNSWORTH ON CONTRACTS § 1.9 at 43-44 (3d ed. 2004).

127 1 E. ALLAN FARNSWORTH, *supra* note 126, at 44.

128 Elvy, *supra* note 112, at 105-12.

129 1 E. ALLAN FARNSWORTH, *supra* note 126, at 44. A minority of jurisdictions, including Maryland, opt for the "gravamen" test instead of the predominant purpose test, which focuses on whether the complaint arises out of the goods or services portion of the transaction. Anthony Pools v. Sheehan, 455 A.2d 434, 440-41 (Md. 1983); Elvy, *supra* note 112, at 105-12.

130 Kline Iron & Steel Co. v. Gray Commc'ns Consultants, Inc., 715 F.Supp. 135, 139 (D.S.C. 1989); *Anthony Pools*, 455 A.2d at 437; Audio Visual Artistry v. Tanzer, 403 S.W.3d 789, 796-804 (Tenn. Ct. App. 2012); Kietzer v. Land O'Lakes, C1-01-1334, 2002 Minn. App. LEXIS 219, at*7-8 (Minn. Ct. App. Feb. 19, 2002)..

131 1 E. ALLAN FARNSWORTH, *supra* note 126, § 3.21 at 318-20; 2 E. ALLAN FARNSWORTH, *supra* note 126, § 8.12 at 493-95; *compare* 2 E. ALLAN FARNSWORTH, *supra* note 126, § 3.21 at 587-89, *with* U.C.C. §§ 2-313-315.

132 1 E. ALLAN FARNSWORTH, *supra* note 126, § 1.10 at 65-66.

133 U.C.C. §2-318; 3 E. ALLAN FARNSWORTH, *supra* note 126.

years depending on the terms contracted by the original parties, while common law could allow up to ten years, depending on the jurisdiction.[134]

2. Consent for Data Collection

The purchase of a device raises the issue of whether the purchaser has provided consent to the device servicer to collect the consumer's voice data. A legal contract governing the relationship between the consumer and the device provider may arise through express language or implied consent by performance by the parties.[135] In an express contract, the parties explicitly state their intention to enter into the contract, either orally or in writing.[136] In contrast, an implied contract is created by conduct; the parties interact in a manner from which a contract can be inferred.[137]

Companies that collect data from individuals browsing their sites generally provide a written agreement that governs both parties' rights and obligations.[138] The agreement may appear in the form of a privacy policy, terms and conditions, or another agreement that provides notice to the user of the website.[139] A company may use the "browse-wrap" method, which either displays the terms and conditions of use on the website or provides a hyperlink to the user.[140] Alternately, a company may use the "click-wrap" method, which requires website users to affirmatively click to confirm they understand and accept the website's policies.[141]

At the very least, a website is required to provide users with notice of its privacy policy.[142] At the beginning of the contractual relationship, the consumer may be able to ascertain a company's privacy policy, since companies must publish or make such policies available.[143] A company's policy may limit its sharing of personal data with third-parties, which creates contractual limitations

---

134 Alaska Stat. § 09.10.053 (2018); Wyo. Stat. Ann. § 1-3-105(a) (2018); U.C.C. §2-725.

135 *Id.* §§ 3.10, 3.13 at 251-52, 270.

136 *Id.* § 3.10 at 251-52.

137 *Id.* at 252.

138 *Browsewrap vs. Clickwrap*, TERMSFEED (Aug. 21, 2018), https://termsfeed.com/blog/browsewrap-clickwrap.

139 *Id.*

140 *Id.*

141 *Id.*

142 *Privacy Policies are Mandatory by Law*, TERMSFEED (Dec. 9, 2018), https://termsfeed.com/blog/privacy-policy-mandatory-law.

143 Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN ST. L. REV. 587, 597 (2007) (explaining "the existing legislation requires that a privacy policy be posted, and that the entity abide by that policy, but does not regulate the substance of that policy.").

to the use of personal data.[144] A company that has already collected and owns personal data directly from consumers is supposed to notify its users of any changes to its privacy policy.[145]

For a contract to be enforceable, there must be a meeting of the minds between the parties.[146] In the case of a website company and its users, the users must give express or implied consent to the terms of the website's agreement.[147] Voice-activated devices may include a "shrink-wrap" agreement, describing the terms and conditions of the contract for the good purchased.[148] If the consumer proceeds to use the device, presumably, the consumer's performance constitutes implied acceptance of the contract with respect to the use of the goods.[149] Arguably, use of the device may constitute consent for the use of the service associated with the device.[150] However, unlike when an internet user enters a website, there is no express agreement presented on the device's display or speakers informing the consumer that a contract has been formed whereby the consumer has consented to use of its personal data.[151]

An enforceable contract governing the consumer's voice data, must have an exchange of consideration between the service provider and the consumer.[152] Device service providers provide that the consumer agrees to receive service and content through the device in exchange for providing voice data.[153] Whether consideration exists in this context is of particular importance to consumers, since consumers may not be able to enforce rights to their own data unless they

---

144 *See* Allyson W. Haynes, *Web Site Visitors and Online Privacy*, 20 S.C. L. 26, 28 (2008) (explaining "In a typical provision, Website users are told that the personal information collected about them may be shared with the Website's "affiliated providers," with third parties if "necessary to fulfill a transaction" or based on the user's consent.").

145 FTC, Self-Regulatory Principles for Online Behavioral Advertising 11-12 (2009).

146 RESTATEMENT (SECOND) OF CONTRACTS § 17 cmt. c (AM. LAW INST. 1981).

147 *Browsewrap vs. Clickwrap*, *supra* note 138.

148 Jim Snell & Christian Lee, *Internet of Things: On the Cusp of a Litigation Explosion*, WESTLAW J. INTELL. PROP. 1, 3 (Nov. 7, 2017), https://www.perkinscoie.com/images/content/1/8/v3/182167/Westlaw-Journal-IP-Perkins-Coie-EA.PDF.pdf.

149 *Browsewrap vs. Clickwrap*, *supra* note 138. A shrink-wrap agreement may contain language that a user of the product agrees to the terms and conditions stated in the agreement (or elsewhere that is accessible).

150 Snell & Lee, *supra* note 149, at 4 (explaining "for enforceable shrink-wrap agreements, courts will find use of the product indicates acceptance of the agreement.").

151 Hines v. Overstock.com, Inc., 668 F.Supp.2d 362, 366-67 (E.D.N.Y. 2009) (explaining that "Unlike a clickwrap agreement, a browsewrap agreement does not require the user to manifest assent to the terms and conditions expressly . . . [a] party instead gives his assent simply by using the website.").

152 RESTATEMENT (SECOND) OF CONTRACTS § 17.

153 *See* Pamela Samuelsson, *Privacy as Intellectual Property*, 52 STAN. L. REV. 1125, 1162-63 (2000).

prove a lack of consideration for authorizing the data's use by the company.[154]

Assuming a contract has been formed and is enforceable, the duration of any consent given is not specified.[155] Device service providers may argue that device owners implicitly authorize the use of their voice data when they purchase, link, and initiate use of the device with their designated account.[156] Theoretically, consumers can interact with the device indefinitely, as long as they maintain an internet connection and user account with the servicer, which means their voice data can be collected indefinitely. The existence of any such ongoing consent would be implied, since—unlike with click-wrap agreements, which require users to scroll through and/or check a box signifying they have read an agreement—consumers using voice-activated devices are not asked to consent expressly to the use of their data each time they make a query through it.[157]

The question of consent also arises when individuals other than the device purchaser interact with the voice-activated device, including members of the purchaser's household or visitors.[158] These individuals may not even realize such devices are recording them.

3. Does Consumer Consent Extend to Third-Party Data Use or Acquisition?

When a device purchaser gives consent to collect the purchaser's voice data —either once for an indefinite duration, or, each time a query is made through the device—the consumer may not knowingly or intentionally give consent for

---

154 *In re* Facebook Privacy Litig., 791 F.Supp.2d 705, at 717 (holding, based on a California statute, the Consumer Legal Remedies Act (CLRA), that because the plaintiffs had not paid fees to use Facebook, they could not be considered "consumers").

155 RESTATEMENT (SECOND) OF CONTRACTS § 23 (explaining that a bargain must have "two manifestations of willingness to make a bargain that are each made with reference to the other.").

156 *See* Audrey Gilbert, *Turning implied consent into express consent*, CYBERIMPACT (Apr. 3, 2016), https://www.cyberimpact.com/en/turning-implied-consent-express-consent (explaining that implied consent can stem from a business relationship, including the purchase of a product).

157 *See Browsewrap vs. Clickwrap*, *supra* note 138 (explaining that click-wrap agreements provide increased notice by requiring users to read or at least acknowledge the existence of an agreement).

158 Raphael Davidian, *Alexa and Third Parties' Reasonable Expectation of Privacy*, 54 AM. CRIM. L. REV. 58, 58 (2017) ("Under current Fourth Amendment doctrine, when someone takes a deliberate step to install a microphone in her home with knowledge that her interactive data will be transmitted to a third party, she has no reasonable expectation of privacy. But a more nuanced question arises when someone who is not the device owner is recorded without consent, and the recording is requested without a warrant."); *see* Gerald Sauer, *A MURDER CASE TESTS ALEXA'S DEVOTION TO YOUR PRIVACY*, WIRED (Feb. 28, 2017, 10:00 AM), https://www.wired.com/2017/02/murder-case-tests-alexas-devotion-privacy ("This brings up a more basic question: Do you have to give informed consent to be recorded each time you enter my Alexa-outfitted home? Do I have to actively request your permission?").

the device servicer to share the data with third parties.[159] Parties in litigation have debated whether consumers provided consent validly, freely and knowingly to third parties.[160]

Entities that collect consumer data are generally required to publish or distribute privacy policies stating how they use the data and with whom they share it (or may share it in the future).[161] Entities are also required to provide updates of any changes to their privacy policy.[162] The Federal Trade Commission (FTC) requires a company that collects PII to provide clear and conspicuous notice to and receive affirmative consent from the individual giving the PII.[163]

---

159 *See* Sauer, *supra* note 162 (describing how Google does not ask for a consumer's permission when it shares voice recordings collected by Google Home, but instead states its intent in the user agreement); *but see* Commission Regulation 2016/679, art. 6, 2016 O.J. (L 119) 59 (EU) (explaining that under the General Data Protection Regulation in Europe, processing, which includes the dissemination of data, is lawful only if "the data subject has given consent to the processing of his or her personal data for one or more specific purposes" but that processing that is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party" may be lawful as long as said interests are not overridden by "the interests or fundamental rights and freedoms of the data subject which require protection of personal data.").

160 Kirch v. Embarq Mgmt. Co., 702 F.3d 1245, 1248 (10th Cir. 2012) ("Embarq then moved for summary judgment on the unlawful-interception claim. It argued that . . . the Kirches had consented to any alleged interception [of information] by agreeing to the terms of Embarq's privacy policy, which gave users notice that their Internet communications could be shared with third parties."); *In re* Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 WL 5423918, at *7 (N.D. Cal. Sept. 26, 2013) ("Google contends that all Plaintiffs have consented to any interception [of information]. Under statute, it is not unlawful 'to intercept a wire, oral, or electronic communication ... where one of the parties to the communication has given prior consent to such interception.'"); Deering v. Centurytel, Inc., No. CV-10-63-BLG-RFC, 2011 WL 1842859, at *1 (D. Mont. May 16, 2011) ("CenturyTel argues that … since Deering acquiesced his consent by using CenturyTel's services knowing his Internet activity could be diverted and used to target him with advertisements, the motion [to dismiss the invasion of privacy claim] must be granted.").

161 CONSUMER FED'N OF CAL., *What Should I Know About Privacy Policies?*, https://consumercal.org/about-cfc/cfc-education-foundation/what-should-i-know-about-privacy-policies-2 (last visited Jan. 6, 2019) ("A privacy policy should explain how the organization collecting personal information intends to use it [and whether customer information is shared with other companies, and to] whom that personal information may be shared.").

162 *Privacy Policy Requirements*, PRIVACYTRUST, https://www.privacytrust.com/certification/privacy/privacy_requirements.html (last visited Jan. 6, 2019) (explaining that one privacy policy requirement for entities is that they must "inform users of . . . any changes in privacy policy").

163 Embry, *supra* note 66 ("The FTC requires that there be clear and conspicuous notice [given by a company collecting PII] and affirmative consent [from an individual giving PII]."); *see Children's Online Privacy Protection Rule: Not Just for Kids' Sites*, FED. TRADE COMM'N (Apr. 2013), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-

4. Contract Law's Remedies for Privacy Policy Breaches

Consumers may sue if their data is leaked outside of the entity or acquired by an unauthorized third parties due to a security breach, provided the consumer can show harm.[164] Consumers who agree to share their personal data may sue these data collectors for breach of contract if they have privity of contract with such entities that collect their data.[165] A breach of contract claim may arise when an entity violates its privacy policy by sharing or selling this data with third-parties, provided the privacy policy states the entity will not share the data.[166] However, if entities are authorized to share data with third-parties, consumers may not have recourse unless they can show the company's failure to publish any effected changes to the policy.[167]

A company could breach or engage in a deceptive practice by pledging customers' personal data as collateral, if that company has promised not to sell or share it. If the company defaults on its debt obligation, the collateralized data could be seized or sold by the party holding the security interest.[168] Thus, "even

---

online-privacy-protection-rule-not-just-kids-sites (explaining that websites and online services covered by the Children's Online Privacy Protection Act (COPPA) must "provide parents with direct notice of their information practices, and get verifiable consent from a parent or guardian before collecting personal information from children.").

164 *See* WASH. REV. CODE ANN. § 19.255.010(13)(a) (2015) (giving an example of a state data breach law which affords consumers injured by a violation of the law the right to "institute a civil action to recover damages."); *see e.g.*, Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692 (7th Cir. 2015) (discussing how customers brought a class action lawsuit against a department store for violation of state data breach laws and the customers had to show "that the data breach inflicted concrete, particularized injury on them" in order to recover).

165 *See Privity*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining privity of contract as "the relationship between the parties to a contract, allowing them to sue each other but preventing a third party from doing so.").

166 *See* Emily Tabatabai et al., *PRIVACY POLICIES AND THE SALE OF CORPORATE ASSETS: It pays to plan ahead to preserve the value of your data assets*, ORRICK TRUST ANCHOR (Oct. 20, 2015), https://blogs.orrick.com/trustanchor/2015/10/20/privacy-policies-and-the-sale-of-corporate-assets-it-pays-to-plan-ahead-to-preserve-the-value-of-your-data-assets/ (explaining that companies that "attempt to transfer data in a manner that conflicts with promises made in its privacy policy may face regulatory scrutiny or litigation.").

167 *See* PRIVACYTRUST, *supra* note 167 (explaining that a "user's choice about personally identifiable information being disclosed to third parties must be honoured," meaning if a user wants their information shared with third parties, an entity will be authorized to share the user's data accordingly and will be shielded from liability when doing so).

168 Tabatabai et al., *supra* note 171 (explaining that companies have the ability to sell data as a corporate asset in a company sale, merger, bankruptcy, or similar corporate transaction); DAVID ZARFES & MICHAEL L. BLOOM, CONTRACTS AND COMMERCIAL TRANSACTIONS 376 (2011) ("A lender may secure the performance of its loan by taking a 'security interest' (a particular kind of property interest) in some of the borrower's assets (i.e., collateral). If a borrower defaults on its loan . . . the secured lender will have certain rights [such as the right to sell the collateral] which it may exercise against the debtor's collateral in which the lender holds a security interest.").

if a company doesn't actually go bankrupt or isn't actually sold, its privacy policy might still be deceptive if it has used its customer data as collateral for a loan."[169] Simply having an agreement to sell customer data in the event of a bankruptcy or sale could make a privacy policy deceptive.[170] If a policy is found to be unfair and deceptive, the FTC may also bring an action under its statutory authority.[171]

C. Limitations in the Law of Secured Transactions

Devices collect and transmit to their service providers a significant amount of data, some of which contains PII. Given PII's high value, entities routinely buy, sell, and share data for money.[172] Some companies use data as collateral to obtain capital or credit.[173] Article 9 of the UCC governs transactions (other than finance leases) that involve procuring a debt through a creditor's interest in a debtor's property.[174] Since security interests are created and perfected differently depending on their collateral classification, the rights of creditors may differ.[175] Therefore, it makes a difference how voice data and customer information are classified.

---

169 Daniel Solove, *Going Bankrupt with Your Personal Data*, TEACHPRIVACY (July 6, 2015), https://www.teachprivacy.com/going-bankrupt-with-your-personal-data; *see* Tabatabai, *supra* note 171 (explaining that the proposed sale of Radio Shack customer's personal information would violate the FTC's Act prohibiting deceptive trade practices as well as the laws of several states that had Radio Shack stores).

170 *See* 15 U.S.C. § 45(a)(2) (2006) (explaining that the FTC may also bring an action under its statutory authority if a company's privacy policy is found to be unfair and deceptive: "The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."); *see, e.g.*, F.T.C. v. Actavis, Inc., 570 U.S. 136, 145 (2013) (explaining that the FTC brought a suit against defendants for allegedly engaging in monopolistic behavior in violation of 15 U.S.C. § 45); Solove, *supra* note 174 ("The FTC has not pursued a case such as this, but any company that has used its customer data as collateral and that has a privacy policy that does not state that data may be transferred in the event of a bankruptcy could find itself charged with engaging in a deceptive practice—even though it has not gone bankrupt or been put up for sale.").

171 15 U.S.C. § 45(a).

172 *Data is giving rise to a new economy*, THE ECONOMIST (May 6, 2017), https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy.

173 U.C.C. §9-102(a)(12) (AM. LAW INST. 2018) (defining collateral as "property subject to a security interest").

174 U.C.C. §1-201(a)(35) (AM. LAW INST. 2018).

175 U.C.C. §§ 9-203, 9-308-13; *see also* SECURED TRANSACTIONS GUIDE 7237060, para. 4, 180 (stating that a security interest is perfected when it has been attached and has been perfected by a type of method and that perfection may be achieved by possession or by control of collateral, or, by filing a financing statement).

UCC Article 9 classifies customer and electronic stored information as a class of personal property called "general intangibles."[176] To perfect a general intangible, the secured party is generally required to file a financing statement with the Secretary of State where the debtor is located.[177] The statement filed must contain basic information about the parties and at least a general description of the collateral.[178]

Although trademarks, patents, and copyrights are not explicitly listed in the definition of "general intangible," the definition's Official Comment includes "intellectual property" as an example of a general intangible.[179] However, "to the extent that a statute, regulation, or treaty of the United States preempts" Article 9, the UCC's rules do not apply.[180] In the case of intellectual property, Article 9 of the UCC may be pre-empted by federal law or if the secured party seeks to record a security interest with the USPTO or United States Copyright Office.[181]

In the case of a patent or trademark, the security agreement creating the security interest would need to specifically identify each intellectual property asset applicable to the security interest.[182] Additionally, a secured party in this situation would file a short-form intellectual property security agreement or other document confirming the security interest for public disclosure within three months of the agreement's date, or before a subsequent purchase.[183]

The Copyright Act preempts Article 9 of the UCC for perfecting a security interest in copyrighted property.[184] To perfect a security interest in registered copyrights and pending copyright applications, secured parties must file a short-form intellectual property security agreement directly with the United States

---

176 U.C.C. §9-102(a)(42) (AM. LAW INST. 2018).

177 U.C.C. §9-312(a) (AM. LAW INST. 2018).

178 U.C.C. §9-502(a) (AM LAW INST. 2018).

179 U.C.C. §9-102 cmt. 5d (AM LAW INST. 2018).

180 U.C.C. §9-109(c)(1) (2010).

181 Daren Orzechowski & Amy Badgasarian, *"Perfecting" Security Interests in United States Patents, Trademarks and Copyrights*, WHITE & CASE TECH. NEWSFLASH (Dec. 18, 2013), https://www.whitecase.com/publications/article/perfecting-security-interests-united-states-patents-trademarks-and-copyrights.

182 Moldo v. Matsco, Inc., 252 F.3d 1039, 1045-46 (9th Cir. 2001) (stating the Patent Act does not preempt every state law, so perfection should be achieved by process laid out in UCC Article 9).

183 Daren Orzechowski & Amy Badgasarian, *"Perfecting" Security Interests in United States Patents, Trademarks and Copyrights*, WHITE & CASE TECH. NEWSFLASH (Dec. 18, 2013), https://www.whitecase.com/publications/article/perfecting-security-interests-united-states-patents-trademarks-and-copyrights.

184 John F. Hornick, *Security Interests in Intellectual Property*, FINNEGAN (2003), https://www.finnegan.com/en/insights/security-interests-in-intellectual-property.html (explaining the process and relevant U.C.C. code provisions to use intellectual property to secure collateral).

Copyright Office.[185] Under the Copyright Act, priority is usually awarded to the first executed transfer over the first recorded transfer.[186] The Act includes in the "transfer of a copyright ownership" a "hypothecation," which "is a form of pawning or pledging an asset as collateral for a debt."[187] To ensure priority, the transfer must be recorded within one month of the transfer agreement's execution or before a later transfer is recorded.[188] However, holders of unregistered copyrights do not have recourse under state law, which governs security interests in unregistered copyrights, because security interests and any remedies thereof are exclusively under federal jurisdiction.[189]

In contrast to the more demanding intellectual property rights regime, a creditor's security interest in general intangibles becomes valid and enforceable against third parties once a general financing statement is filed.[190] For this reason, Professor Xuan-Thao Nguyen suggests that UCC Article 9's procedures for creating enforceable security interests facilitate collateralization of consumer information and contribute to the violation of consumer privacy.[191] One benefit to having a security interest is the enforceability against the debtor and/or third parties.[192] This means that "if the defaults, the creditor may repossess and/or sell the collateral property to satisfy the debt."[193] This raises the question of whether a company is prohibited from collateralizing personal data that it may not be allowed to sell in compliance with a regulation of its own privacy policy.

In the event of a company's acquisition, merger, ownership change, or default, a creditor or other unforeseen party may acquire the data previously owned by the primary company.[194] Article 9 of the UCC provides for temporary perfection in collateral owned by a successor before the merger, or, collateral

---

185 *Id*.

186 *Id*.

187 17 U.S.C. § 205(d) (2018); Hornick, *supra* note 189.

188 Hornick, *supra* note 189.

189 *In re* World Auxiliary Power Co., 303 F.3d 1120, 1126 (9th Cir. 2002) (holding that unregistered copyrights are not covered by the Copyright Act, and there is no way for a secured creditor to preserve a priority in an unregistered copyright); WILLIAM D. WARREN & STEVEN D. WALT, SECURED TRANSACTIONS IN PERSONAL PROPERTY 385 (Robert C. Clark et al. eds., 9th ed. 2013).

190 Joseph H. Flack, *Secured Transactions: Practical Things Every Business Lawyer Should Know About UCC Article 9*, AMERICAN BAR ASSOC., https://apps.americanbar.org/buslaw/committees/CL983500pub/newsletter/201103/flack.pdf (last visited Jan. 13, 2019).

191 Nguyen, *supra* note 13, at 588-90.

192 U.C.C. §9-203(b) (AM. LAW INST. 2018).

193 *UCC Article 9 Amendments (2010) Summary*, UNIFORM LAW COMM'N, http://www.uniformlaws.org/ActSummary.aspx?title=UCC%20Article%209%20Amendments%20(2010) (last visited Dec. 5, 2018).

194 Sarah Berger, *Keeping track of your data is getting harder to do*, BANKRATE (Aug. 18, 2016), https://www.bankrate.com/finance/identity-theft/consumer-data-company-acquisition.aspx.

acquired by the successor within four months after the date of the merger.[195]

However, it is uncertain what happens to the data assets of a company in bankruptcy. Bankruptcy trustees have an obligation to maximize the recovery for unsecured creditors, while bankruptcy courts have an interest in balancing the rights of the debtor, secured creditors, and unsecured creditors.[196] Thus, a bankruptcy may result in transfer or liquidation of all of a debtor's allowed assets to satisfy a debt, which may include personal data assets.[197]

At least five recent corporate bankruptcies have brought to light issues with personal data held as assets at the time of bankruptcy.[198] As an example, RadioShack had to destroy valuable customer data because the bankruptcy court would not let the winning bidder purchase it, since it violated RadioShack's privacy policy.[199]

IV. SOLUTIONS THROUGH PROPERTY LAW, SECURED TRANSACTIONS, AND STATUTES

A. Voice-Captured Data Should Be Classified as an Independent Property Class

Ideally, a separate class of property should be created that derives from a person's private physical being, akin to a person's tissue or genetic property. The hallmark of this type of property is that it is not designed to be sold for commercial purposes. Rather, data collectors may share such data with authorized users by consensual agreement, but it remains property of the user, as the originator. As an alternative, voice-captured personal data should be classified as a type of intellectual property because of its unique quality as recorded speech, in contrast with other types of data which have found little success in being classified as intellectual property.

Either of these two classifications would allow voice-captured data to benefit from property law's legal framework, which is uniquely suited to handle such data ownership, since it allows shared ownership with multiple concurrent users

---

195 UCC § 9-508(b)(1) (AM. LAW INST. 2018).

196 11 U.S.C. § 704(a); Steven Rhodes, *The Fiduciary and Institutional Obligations of a Chapter 7 Bankruptcy Trustee*, 80 AM. BANKR. L.J. 147, 148-49 (2006).

197 JEREMIAH J. SPIRES, 6 DOING BUSINESS IN THE UNITED STATES §94.06 (James M. Wilson, Jr. ed., 2010).

198 *In re* Radio Shack, No. 15-10197, 550 B.R. 700, 704 (Bankr. D. Del. 2016); *In re* BPS US Holdings, Inc., No. 16-12373, 2017 WL 4990423, at *1 (Bankr. D. Del. 2017); *In re* Aeropostale, Inc., No. 16-11275, 555 B.R. 369, 411 (Bankr. S.D.N.Y 2016); *In re* Golfsmith Int'l Hold., Inc., No. 16–12033, 2016 WL 10574676 (Bankr. D. Del. 2016); *In re* Sports Auth. Hold. Inc, No. 16-386-SLR, 2016 WL 3041846 (D. Del. 2016).

199 *In re* Radio Shack, No. 15-10197, 550 B.R. 700, 704 (Bankr. D. Del. 2016).

of the same asset.[200] Property law allows multiple parties to hold, use, or inherit rights to the same property concurrently.[201] Likewise, a single owner of property may sell, license, and use such property as collateral.[202]

Professor Jane Baron suggests "the bundle-of-rights metaphor captures the fact that ownership of information is divided. It also helps show that the rights, powers, privileges, etc. of any one party with respect to another will not necessarily be the same as another's with respect to that same other party."[203] This bundle-of-rights metaphor applies to the exchange of personal data "precisely because it heightens attention to the possibility of divided, but shared, rights."[204]

At the same time, property law's creation of legal relationships between parties and concurrent common interests promote better choices with the goal of property preservation and possible value enhancement. Additionally, it recognizes public rights in private property. Perhaps this is why commercial law is starting to use property rights in analyzing contracts involving hybrid goods and intangible assets.[205]

B. Consumers Should Be Notified of the Creation and Transfer of Security Interests in their Personal Voice Data

Adjusting the process by which security interests in highly personal data are created and enforced may help protect the data's integrity while minimizing unintended transfers that may harm consumers. This would entail special rules in drafting financing statements for collateral that is classified as personal data,

---

200 Anna di Robilant, *Property: A Bundle of Sticks or a Tree?*, 66 VAND L. REV. 869, 870 (2013).

201 *Id*. at 879.

202 *Id*. at 878.

203 Jane B. Baron, *Rescuing the Bundle-of-Rights Metaphor in Property Law*, 82 U. CIN. L. REV. 57, 96 (2013).

204 *Id*. at 99.

205 Robilant, *supra* note 205 (stating that "neither the ownership model nor the bundle of sticks model accounts for the increasingly resource-specific nature of property law . . . [but in recent years], [s]ocial, economic, and technological changes have transformed the nature of certain resources, creating regulatory dilemmas that are resource specific"); Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 389 (2015) (indicating that "individual empowerment [over data privacy] is not enough because an individual's disclosure of information about herself impacts many other people"); Baron, *supra* note 208 (arguing that "the bundle-of-rights conceptualization remains useful . . . [because it] produces more precise specification of the legal relations of parties in both simple and complex property arrangements . . . it clarifies the normative choices that underlie decisions about property . . . [and] it focuses attention on the quality of the relationships that property constructs").

as well as limitations on who may claim the right to possess it in the event of default.[206] The consumer may also have to provide approval at certain stages of the transaction.

First, financing statements would need to specify that they contain personal data assets. Currently, financing statements do not require a high level of specificity as to what the security agreement contains.[207] Second, secured parties would be required to file financing statements listing such assets. Currently, filing is not required, though it helps the secured party assert a claim in the event of a contest.[208] Filing with the proper authorities would not only notify other creditors, but it would also notify consumers that the data collector has allowed a third-party to acquire a security interest in it.[209] Thus, even if the data is not technically sold or shared through transmission, consumers are alerted to the possibility of the data changing hands in the future.

Third, parties seeking perfection of security interests in personal data would need to file a statement with the FTC or other appropriate agency, similar to the process by which security interests in copyrights are currently perfected.[210] This would put the agency on notice. Fourth, the FTC or designated agency would be required to review and approve any transfer or liquidation of personal data collateral stemming from the debtor's default. This would be similar to the "consumer ombudsman" appointed in bankruptcies involving personal data

---

206 *See* Elvy, *supra* note 5 at 1374-75 (wondering if "high-value, data-generating consumers [could] begin . . . using their data as collateral to obtain financing in a transaction subject to Article 9 of the Uniform Commercial Code").

207 *See* U.C.C § 9-502. (AM. LAW INST. & UNIF. LAW COMM'N 2010) (stating in the official comment, that within the notice filing system it is not necessary to file "the security agreement itself, but only a simple record [in the financing statement] providing a limited amount of information").

208 *See* U.C.C §9-314 (AM. LAW INST. & UNIF. LAW COMM'N 2000) (stating that "[a] security interest in investment property, deposit accounts, letter-of-credit rights, or electronic chattel paper may be perfected by control of the collateral"); *see also* U.C.C §9-313 (AM. LAW INST. & UNIF. LAW COMM'N 2000) (stating that "a secured party may perfect a security interest in negotiable documents, goods, instruments, money, or tangible chattel paper by taking possession of the collateral").

209 *See* U.C.C § 9-502. (AM. LAW INST. & UNIF. LAW COMM'N 2010) (indicating in the official comment, that "[t]he notice itself indicates merely that a person may have a security interest in the collateral indicated . . . [and that] [f]urther inquiry from the parties concerned will be necessary to disclose the complete state of affairs").

210 *See* 17 U.S.C. § 205(a) (stating that "any transfer of copyright ownership or other document pertaining to a copyright may be recorded in the Copyright Office if the document filed for recordation bears the actual signature of the person who executed it . . . [and] may be submitted to the Copyright Office electronically, pursuant to regulations established by the Register of Copyrights"); *see also* U.S. COPYRIGHT OFFICE, CHAPTER 2300: RECORDATION, 2014 WL 7749598, at *16 (last revised 2017) (indicating that, "some courts have held that a security interest in a registered work must be recorded with the U.S. Copyright Office in order to perfect the creditor's interest").

(discussed below).[211]

C. Federal or State Statutes Should Protect and Restore Consumers' Rights in their Personal Voice Data

1. Summary of Existing Statutes Governing Personal Data

Ultimately, statutory relief on the federal or state level should effectively protect and restore certain rights to consumers in their own personal data, especially data captured in the privacy of their homes. Although the collection, use, and sale of personal data is already governed by certain statutes, they tend to focus on specific industries or transaction types.[212]

The Electronic Communications Privacy Act (ECPA) protects private electronic communications from unauthorized access, interception or disclosure by the federal government.[213] It has been asserted in numerous lawsuits involving the alleged misuse of private information by online companies, where,

---

211 11 U.S.C. § 332(b) (stating that a consumer privacy ombudsman is a disinterested party appointed to "assist [a bankruptcy] court in its consideration of the facts, circumstances, and conditions of the proposed sale or lease of personally identifiable information . . . [weighing factors like] . . . (1) the debtor's privacy policy; (2) the potential losses or gains of privacy to consumers if such sale or such lease is approved by the court; (3) the potential costs or benefits to consumers if such sale or such lease is approved by the court; and (4) the potential alternatives that would mitigate potential privacy losses or potential costs to consumers").

212 Gramm-Leach-Bliley Act, 15 U.S.C. §6801-6809. (Other regulations not discussed here that govern consumer data include: 1. The Gramm-Leach-Bliley Act, which impose privacy rules relating to the personal financial information of consumers. Gramm-Leach-Bliley applies to any financial institution collecting non-public personal information from individuals or consumers who obtain financial products or services for personal, family, or household purposes; hence, companies offering banking, insurance, securities, or financial advising services will likely be governed. However, to date, no enforcement actions have been brought under this act against companies operating online. 2. The Cable Communications Policy Act, which regulates the collection and use of personal information from cable subscribers. 3. The Equal Credit Opportunity Act, which prohibits creditors from gathering specific types of information from applicants (such as sex, race, or religious data). 4. The Right to Financial Privacy Act, which regulates the ability of financial institutions to release consumer information to the federal government. 5. The Computer Fraud and Abuse Act, which criminalizes the unauthorized access to certain financial and other information maintained by the government but can also be alleged as a private cause of action under appropriate circumstances where damage can be proven. 6. The Privacy Act of 1974, which prohibits the federal government from obtaining, maintaining and using federal agency records containing personal information that is irrelevant to accomplishing the agency's purpose).

213 Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22 (2012).

for example, plaintiffs have claimed that a company using cookies violates ECPA.[214] Courts have at least considered applying ECPA to suits involving personal data, although most courts find ECPA an insufficient legal argument in such suits.[215] *In re Facebook Privacy Litigation*, the court dismissed the plaintiffs' claims under ECPA, finding that "personal information" was not property under California's consumer protection law.[216] The court distinguished one of its prior cases, *Doe 1 v. AOL, LLC*, and found that, because the plaintiffs had not paid fees to use Facebook, they were not "consumers," and thus could not state a claim under the California consumer protection statutes.[217]

The Federal Trade Commission Act gives the FTC power to take action against companies which fail to comply with their own privacy policies or which otherwise misrepresent their information management practices.[218] In *FTC v. Toysmart.com*, Toysmart promised that it would never share customer information with a third party in its privacy policy.[219] When Toysmart filed for bankruptcy, its main asset was its customer data, which was highly coveted due to its value.[220] Since selling the data to a new corporate buyer would violate Toysmart's promise not to share customer data with a third party, the FTC issued a complaint that Toysmart violated Section 5 of the FTC Act, which "prohibits unfair or deceptive acts or practices in or affecting commerce."[221] A breach of a privacy policy is a deceptive practice.[222] Consequently, Toysmart settled with the FTC by agreeing to sell its business only to a "Qualified Buyer" that was in a similar line of business, in this case in "areas of education, toys, learning, home and/or instruction, including commerce, content, product and services."[223] The buyer would also have to abide by the terms of Toysmart's privacy policy for the data it acquired from Toysmart.[224]

---

214 *In re* Pharmatrak, Inc. Privacy Litig., 292 F.Supp.2d 263 (D. Mass 2003)

215 *In re* Facebook Privacy Litig., 791 F.Supp.2d at 712.

216 *Id.* at 714.

217 *Id.;* Doe 1 v. AOL LLC, 719 F.Supp.2d 1102, 1111 (N.D. Cal. 2010).

218 Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2012).

219 *FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding (last visited Oct. 10, 2018).

220 Mitchel Carrington, *Big Data Bankruptcy Sale Derailed – RadioShack's Customer Information Draws Objections*, BUTLER SNOW (Apr. 7, 2015), https://www.butlersnow.com/2015/04/big-data-bankruptcy-sale-derailed-radioshack-customers-information-draws-objections/.

221 15 U.S.C. § 45.

222 Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of* Privacy, 114 COLUM. L. REV. 583, 628 (Jan. 2014).

223 *FTC Announces Settlement with Bankrupt Website*, *supra* note 219.

224 Solove, *supra* note 169; *Business Transfer Clause in Privacy Policy*, TERMSFEED, https://termsfeed.com/blog/business-transfer-privacy-policy/ (last visited Sept. 30, 2018).

The Children's Online Privacy Protection Act protects the personal information of children under the age of thirteen that is collected online.[225] Claims have been made that voice-activated digital assistants in homes may violate children's privacy laws.[226]

Few statutes address the collection and use of PII.[227] The Health Insurance Portability Act imposes security standards to the privacy of individually identifiable health information.[228] This may apply to any e-commerce company with a focus on health care or related topics.[229] However, voice-captured biometric data such as size, weight, physical discomforts, lifestyle preferences, and pregnancy, may violate health privacy laws.[230]

The Bankruptcy Abuse and Consumer Protection Act of 2005 (BACPA) instituted safeguards to protect consumer data by requiring use of a "consumer ombudsman" in bankruptcies involving consumer data.[231] Section 101(41A) of the Bankruptcy Code defines PII within the meaning of the Code, "if provided by an individual in connection with obtaining a product or service from the debtor primarily for personal, family or household purposes."[232] Section 363(b)(1) of the Code provides that if the debtor has a privacy policy in effect at the time of the bankruptcy filing which prohibits the transfer of PII, the PII cannot be sold in bankruptcy unless additional requirements are satisfied.[233] If triggered, section 363(b)(1) prohibits the sale of PII unless the bankruptcy court finds that the sale is consistent with the debtor's privacy policy or the court approves the sale at a hearing after (a) appointing a consumer privacy ombudsman to assist the court in reviewing the facts and circumstances of the sale and (b) finding that the sale of the information would not violate applicable

---

225 Children's Online Privacy Protection Rule, 16 C.F.R. §312 (2013).

226 Hillary Brill & Scott Jones, *Little Things and Big Challenges: Information Privacy and the Internet of Things*, 66 AM. U. L. REV. 1183, 1201 (2017); Elvy, *supra* note 5, at 1377; Lipman, *supra* note 10 at 789.

227 Wrongful Disclosure of Video Tape Rental or Sale Records, 18 U.S.C.A. § 2710 (2013); Protection of Subscriber Privacy, 47 U.S.C.A § 551 (2001).

228 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

229 Newtek, *Does Your Business Need to be HIPAA – Compliant?*, FORBES (Feb 6, 2014, 2:11 PM), https://www.forbes.com/sites/thesba/2014/02/06/does-your-business-need-to-be-hipaa-compliant/#9e84a3b3d7cc (explaining that any business handling health care information needs to be HIPAA compliant).

230 Drew Harwell, *Companies Race to Gather a Newly Prized Currency: Our Body Measurements*, WASH. POST (Jan. 16, 2018), https://www.washingtonpost.com/business/economy/companies-race-to-gather-a-newly-prized-currency-our-body-measurements/2018/01/16/5af28d98-f6e8-11e7-beb6-c8d48830c54d_story.html?utm_term=.f0a44cccef1d.

231 11 U.S.C. § 332 (2009).

232 11 U.S.C. § 101(41A) (2016).

233 11 U.S.C. § 363(b)(1) (2010).

non-bankruptcy law.[234] This issue has been litigated in the *RadioShack* bankruptcy case described above, as well as in other cases.[235]

2. Proposed New Legislation Governing Use of Voice-Captured Personal Data

Voice-captured data from consumer devices may contain PII, since device owners are linked to an account identifying them as specific users.[236] This is distinct from anonymous IP addresses, which identifies computers and other devices connected to the Internet.[237] This fact, combined with the private nature of information typically transmitted by household voice-activated devices—health, measurements, personal preferences, and personal conversations, to name a few—makes such data even more critical to protect from dissemination, particularly for commercial uses.[238]

Voice-activated devices also capture data from children under thirteen.[239] This collection of data from children could be illegal and violate child privacy laws.[240] Even if collecting such data is permissible, its acquisition or use by third-parties may not be.[241]

The European Union's recent General Data Protection Regulation (GDPR) provides a robust model enhancing the rights of citizens to affirmatively consent, access, transfer, and erase data collected from them.[242] GDPR may already affect

---

234 *Id*.

235 *In re* Radio Shack, No. 15-10197, 550 B.R. 700, 703 (Bankr. D. Del. 2016); *In re* BPS US Holdings, Inc., No. 16-12373, 2017 WL 4990423, at *1 (Bankr.D. Del. 2017); *In re* Aeropostale, Inc., No. 16-11275, 555 B.R. 369, 375 (Bankr. S.D.N.Y 2016); *In re* Golfsmith Int'l Hold., Inc., No. 16–12033, 2016 WL 10574676, at *1 (Bankr .D. Del. 2016); *In re* Sports Auth. Hold. Inc, No. 16-386-SLR, 2016 WL 3041846, at *1 (Bankr. D. Del. 2016).

236 *See* Eric Boughman et al., *"Alexa, Do You Have Rights?": Legal Issues Posed by Voice-Controlled Devices and the Data They Create*, AM. BAR ASS'N: BUS. L. TODAY (July 2017), https://www.americanbar.org/publications/blt/2017/07/05_boughman.html (explaining that voice data can become "finely turned to each individual user").

237 *See* Alex Johnson, *The Internet is Now Officially Too Big as IP Addresses Run Ou*t, NBC NEWS (July 2, 2015, 7:18 PM), https://www.nbcnews.com/news/us-news/internet-now-officially-too-big-ip-addresses-run-out-n386081 (defining IP addresses as "the numbers that identify every computer, smartphone and device connected to the Internet").

238 *See* Harwell, *supra* note 230 (detailing the type of personal information collected by companies).

239 Mark Harris, *Virtual Assistants Such as Amazon's Echo Break US Child Privacy Law, Experts Say*, GUARDIAN (Feb. 15, 2018, 4:23 PM), https://www.theguardian.com/technology/2016/may/26/amazon-echo-virtual-assistant-child-privacy-law.

240 *Id*.

241 *See id.* (highlighting the story of two software developers who were fined $300,000 for letting third-party advertisers collect data from children through their application).

242 *A New Era for Data Protection in the EU: What Changes after May 2018*, at 1-3, https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf (last visited Sept. 30, 2018); Alex Hern, *What is GDPR and How Will it*

personal data usage in the United States.[243] This legislation, which became effective May 25, 2018, is designed to "harmonize data privacy laws across Europe, [protect] and empower all EU citizens data privacy[,] [and reshape] the way organizations across the region approach data privacy."[244] By "replacing the 1995 data directive, GDPR comprises ninety-nine articles setting out the rights of individuals and obligations placed on organizations covered by the regulation."[245] Among these is the right of people "to have easier access to the data companies hold about them, a new fines regime and a clear responsibility for organizations to obtain the consent of people they collect information about."[246]

Amongst the changes, the GDPR creates the right of individuals to access the data companies hold about them—not only free of charge, but within one month of the request.[247] This combined with a portability provision, gives individuals the right to also transmit or transfer the data a company holds about them to a different company.[248] Moreover, under the "Right to Be Forgotten," individuals can have their data erased when it is no longer necessary for the purpose for which it was collected.[249] Grounds for erasing data include the individual's having withdrawn consent, a lack of legitimate interest in keeping it, and if it was unlawfully used.[250]

The standard for providing consent became stricter under the GDPR, as companies now have to provide individuals with an intelligible and more easily accessible form to provide consent, and that form must describe the purpose for which the collected data will be used.[251] Not only must consent be described clearly and provided without confusion, individuals have the right to withdraw

---

Affect You?, GUARDIAN (May 21, 2018, 9:40 AM), https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you (explaining that this new regulation entails more consumer power over the management of personal data).

243 Jeff John Roberts, *GDPR Is in Effect: Should U.S. Companies Be Afraid?*, FORTUNE (May 25, 2018), http://fortune.com/2018/05/24/the-gdpr-is-in-effect-should-u-s-companies-be-afraid/.

244 EU GDPR PORTAL, https://www.eugdpr.org/key-changes.html (last visited Apr. 18, 2018); *see also* Matt Burgess, *What is GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED UK (Apr. 5, 2018), http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

245 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the procession of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, 3.

246 *Id*. at 11

247 *Id*.

248 *Id*. at 13.

249 *Id*. at 12.

250 *Id*.

251 *Id*. at 37.

their consent as easily as they provide it.[252]

Although the GDPR does not expressly protect voice data captured by smart speakers, Article 22 of the GDPR addresses artificial intelligence, stating "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her" without clear consent.[253] As a result, in Europe, AI technologies that interact with consumers, such as smart speakers and self-driving cars, will now have to provide explicit statements that they are listening and receive opt-in consent to record.[254] Devices such as Amazon Echo or Google Home might satisfy this requirement by playing a brief verbal statement upon setup that asks the owner to approve the use of his or her personal data, though there could be a need for additional periodic consents.[255]

Another GDPR provision that could impact voice data pertains to rules about algorithm decision making.[256] The "GDPR provides that a person whose data is collected has a general right to a human review and explanation of algorithmic decisions involved in the process, which may become problematic for companies that automate certain data collection processes."[257]

Following enactment of the GDPR, the European Union's Council promptly drafted the equally significant E-Privacy Regulation (EPR), expected to take effect in 2019 or 2020.[258] The EPR is intended to complement GDPR by restricting the ways in which voice data may be used.[259] While EPR's

---

252 *Id*.

253 Greg Sterling, *Echo and Home Will Probably Have to Tell You They're Always Listening — in Europe*, SEARCH ENGINE LAND (Oct. 11, 2017, 10:44 AM), https://searchengineland.com/echo-home-will-probably-tell-theyre-always-listening-europe-284435.

254 *Id*.

255 *Id*.

256 CE Pro Editors, *How GDPR Privacy Rules Could Hamper Smart Home AI*, CE PRO (May 22, 2018), https://www.cepro.com/article/gdpr_privacy_rules_smart_home_AI.

257 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the procession of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, 9.

258 Shannon Bond, *Alexa Is Always Listening, GDPR Is Here, Uber Crash Report, F1 Goes over the Top*, FIN. TIMES (May 27, 2018), https://www.ft.com/content/c6ca3c36-61ec-11e8-a39d-4df188287fff; Erika Morphy, *What You Should Know about the ePrivacy Regulation*, CMSWIRE: CUSTOMER EXPERIENCE (Aug. 27, 2018), https://www.cmswire.com/customer-experience/what-you-should-know-about-the-eprivacy-directive/; Conner Forrest, *GDPR vs. ePrivacy: The 3 Differences You Need to Know*, TECHREPUBLIC (May 29, 2018, 10:48 AM), https://www.techrepublic.com/article/gdpr-vs-eprivacy-the-3-differences-you-need-to-know/.

259 Morphy, *supra* note 258; Forrest, *supra* note 258; Ezra Steinhardt, *Voice Technologies, Meet the EU E-Privacy Regulation*, INSIDE PRIVACY (Jan. 19, 2018), https://www.insideprivacy.com/international/european-union/voice-technologies-meet-the-eu-e-privacy-regulation/; Council Directive 17/0003, 2017 O.J. (EC) [hereinafter *Council*

predecessor, the E-Privacy Directive, originally regulated email and SMS text messages—excluding newer communication providers such as instant-messaging and voice-over IP companies—EPR's coverage extends beyond the traditional wired, mobile, and satellite-based telecommunications providers to include WhatsApp, Facebook Messenger, and Skype, among others.[260]

Unlike the GDPR, which focuses on protecting personal data, the EPR applies to confidentiality in electronic communications, including confidentiality of non-personal data and meta-data that is related to a person.[261] Furthermore, EPR proposes to limit the use of voice data by prohibiting its processing by anyone except the end-user, potentially cutting out entities that perform product research, design, and development, and by restricting the legitimate grounds for processing to those entities obligated to fulfil a contract or who have explicit consent to process the data.[262] EPR also addresses grounds for retention and deletion of voice data.[263]

The EPR will apply to U.S. companies that provide electronic communications and that use such communications to send direct marketing content, collect information from users, and implement cookies, including messaging applications.[264] Companies will need to secure the contents and metadata from those communications by anonymizing or deleting it.[265]

Where neither federal nor foreign laws are able to reach and protect voice-captured data, progressive state laws may help fill in gaps.[266] California is one of the first states to codify the right of privacy in its constitution, and continues to be on the forefront of protecting certain types of consumer data.[267] These laws attempt to balance commercial interests with consumer privacy interests by placing limits on the sale and sharing of personal data acquired in certain circumstances.[268] California's legislature has introduced as many as fourteen

---

Directive].

260 Forrest, *supra* note 258; *Council Directive*, *supra* note 259.

261 Morphy, *supra* note 258; *Council Directive*, *supra* note 259

262 Steinhardt, *supra* note 259.

263 *Id*.; *Council Directive*, *supra* note 259.

264 Morphy, *supra* note 258.

265 *Id*.

266 Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 20, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

267 Hogan Lovells, *California Continues to Shape Privacy and Data Security Standards*, INT'L ASS'N OF PRIVACY PROF'LS – PRIVACY TRACKER (Oct. 1, 2013), https://iapp.org/news/a/california-continues-to-shape-privacy-and-data-security-standards/; 2018 Cal. Stats. ch. 55.

268 *See* Hogan Lovells, *supra* note 267; *see also* A.B. 375, 2017-2018 Gen. Assemb., Reg. Sess. (Cal. 2018) (to be codified at Cal. Civ. Code § 1798).

new bills pertaining to privacy in one year.[269] For example, in addition to requiring all websites that collect personal data to display a privacy policy, California's Attorney General developed an agreement with mobile application platforms that encourages developers to provide users with privacy policies before downloading the application.[270]

In 2015, California's "Privacy Rights for California Minors in the Digital World" went into effect, which requires website operators that target minors (or know that minors use their websites) to allow minors the ability to access and delete information posted by the minors.[271] In addition, such websites must inform minors of their rights and how they may exercise those rights.[272] In the same year, an amendment to California's Online Privacy Protection Act was signed, which requires website operators to disclose if third parties, such as advertising networks and data analytics companies, collect PII that reveal a consumer's online history, including whether the consumer browses different websites in conjunction with the operator's sites and services.[273] Website operators must also disclose how they treat consumers' elections to use such signals as do-not-track mechanisms by which consumers may indicate data collection preferences during their online sessions.[274]

Most recently, California ushered in the groundbreaking California Consumer Privacy Act (CaCPA) of 2018, which gives its residents more control over their data that is collected by companies.[275] By housing the world's fifth largest economy, America's most populated state has made waves on this side of the Atlantic by arming its consumers with unprecedented rights to access, protect, and delete data collected about them.[276]

---

269 Hogan Lovells, *supra* note 267/; Ellen Tannem, *How the California Data Privacy Law Could Cause Shockwaves in the US*, SILICONREPUBLIC (Jul 17, 2018), https://www.siliconrepublic.com/enterprise/california-data-law-us.

270 Hogan Lovells, *supra* note 267.

271 Cal. Bus. Prof. Code § 22580 (2018).

272 Hogan Lovells, *supra* note 267.

273 Cal. Bus. Prof. Code § 22575-579 (2018).

274 Hogan Lovells, *California Continues to Shape Privacy and Data Security Standards*, INT'L ASS'N OF PRIVACY PROF'LS – PRIVACY TRACKER (Oct. 1, 2013), https://iapp.org/news/a/california-continues-to-shape-privacy-and-data-security-standards/; *Cal. Online Privacy Protection Act (CalOPPA)*, EDUC. FOUND.: CONSUMER FED'N OF CALIFORNIA (July 29, 2015), https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/.

275 A.B. 375, 2017-2018 Gen. Assemb., Reg. Sess. (Cal. 2018) (to be codified at Cal. Civ. Code § 1798.185); Lothar Determann, *Analysis: The California Consumer Privacy Act of 2018*, INT'L ASS'N OF PRIVACY PROF'LS – PRIVACY TRACKER (July 2, 2018), https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/.

276 *California Population 2018*, WORLD POPULATION REV., http://worldpopulationreview.com/states/california-population/ (last visited Sept. 17, 2018); Navneet Mathur, *We're Months into GDPR. So, What's Next?*, DATANAMI (Sept. 12, 2018), https://www.datanami.com/2018/09/12/were-months-into-gdpr-so-whats-next/; Determann,

Enacted in June 2018 and amended in August 2018, CaCPA is anticipated to take effect January 1, 2020.[277] This sweeping legislation protects the personal information of not only California's consumers (even those who temporarily leave the state) but of its employees, students, and patients.[278] Likewise, "personal information" is defined broadly as "any information that . . . relates to . . . a particular consumer or household" and can be protected even if it does not contain a name.[279] This unnamed personal data may include a household's utility usage, a person's IP address or browsing history, and an employee's job description—provided it can be "reasonably linked, directly or indirectly, with a particular consumer or household."[280]

CaCPA allows protected individuals to request a record of an organization's data about the individual with respect to how the organization is using and sharing that data with third-parties.[281] Organizations that sell data will be required to disclose it, and protected individuals will have the right to object to the sale of their data. Objection to sale of data will become relatively easy since organizations will have to display a conspicuous "Do Not Sell My Personal Information" button on their home page.[282] Organizations that sell children's data will require children aged between 13 and 16 years old to opt in (or, if children are under 13 years old, their parents).[283]

Protected individuals will also have the right to have their data erased, subject to exceptions for completing business transactions, doing research, complying with free speech, and using the data internally for analytical purposes.[284] Companies located worldwide will be required to comply with CaCPA if they receive personal data from California residents and engage—either by themselves or through a parent/subsidiary—in one of the following: (1) earn an annual gross revenue of $25 million; (2) hold personal information of at least

---

supra note 275.

277 *California Consumer Privacy Act*, INT'L ASS'N OF PRIVACY PROF'LS – RESOURCE CENTER, https://iapp.org/resources/topics/california-consumer-privacy-act/ (last visited Sept. 17, 2018).

278 Determann, *supra* note 275.

279 Cal. Civ. Code §1798.140(o)(1) (2018); Determann, *supra* note 275.

280 Determann, *supra* note 275; Michael Lamb, *California Legislature Publishes CaCPA Amendments; Vote Scheduled for this Week*, INT'L ASS'N OF PRIVACY PROF'LS – PRIVACY TRACKER (Aug 27, 2018), https://iapp.org/news/a/california-legislature-publishes-cacpa-amendments-vote-scheduled-for-this-week/.

281 *California Consumer Privacy Act*, *supra* note 277.

282 *Id.;* Determann, *supra* note 275; Kristen J. Mathews & Courtney M. Bowman, *The California Consumer Privacy Act of 2018*, PROSKAUER: PRIVACY L. BLOG (July 13, 2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/.

283 *California Consumer Privacy Act*, *supra* note 277.

284 *Id.*

50,000 California residents, households or devices per year; or (3) derive at least half of their revenue from selling California residents' personal information.[285]

Other laws addressed by California's legislature include placing data restrictions on credit-card purchases and debit-card purchases, regulating how consumer health management applications can use data, and facilitating consumers' rights to a class action lawsuit for harm arising from sharing their PII without express opt-in consent.[286]

Surprisingly, some of the nation's most prominent technology companies are now lobbying for a federal privacy law.[287] Reacting to concerns that CaCPA could spur legislation in other states, which could lead to potentially more constraints than GDPR, technology leaders such as Facebook, Google, IBM, and Microsoft hope to mobilize a federal privacy law that would supersede California's privacy law and replace it with more flexible rules on a national level. These laws would leave the relative discretion in how to handle personal digital information up to the companies in question.[288] While technology companies argue that increased state legislation could lead to a compliance nightmare, consumer and privacy groups worry that weakening California's standards could have an adverse effect on consumers, particularly in light of Facebook's recent scandal involving the allegedly unauthorized harvesting of psychographic personal data from 50 million Facebook profiles by consultancy firm Cambridge Analytica.[289] Notwithstanding, Google, Facebook, and other tech giants concede increased regulation of data privacy is inevitable, which may explain the rush to adopt voluntary standards instead of forced mandates.[290]

V. CONCLUSION

First, property law principles should be used alongside contract law to identify and assign appropriate rights to various owners of voice-captured personal data. This is particularly critical to address the sharing and commercial dissemination of personal data beyond a consumer's contracted consent. Second, UCC Article 9 may benefit from an amendment as it pertains to creation, perfection, and repossession of security interests in data. At the very least, companies that claim

---

285 Mathews & Bowman, *supra* note 282; Determann, *supra* note 275.

286 Hogan Lovells, *supra* note 267.

287 Cecilia Kang, *Tech Industry Pursues a Federal Privacy Law, on Its Own Terms*, N.Y. TIMES (Aug. 26, 2018), https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html.

288 *Id*.

289 *Id*.; Sam Meredith, *Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal*, CNBC (Apr. 10, 2018, 7:22 AM), https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html.

290 Kang, *supra* note 287.

to have a policy of not selling personal data should be limited in their ability to collateralize personal data assets. Third, voice-captured data collected in consumers' homes deserves a higher level of regulation on a federal level than currently governs data collected by computer or handheld devices through internet browsers. This is critical to protect at-risk parties such as children or unsuspecting household guests who did not provide consent for their voice data to be shared. Even for those adult device users that consented to using the device, stricter measures are warranted due to the intimate nature of conversations and sounds that voice-activated devices may pick up in the privacy of their homes. The recent push by Europe and California to better balance the commoditization of data with the rights of individuals to access and protect their personal data underscores the urgency of addressing this issue using a single, streamlined regulatory scheme.