NOTES

PRIVACY PROTECTIONS FOR SECONDARY USERS OF COMMUNICATIONS-CAPTURING TECHNOLOGIES

ALEX B. LIPTON*

Consumer products increasingly record the content of user communications without regard to whether the recorded individual is the primary user—the purchaser of the product—or the secondary user—an individual who uses the product but is not the purchaser. The distinction between primary and secondary users proves significant when considering the enforceability of the product's privacy policy, which purports to establish user consent to the collection of communications content but is only agreed to by the primary user, and protections available under federal and state statutes, many of which prohibit the recording of communications content without consent, and may thus benefit secondary users. This Note analyzes several privacy policies accompanying communications-capturing technologies as well as state eavesdropping laws and the Electronic Communications Privacy Act to demonstrate that the current consumer privacy regime does not adequately protect secondary users of communications-capturing technologies.

In designing protections for secondary users, this Note argues against requiring companies to provide front-end protection through notice of their privacy policies. Instead, this Note proposes a framework for incentivizing communications-capturing technology producers to distinguish between primary and secondary user data use on the back end.

 J.D. Candidate, 2016, New York University School of Law; A.B. 2011, Harvard College. I am grateful for the support of the Furman Academic Scholars Program, the Mitchell Jacobson Leadership Program in Law and Business, the Information Law Institute, and the 2015–16 Editorial Board of the *New York University Law Review*. Special thanks to Professors Barry Friedman, Clayton Gillette, Florencia Marotta-Wurgler, Helen Nissenbaum, Ira Rubinstein, and Katherine Strandburg.

Introduction

Amazon Echo, which serves as a personal home assistant that responds to voice commands, captures the content of communications within your home.[1] Samsung's SmartTV records what you and others say in your living room and transmits it to a third party.[2] Mattel's newest doll, the Hello Barbie, records what young users say to the doll and transmits that information to a server in order to improve the doll's responses to users.[3] Though they all serve beneficial purposes, these "communications-capturing technologies" record the content of user communications without regard to whether the recorded individual is the purchaser or a nonpurchaser user. Companies justify expansive collection and disclosure of primary user data based on consent to the terms of their privacy policies.[4] But when did nonpurchaser users consent to having their communications data collected by these communications-capturing technologies? Do any legal protections

[1] *See* Sam Machkovech, *Amazon Announces Echo, a $199 Voice-Driven Home Assistant*, Ars Technica (Nov. 6, 2014), http://arstechnica.com/gadgets/2014/11/amazon-announces-echo-a-199-voice-driven-home-assistant ("[W]e look forward to testing everything else advertised about the Amazon Echo, including its ability to hear words at almost any volume in a nearby vicinity . . . .").

[2] *See Samsung Privacy Policy—SmartTV Supplement*, Samsung, http://www.samsung.com/sg/info/privacy/smarttv.html (last visited Jan. 11, 2016) ("[I]nteractive voice commands may be transmitted (along with information about your device, including device identifiers) to a third-party service provider (currently, Nuance Communications, Inc.) that converts your interactive voice commands to text and to the extent necessary to provide the Voice Recognition features to you."); Chris Matyszczyk, *Samsung Changes Smart TV Privacy Policy in Wake of Spying Fears*, CNET (Feb. 10, 2015, 12:35 PM), http://www.cnet.com/news/samsung-changes-smarttv-privacy-policy-in-wake-of-spying-fears (describing Samsung's attempts to allay fears about passive recording of communications content in the living room).

[3] *See* Sarah Halzack, *Privacy Advocates Try to Keep 'Creepy,' 'Eavesdropping' Hello Barbie from Hitting Shelves*, Wash. Post (Mar. 11, 2015), http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/11/privacy-advocates-try-to-keep-creepy-eavesdropping-hello-barbie-from-hitting-shelves ("Hello Barbie works by recording a child's voice with an embedded microphone that is triggered by pressing a button on the doll. As the doll 'listens,' audio recordings travel over the Web to a server . . . . That information is used to help form Hello Barbie's responses.").

[4] *See infra* notes 23–25 and accompanying text (describing expansive data collection and use practices described in companies' privacy policies).

exist to either prevent data collection of nonpurchaser users or protect their already-collected data?

Purchasers of a product—whom I call "primary users"—consent to having their communications recorded when they agree to the terms of company privacy policies.[5] Privacy policies arguably provide primary users with notice about how their data will be collected and used by companies.[6] They also, however, prevent primary users from making statutory claims against the seller for privacy intrusions because current statutes provide exceptions based on consent.[7]

Nonpurchaser users—whom I call "secondary users"—also use communications-capturing technologies when, for example, they visit the home of a friend and use the products. Under even the broadest view of assent in consumer contracts, secondary users do not consent to the product's collection of their communications data or the terms described in privacy policies.[8] Despite the fact that secondary users did not consent to or even receive notice of the privacy policy, their data—and, more specifically, the content of their communications—will be recorded, transmitted, and potentially disclosed to third parties when they use, or are simply in the vicinity of communications-capturing technologies. Secondary users are unable to enjoy even the limited legal protections provided by privacy policies because they are not parties to the contracts. Instead, secondary users must rely on a patchwork of privacy statutes not designed with communications-capturing technologies in mind. However, this Note shows how even

---

[5] *See, e.g.*, Nguyen v. Barnes & Noble, Inc., 763 F.3d 1171, 1177 (9th Cir. 2014) ("[W]here, as here, there is no evidence that a website user had actual knowledge of the agreement, the validity of the browsewrap agreement turns on whether the website puts a reasonably prudent user on inquiry notice of the terms of the contract."); Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors,* 44 AM. BUS. L.J. 55, 64 (2007) (describing privacy policies as ways to "provide notice to customers of a company's privacy practices before any commercial transaction occur[s]"); Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN ST. L. REV. 587, 596 (2007) ("[M]ost websites in fact present these policies and amendments thereto as binding upon visitors, using the language of contract and assent. AOL's Terms of Use state: 'Your ongoing use of AOL.COM signifies your consent to the information practices disclosed in our Privacy Policy.'").

[6] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 79–80 (Jack M. Balkin & Beth Simone Noveck eds., 2004). *But see* Florencia Marotta-Wurgler, *Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts*," 78 U. CHI. L. REV. 165 (2011) (finding that mandatory disclosure does not significantly increase readership of online contracts).

[7] *See infra* Part III (describing statutory exceptions based on consent).

[8] *See Nguyen*, 763 F.3d at 1177 (noting that putting a consumer on inquiry notice suffices for consumer contract formation).

these privacy statutes will not provide secondary users with adequate protection from communications-capturing technologies.

In our current consumer privacy regime, we tolerate expansive and often unpopular data use practices because primary users consented to those practices when they purchased the product or agreed to the privacy policy. Secondary users, however, do not purchase the products and never agree to—or even have an opportunity to view—the privacy policies governing communications-capturing technologies. The current state of affairs leaves secondary users exposed to significant privacy risks without even the minimal safeguards available to primary users.

We should be troubled by the rise of communications-capturing technologies and their effect on secondary users for three reasons. First, surreptitiously recording communications without consent has long been viewed as a privacy violation.[9] Second, secondary users will likely comprise a much larger group than primary users, since several secondary users could have their communications captured for every primary user. Third, the failure to protect secondary users who never have the opportunity to and never actually consent to the capture of their communications content threatens to further dilute the concept of consent, a concept that has been steadily eroding in the age of digital browsewrap agreements.[10] This Note is motivated by the strong sentiments against nonconsensual communication capture, the potentially large and unrecognized constituency of affected secondary users, and the eroding effect these technologies may have on consumer privacy protections. While there may be debate over the significance and extent of the privacy protections secondary users should be afforded, protections should be fully considered before the ubiquity of communications-capturing technologies outpaces the law's ability to respond.

Part I of this Note provides definitions of "communications-capturing technologies," "primary users," and "secondary users." Part II analyzes several privacy policies accompanying communications-capturing technologies and describes why courts will not consider secondary users parties to these privacy policies. Part III surveys state eavesdropping laws and the Electronic Communications Privacy Act to show that claims available to nonconsenting secondary users under

---

[9] *See infra* Part III (surveying single-party and all-party consent exceptions in state recording statutes).

[10] *See* Juliet M. Moringiello & William L. Reynolds, *From Lord Coke to Internet Privacy: The Past, Present, and Future of the Law of Electronic Contracting*, 72 MD. L. REV. 452, 454 (2013) (describing the departure from requiring express manifestations of assent in electronic contracting).

state and federal statutes do not provide adequate protection from communications-capturing technologies. Part IV proposes a set of legal requirements that could protect secondary user communications from communications-capturing technologies. In designing protections for secondary users, I argue against requiring companies to provide front-end protection in the form of notice of the privacy policy terms. Instead, I would allow producers of communications-capturing technologies to freely collect secondary user communications. However, if producers of communications-capturing technologies collect secondary user communications, they must distinguish between primary and secondary user communications on the back end. Companies that successfully distinguish between primary and secondary user communications can treat primary user communications in accordance with their privacy policies, but must adhere to strict use and resale restrictions with respect to secondary user communications. Companies that fail to distinguish between primary and secondary user communications must treat all of their recorded communications as belonging to secondary users. This framework encourages the adoption of innovative communications-capturing technologies while protecting secondary users, who do not consent to the back-end use and disclosure of their communications as described in privacy policies.

I
DEFINITIONS

A. Communications-Capturing Technology

Communications-capturing technologies have two distinct features: (1) they record the content of user communications, not just the metadata and (2) they transmit that content either back to the product manufacturer or to a third party, which contracts with the manufacturer to analyze and store user communications. Why focus on communications content and not on user data of any kind? The law affords a high degree of privacy to the content of communications.[11] Because of this long tradition of protecting the privacy of user communications, courts and regulators may be more willing to afford secondary users protections for communications content where secondary data capture would otherwise be viewed as incidental or insignificant.

[11] *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1017–31 (2010) (describing the content/non-content distinction in privacy law); Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2112–13 (2009) (describing the history and importance of the content/non-content distinction).

Consider the following examples: The Samsung SmartTV would be considered a communications-capturing technology because it (1) records the words (i.e. the actual content) spoken by users and (2) transmits user communications to a centralized server.[12] Fitness trackers, such as certain versions of the Jawbone or Fitbit, track and record users' location, calories burned, and steps taken, and transmit this data to a centralized server.[13] While secondary users could easily borrow these items from primary users and thus have their data recorded and transmitted, the data collected is not *communications content*, and therefore, these trackers are not communications-capturing technologies. These internet-connected products, sometimes referred to as examples of the "Internet of Things,"[14] are also deserving of scrutiny, but are not the focus of this Note. Similarly, simple pedometers which record steps taken but do not transmit that data to a centralized server do not pose the same risks to secondary users as communications-capturing technologies, and thus are not discussed. Finally, products that store communications locally but do not transmit those communications to a central location are not the focus of this Note, as those products inherently constrain the ability of companies to use and disclose user communications.

B. Primary and Secondary User

I define the "primary user" as the purchaser of the product and the "secondary user" as any nonpurchaser user of the product. The law regularly distinguishes between purchaser and nonpurchaser users. In the products liability context, for example, the law at first afforded different protections for primary and secondary users, and only began to recognize the need to protect secondary users during the last century.[15] The law also distinguishes between parties to the

---

[12] *See* Matyszczyk, *supra* note 2 (describing the data privacy practices and backlash surrounding the announcement of the Samsung SmartTV).

[13] *See Privacy Policy*, FITBIT, http://www.fitbit.com/legal/privacy-policy (last updated Dec. 14, 2014) (outlining the type of information that may be collected by Fitbit products); *UP Privacy Policy*, JAWBONE, https://jawbone.com/up/privacy (last visited Jan. 17, 2016) (outlining the type of information that may be collected by Jawbone products).

[14] *See, e.g.*, FEDERAL TRADE COMMISSION, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 5, 14–46 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (defining the "Internet of Things" and discussing its privacy implications).

[15] *See* MacPherson v. Buick Motor Co., 111 N.E. 1050, 1053 (N.Y. 1916) (removing the requirement of privity of contract for duty in negligence actions); William M. Landes & Richard A. Posner, *A Positive Economic Analysis of Products Liability*, 14 J. LEGAL STUD. 535, 550–51 (1985) (noting the slow demise of the bystander rule in products liability, which denied recovery to nonpurchaser users injured by defective products).

contract—which, in the case of consumer products, would most often be the purchaser of the product and the seller or manufacturer—and nonparties through the language of privity.[16] Save for limited applications of the third-party beneficiary rule,[17] individuals who are not parties to a contract may not maintain an action for breach of contract. As described below in Part II, secondary users will not be considered parties to privacy policies for communications-capturing technologies, and will thus be afforded different protections than purchasers, who will almost certainly be considered parties to the contract under modern consumer contract law.

While the concept of secondary users has been extensively discussed in other legal contexts,[18] the distinction between primary and secondary users has not yet been introduced in consumer privacy statutes, case law, or scholarly articles. This Note represents the first attempt to define secondary users as an important constituency in the consumer privacy context.

My focus on secondary users should not be read as a suggestion to ignore the privacy harms which can and do affect primary users of communications-capturing technologies. The goal of this Note, however, is not to discuss all of the privacy harms which could occur with the use of communications-capturing technologies, but to bring to light a constituency whose privacy interests have been largely ignored in privacy debates. As the use of communications-capturing technologies grows, so too will the importance of designing privacy protections with secondary users in mind.

Before suggesting designs for new privacy protections, we must first survey what protections are available to users of communications-capturing technologies today.

---

[16] *See* Richard A. Epstein, *Into the Frying Pan: Standing and Privity in Telecommunications Law*, 4 COLUM. SCI. & TECH. L. REV., 1, 7 (2003) (describing the role of privity in contract law). While privity usually describes the relationship between purchasers and the manufacturer or seller, modern consumer contract law would also recognize a contract between an individual who did *not* purchase the product but who, at a minimum, was put on inquiry notice of the language of a privacy policy or terms and conditions when receiving the product from the individual who did purchase the product. *Cf.* Nguyen v. Barnes & Noble, Inc., 763 F.3d 1171, 1177 (9th Cir. 2014) (noting that an online consumer contract will be upheld against the user where "the website puts a reasonably prudent user on inquiry notice of the terms of the contract").

[17] *See* Anthony Jon Waters, *The Property in the Promise: A Study of the Third Party Beneficiary Rule*, 98 HARV. L. REV. 1109 (1985) (describing historical applications of the third-party beneficiary rule).

[18] *See, e.g.*, CHARLES J. NAGY, JR., AMERICAN LAW OF PRODUCTS LIABILITY § 33:19 (3d ed. 2016) ("Many courts have held that the ultimate user of a product must be warned. Simply warning an immediate purchaser or dealer may not be enough . . . ."); Brizendine v. Visador Co., 437 F.2d 822, 828 (9th Cir. 1970) ("The manufacturing supplier's duty to warn . . . is not limited to warning the immediate purchaser.").

II
CONTRACTUAL PROTECTIONS FOR PRIMARY USERS: PRIVACY POLICIES OF COMMUNICATIONS-CAPTURING TECHNOLOGIES

Privacy policies, which outline how personal information about the user will be recorded, used, or disclosed by companies, provide the first level of protection for users of communications-capturing technologies.[19] A company can choose whether or not to adopt a privacy policy,[20] though in practice, the vast majority of companies operating online have privacy policies which explain how they use consumer data.[21] Widespread adoption of privacy policies may be due to the fact that California requires privacy policies for any company which collects the personal information of California residents, effectively setting a default requirement for any major website or data-capturing technology.[22] While reputational constraints may limit the extent to which companies engage in unpopular data practices,[23] in principle, companies that adopt privacy policies have nearly complete control over what terms to include, and can thus include terms that would offend even the least privacy-focused consumer.[24] Additionally, consumers typically do not have the opportunity to negotiate or alter the terms of a company's privacy policy.[25]

Given the fact that companies are not required to adopt these policies, can add nearly any pro-seller term they choose, and do not

---

[19] *See* SOLOVE, *supra* note 6 (describing privacy policies as ways for companies to describe and limit the "future uses of . . . information"); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 592 (2014) ("These policies described the various ways in which websites collected, used, and shared a visitor's personal information, as well as the various ways that information was protected.").

[20] Solove & Hartzog, *supra* note 19, at 593–94.

[21] Haynes, *supra* note 5, at 593–94.

[22] Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2008).

[23] *See, e.g.*, Tomio Geron, *After Backlash, Instagram Changes Back to Original Terms of Service*, FORBES (Dec. 20, 2012, 7:39 PM), http://www.forbes.com/sites/tomiogeron/2012/12/20/after-backlash-instagram-changes-back-to-original-terms-of-service (describing consumer backlash to Instagram's changed privacy policy and the removal of several offensive terms in the new policy).

[24] *See, e.g.*, *Microsoft Services Agreement*, MICROSOFT, http://www.xbox.com/ro-RO/legal/livetou (last visited Jan. 19, 2016) ("You should not expect any level of privacy concerning your use of the live communication features (for example, voice chat, video and communications in live-hosted gameplay sessions) offered through the Xbox Live/Games for Windows-Live service. We may monitor these communications to the extent permitted by law.").

[25] *See* SOLOVE, *supra* note 6, at 83 ("Most privacy policies provide no way for customers to prevent changes in the policy, and they lack a binding enforcement mechanism.").

provide consumers with the opportunity to alter terms, it might seem odd to label privacy policies as a form of privacy protection. Moreover, very few users read privacy policies, which are long and difficult to read, thus reducing their effectiveness as a form of notice on the front end.[26]

However, at least in principle, privacy policies do provide some limited front-end and back-end protections for product purchasers. Once primary users receive notice of a privacy policy's terms, they can either choose to exit the commercial relationship or continue if they do not find the terms objectionable. This "notice-and-choice" mechanism provides the buyer with a limited form of front-end privacy protection.[27] However, the potential front-end protection provided by privacy policies depends on the buyer reading the privacy policy and choosing not to purchase or continue using the product.[28] Though many users do not take advantage of the notice-and-choice mechanism when they choose not to read the privacy policy,[29] improved notice mechanisms may potentially improve the strength of this protection.[30]

If a seller violates its product's privacy policy by using data in a way that does not accord with the policy's terms, buyers can bring a breach of contract claim, thereby providing buyers with a form of back-end protection as well.[31] In practice, however, these back-end,

---

[26] *See* Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 546 (2014) ("Consumers seldom read the form contracts that firms offer."); Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1, 19, 22 (2014) (providing empirical evidence in support of the argument that consumers seldom read end-user license agreements, and finding that only six per every 1000 retail shoppers read the agreements).

[27] *See* Solove & Hartzog, *supra* note 19, at 592 (describing private industry's preference for self-regulation through a "notice and choice" mechanism).

[28] *See* Bakos, Marotta-Wurgler & Trossen, *supra* note 26, at 24, 27 (evaluating the informed minority hypothesis and concluding that almost no one reads their privacy policies or terms of use agreements).

[29] *See id*. at 19, 22 (providing empirical evidence that only a minute percentage of users read end-user license agreements).

[30] *See, e.g.*, YANG WANG ET AL., A FIELD TRIAL OF PRIVACY NUDGES FOR FACEBOOK (2014), http://yangwang.syr.edu/papers/CHI2014.pdf (suggesting that the notice system named "privacy nudges," which advise the user on potential privacy implications, can prevent users from making privacy disclosures that they later regret); M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1027, 1036–37 (2012) (providing examples of "'visceral' notice," such as the sound of a camera shutter even with new technologies that do not have a physical shutter mechanism, that help individuals recognize potential privacy-violating activities without textual notice).

[31] *See, e.g.*, *In re* Google, Inc. Privacy Policy Litig., 58 F. Supp. 3d 968, 986 (N.D. Cal. 2014) (holding that the plaintiff class adequately stated a claim for breach of contract when Google disclosed user data to third parties in violation of the company's privacy policy).

contract-based claims rarely succeed, often because the plaintiff fails to demonstrate any damages resulting from breach.[32] Though private actions for breach of privacy policies generally do not fare well, in certain instances, the Federal Trade Commission ("FTC") will bring an enforcement action when a seller breaches their privacy policy.[33] FTC enforcement actions provide another form of back-end protection based on the privacy policy.

Even the very limited protective features of privacy policies mentioned above—namely, the notice-and-choice feature as well as the opportunity to bring an action against the seller for breach—are unavailable to secondary users. Secondary users have no ex ante opportunity to read privacy policies in any meaningful sense, obviating any potential protections that a notice-and-choice mechanism could provide.[34] Similarly, since secondary users arguably are not parties to any contract formed by privacy policies, they will not be able to sue sellers for breach ex post.

However, the question of whether a secondary user is a party to the privacy policy of a communications-capturing technology is not so clear. It might seem reasonable to conclude that secondary users never enter into any kind of contract with the seller of a product they did not purchase, and therefore cannot avail themselves of the protections created by privacy policies.[35] However, the actual privacy policies of current communications-capturing technologies reveal several

---

[32] *See, e.g.*, *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 324–27 (E.D.N.Y. 2005) (denying breach of contract claims under the privacy policy where plaintiffs were unable to prove damages).

[33] *See* Solove & Hartzog, *supra* note 19, at 585 (describing the FTC's role as the agency which enforces breached privacy policies under their authority to police "unfair and deceptive" practices).

[34] This assumes, as is currently the case, that communications-capturing technologies do not provide notice and an opportunity to exit or consent every time someone other than the primary user begins using the product. Though manufacturers could introduce this front-end protection for secondary users, it will likely introduce too much friction in the user experience (as discussed in Part IV) and therefore is unlikely to be adopted.

[35] Privity is not required in the products liability context. *See* RESTATEMENT (SECOND) OF TORTS § 402A(2)(b) (1965) (noting that a user or consumer who has not bought a product from or entered into any contractual relation with a seller can bring an action where the defective product caused physical harm). However, actions under state law for breach of contract still require privity between the user and seller. *See, e.g.*, Montgomery v. Kraft Foods Glob., Inc., No. 1:12-CV-00149, 2012 WL 6084167, at *17 (W.D. Mich. Dec. 6, 2012) ("Contractual privity is an essential element of a breach of contract claim under Michigan law. No privity of contract exists between a consumer, who buys from a retailer, and a manufacturer who has not sold directly to the consumer." (internal citation omitted)). Given that privity of contract is not extended to remote *purchasers* of the product, I argue that privity of contract will not extend to remote *users* who did not purchase the product from a primary user, but instead, for example, use the product while visiting a primary user's home.

attempts by companies to capture the consent of secondary users.[36] These attempts to capture secondary user consent may be based on a belief that statutory protections are more robust than the limited remedies available for privacy policy breaches under a theory of contract,[37] and thus capturing secondary users within the privacy policy will be less costly to the seller overall.

Attempts to capture secondary user consent in privacy policies comes in the form of two types of clauses. The first type claims that the primary user represents that he or she will obtain consent from any secondary user that uses the product. I call this type of clause a "vicarious consent" clause, as it attempts to use the primary user's consent to vicariously capture secondary user consent. For example, ToyTalk, the company that produces the technology that will be incorporated in Mattel's Hello Barbie, includes the following clause in its privacy policies:

> By using any Service, you consent to ToyTalk's collection, use and/or disclosure of your personal information as described in this Policy. By allowing other people to use the Service via your account, you are confirming that you have the right to consent on their behalf to ToyTalk's collection, use and disclosure of their personal information as described below.[38]

Under the ToyTalk vicarious consent clause, it appears that the primary user's consent operates to bind not only the primary user's child who uses the Hello Barbie, but also any other children who visit the primary user's home and play with their children's communications-capturing toys. However, the enforceability of such a clause will almost certainly be called into question, especially outside of the parent-child context.[39]

---

[36] *See infra* notes 38, 41 and accompanying text (describing clauses in communications-capturing technologies which attempt to capture secondary user consent).

[37] Statutory remedies for privacy violations likely exceed damages that one could recover under a theory of contract, especially given the difficulty plaintiffs face when attempting to allege privacy damages under a breached privacy policy. *See* CAL. PENAL CODE §§ 631(a), 637.2 (West 2010) (setting forth criminal penalties for wiretapping, including imprisonment for up to a year or a maximum fine of $2,500 for first-time offenders, and providing injured persons with a civil cause of action); *JetBlue*, 379 F. Supp. 2d at 324–27 (describing the plaintiff's failure to allege privacy damages sufficient to maintain a claim under breach of contract).

[38] *Privacy Policy Terms of Use FAQ*, TOYTALK (Jan. 11, 2016), https://www.toytalk.com/legal/privacy.

[39] *Compare* Pollock v. Pollock, 154 F.3d 601, 610 (6th Cir. 1998) (holding that guardians with a "good faith" basis to believe that recording is "necessary and in the best interest of the child" may vicariously consent on behalf of the child for the purposes of the statute), *with* Debra Bogosavljevic, Note, *Can Parents Vicariously Consent to Recording a Telephone Conversation on Behalf of a Minor Child?: An Examination of the Vicarious Consent Exception Under Title III of the Omnibus Crime Control and Safe Streets Act of*

The second type of clause that attempts to capture secondary user consent simply states that by "using this product" you agree to the privacy policy. I call this type of clause a "use-equals-consent" clause. It resembles language commonly used in browsewrap agreements in online transactions.[40] An example of a use-equals-consent clause appears in the privacy policy provided by Nuance, the company that produces the speech-recognition technology for Samsung's SmartTVs:

> By using the Website or Nuance Products, you consent to the collection and use of your Personal Information by Nuance consistent with applicable data protection law and this Privacy Policy which is expressly incorporated into any applicable Website or Nuance Product Terms of Use or End-User License Agreement.[41]

Note that the use-equals-consent clause, while conceptually similar to those found in online browsewrap agreements, differs in at least one important way. With typical browsewrap agreements online, the seller can argue that the buyer was put on notice of the terms via a hyperlink on the website.[42] Use-equals-consent clauses like Nuance's assume that use of the product operates as consent to the privacy policy. Unlike a website, which can provide a hyperlink to the privacy policy's terms, many communications-capturing technologies, such as the Hello Barbie, will not provide such a link or notice mechanism to secondary users.[43]

The best evidence of how courts will interpret privacy policy clauses attempting to capture secondary user consent can be found in the existing clickwrap, browsewrap, and shrinkwrap jurisprudence

---

1968, 2000 U. ILL. L. REV. 321 (arguing that although some courts have held that guardians may consent on behalf of their children for the purposes of the Omnibus Crime Control and Safe Streets Act, other courts have rejected this approach and rightly refused to create a vicarious consent exception where none exists in the statute's language).

[40] *See, e.g.*, Nguyen v. Barnes & Noble, Inc., 763 F.3d 1171, 1174 (9th Cir. 2014) (citing Barnes & Noble's browsewrap clause governing its terms of use agreement, which stated that "[b]y visiting any area in the Barnes & Noble.com Site, creating an account, [or] making a purchase via the Barnes & Noble.com Site . . . a User is deemed to have accepted the Terms of Use" (second and third alterations in original)).

[41] *Nuance Communications, Inc. Privacy Policy General Information*, NUANCE, http://www.nuance.com/company/company-overview/company-policies/privacy-policies/index.htm (last visited Jan. 23, 2016).

[42] *See* Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 460 (2006) (defining "browsewrap" licenses).

[43] ToyTalk states that it will probably provide the privacy policy terms on an app that parents are required to download before children can use the voice-recognition features. *See* Halzack, *supra* note 3 ("But before the technology is activated, parents probably will have to sign into an app, create an account and consent to their children's voices being recorded, ToyTalk says."). However, these terms will not be present when secondary users attempt to use the product.

governing terms of use and privacy policies.[44] Clickwrap agreements are online agreements that require users to affirmatively agree to the terms—typically by clicking a box stating "I agree"—before using the product.[45] Browsewrap agreements provide terms, typically in a hyperlink somewhere on the website, and also do not require the user to read the terms.[46] However, unlike clickwrap agreements, browsewrap agreements do not require users to click "I agree" before using the product. Instead, the mere use of the product in combination with the availability of the terms on the website purportedly signals assent to the browsewrap agreement.[47] In this sense, browsewrap agreements are similar to their offline predecessors, shrinkwrap agreements, in which users agree to the terms accompanying physical copies of software by breaking the shrinkwrap packaging and running the program on their computer, even though they may not have read or expressly assented to the terms as required in clickwrap agreements.[48]

Courts enforce clickwrap agreements in which users affirmatively assent to the terms of a policy, even where users do not read the terms.[49] Browsewrap agreements, which were at first viewed with

---

[44] *Compare* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1452 (7th Cir. 1996) ("ProCD proposed a contract that a buyer would accept by *using* the software after having an opportunity to read the license at leisure. This Zeidenberg did. He had no choice, because the software splashed the license on the screen and would not let him proceed without indicating acceptance." (emphasis in original)), *with Nguyen*, 763 F.3d at 1178–79 ("Where a website . . . provides no [other] notice [of its terms of use] to users nor prompts them to take any affirmative action to demonstrate assent, even close proximity of the hyperlink to relevant buttons users must click on—without more—is insufficient to give rise to constructive notice."), *and* Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 32 (2d Cir. 2002) ("[W]here consumers are urged to download free software at the immediate click of a button, a reference to the existence of license terms on a submerged screen is not sufficient to place consumers on inquiry or constructive notice of those terms.").

[45] *See* Lemley, *supra* note 42, at 459–60 (discussing clickwrap, browsewrap, and shrinkwrap licenses).

[46] *Id.* at 460; Fteja v. Facebook, Inc., 841 F. Supp. 2d 829, 836 (S.D.N.Y. 2012) (describing browsewrap agreements as agreements "where website terms and conditions of use are posted on the website typically as a hyperlink at the bottom of the screen" (citing Hines v. Overstock.com, Inc., 668 F. Supp. 2d 362, 366 (E.D.N.Y. 2009))).

[47] Lemley, *supra* note 42, at 459–60; *see Specht*, 306 F.3d at 32 (describing notice requirements for the enforceability of browsewrap agreements).

[48] *See* Lemley, *supra* note 42, at 467 (explaining the theory of assent underlying shrinkwrap agreements).

[49] *See Nguyen*, 763 F.3d at 1176 ("Courts have also been more willing to find the requisite notice for constructive assent where the browsewrap agreement resembles a clickwrap agreement—that is, where the user is required to affirmatively acknowledge the agreement before proceeding with use of the website."); Lemley, *supra* note 42, at 466 ("Because the user has 'signed' the contract by clicking 'I agree,' every court to consider the issue has held clickwrap licenses enforceable.").

skepticism by many courts,[50] have been increasingly accepted as enforceable agreements where the seller puts a "reasonably prudent user on inquiry notice of the terms."[51] What conduct by sellers puts users on inquiry notice in the browsewrap context? The court in *Specht v. Netscape Communications Corp.* stated that "where consumers are urged to download free software at the immediate click of a button, a reference to the existence of license terms on a submerged screen is not sufficient to place consumers on inquiry or constructive notice of those terms."[52] Thus, communications-capturing technologies which require users to take some action, such as pushing a button,[53] but make no reference to the existence of terms anywhere on the product, will not place either primary or secondary users on notice of the terms under the reasoning in *Specht*.

Companies that produce communications-capturing technologies will likely rely on two theories to argue that primary users agreed to their privacy policies. First, companies will require primary users to affirmatively agree to terms on a website, smartphone application, or other display where the terms are available before allowing them to use the product.[54] Courts would enforce these policies against primary users for the same reason that they enforce clickwrap agreements: Although the users most likely did not read the terms, they had the opportunity to do so and expressly agreed to the terms notwithstanding their failure to read.[55] However, the communications-capturing technologies described throughout this Note have thus far not required secondary users to affirmatively agree to the terms before permitting them to use the product. Implementing this scheme would likely create too much friction before use for casual users, which companies generally want to limit, and would also not be particularly helpful to secondary users, who would most likely not read the terms before clicking "I agree."[56]

Second, companies may rely on the reasoning in shrinkwrap cases, arguing that when primary users purchased and began using the

---

[50] *See, e.g.*, *Specht*, 306 F.3d at 32 ("[A] reference to the existence of license terms on a submerged screen is not sufficient to place consumers on inquiry or constructive notice of those terms.").

[51] *Nguyen*, 763 F.3d at 1177.

[52] *Specht*, 306 F.3d at 32.

[53] *See, e.g.*, Halzack, *supra* note 3 (describing how the Hello Barbie requires the push of a button before recording begins).

[54] *See supra* note 43 and accompanying text (describing how the Hello Barbie will likely require parental registration and consent before use).

[55] *See, e.g.*, Davidson & Assocs. v. Jung, 422 F.3d 630, 635, 639 (8th Cir. 2005) (enforcing an online agreement without hesitation where the user clicked "I agree").

[56] *See supra* note 26 and accompanying text (describing the tendency of users to not read privacy policies).

product, they agreed to the terms sight unseen.[57] Courts justify the enforcement of these shrinkwrap agreements where the users have the opportunity to read the terms after purchase and can return the product for a full refund within a reasonable period of time if they disagree with the terms.[58] The reasoning from the shrinkwrap cases, however, would only apply to primary users, who purchased the product, and not to secondary users.

As described above, communications-capturing technologies provide no notice to secondary users of the terms of their privacy policies. While secondary users may be put on notice that they are being recorded when using technologies that require users to push a button or do some other affirmative action,[59] the existence of a recording button does not suffice to put secondary users on inquiry notice of the terms or data use practices described in privacy policies.[60] Based on existing clickwrap, browsewrap, and shrinkwrap precedent governing terms of use agreements, I conclude that privacy policies will be unenforceable against secondary users.

This conclusion both benefits and harms secondary users. It benefits secondary users because they will not be considered consenting parties to privacy policies that permit expansive data collection and use, as most do. Secondary users will thus not, on this basis, be prevented from availing themselves of several statutory protections unavailable to consenting primary users.[61] However, secondary users will be unable to rely on contract-based protections arising from privacy policy breaches. In order to weigh the impact of the lack of a contract between a secondary user and a communications-capturing technology company, we must consider the effectiveness of statutory protections available to secondary users who never consented to data acquisition. Part III sheds light on whether existing statutes could be used to protect secondary users, even if the statutes were not enacted with secondary users of communications-capturing technologies in mind.

---

[57] *See supra* note 44 and accompanying text; *see also* Florencia Marotta-Wurgler, *Are "Pay Now, Terms Later" Contracts Worse for Buyers? Evidence from Software License Agreements*, 38 J. LEGAL STUD. 309 (2009) (referring to these contracts as "pay now, terms later" agreements and finding that the terms within these agreements are no worse for consumers than the terms found in clickwrap agreements).

[58] *See, e.g.*, Davidson & Assocs., 422 F.3d at 635 ("If the user does not agree to these terms, the game may be returned for a full refund of the purchase price within thirty (30) days of the original purchase.").

[59] *See* Halzack, *supra* note 3 (describing the functionality of the Hello Barbie).

[60] *See* Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 32 (2d Cir. 2002) (explaining what suffices to put users on inquiry notice, and specifically stating that an unapparent hyperlink containing the terms somewhere on the website would not be sufficient).

[61] *See infra* Part III (describing state and federal statutory privacy protections).

III
Potential Statutory Protections for Secondary Users

A. State Eavesdropping Statutes

State eavesdropping statutes protect wire, electronic, or oral communications from being surreptitiously recorded.[62] These statutes can be divided into two categories: "all-party consent" statutes, in which all parties must consent before recording can take place, and "single-party consent" statutes, in which only one party to the communication must consent to the recording.[63] As discussed below, the distinction between all-party consent and single-party consent regimes will prove relevant given that secondary users never consent to the privacy policy's data collection and use terms in privacy policies.

In order to ground the discussion, this Section focuses only on two particular state statutes—one from an "all-party consent" state (Florida) and one from a "single-party consent" state (Delaware). These statutes share similar language with other states' all-party consent and single-party consent statutes, respectively, making them representative for purposes of analysis.[64] By comparing the all-party consent and single-party consent statutes, I hope to illustrate how protections for secondary users would differ between two types of state regimes.

1. All-Party Consent Statute: Florida

Florida's eavesdropping statute states the following: "Except as otherwise specifically provided in this chapter, any person who: (a) Intentionally intercepts . . . any wire, oral, or electronic communication . . . shall be punished . . . ."[65] In order to determine whether or not this statute could protect secondary users of communications-capturing technologies, we must ask the following questions: Are snippets of speech spoken to a consumer product—not to another person

---

[62] *See* Reporters Comm. for Freedom of the Press, Reporter's Recording Guide 2 (2012), http://www.rcfp.org/rcfp/orders/docs/RECORDING.pdf (providing an overview of state and federal recording statutes).

[63] *Id.*

[64] These statutes were chosen for their clarity, though their structure and content are representative of other state recording statutes. *Compare, e.g.*, 720 Ill. Comp. Stat. Ann. 5/14-2 (Supp. 2015) (providing an example of an all-party consent statute similar to the one used in Florida), *with* Minn. Stat. Ann. § 626A.02 (West 2009 & Supp. 2015) (providing an example of a single-party consent statute similar to the one used in Delaware). For a complete list of which states adhere to single- and all-party consent exceptions for communications interceptions, see Reporters Comm. for Freedom of the Press, *supra* note 62, at 3.

[65] Fla. Stat. Ann. § 934.03 (West 2001 & Supp. 2015).

in conversation—the type of "oral" or "electronic communication" that is covered under the statute? Does the company "intercept" this communication when it records secondary user communications?

The statute defines "oral communication" as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."[66] Florida's statute, like many other statutes, does not refer to a "conversation" and thus does not appear to preclude human-to-machine snippets of speech.[67] But do secondary users exhibit an expectation that such communications are not subject to interception? Where the communications-capturing technology requires an affirmative action like the push of a button before recording user communications, courts may find that the secondary user had an expectation that the communication was subject to interception, and therefore the communications would not qualify as "oral communication[s]" under the statute.[68] Thus, user interactions with communications-capturing technologies may not qualify as the type of oral communications protected under state eavesdropping statutes.

Even if these snippets of speech did not qualify as oral communications, they might alternatively qualify as electronic communications protected under the eavesdropping statute. The statute defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or

---

[66] FLA. STAT. ANN. § 934.02(2) (West 2001 & Supp. 2015).

[67] *But see, e.g.*, ALASKA STAT. § 42.20.310 (2014) (using the language of "conversation" instead of "communication").

[68] *See* RESTATEMENT (SECOND) OF CONTRACTS § 19 cmt. a (1981) ("Words are not the only medium of expression. Conduct may often convey as clearly as words a promise or an assent to a proposed promise."). However, in a recent case, even Chief Justice Roberts and Justice Scalia acknowledged that users may be confused about the ramifications of button pushing with new technologies. During oral arguments in *City of Ontario v. Quon*, 1560 U.S. 746 (2010), Chief Justice Roberts admitted confusion surrounding the routing of text messages through service providers, saying "I thought, you know, you push a button; it goes right to the other [cell phone]." Transcript of Oral Argument at 49, City of Ontario v. Quon, 560 U.S. 746 (2010) (No. 08-1332). Justice Scalia responded, saying "[y]ou mean it doesn't go right to the other thing?" *Id.* The open question is not whether users reasonably expect they are being recorded when they use communications-capturing technologies, as recording is inextricably linked with the voice-recognition service these products provide, but whether users reasonably expect that their recordings are being transmitted to a third party or other centralized source. The language of several state recording statutes suggests that the mere push of a button would not be sufficient to trigger a reasonable expectation of recording, though the statutes were written well before the existence of communications-capturing technologies. *See, e.g.*, CONN. GEN. STAT. ANN. § 52-570(d) (West 2013) (stating that recording is only permissible when preceded by verbal or written consent, verbal notification, or a specific type of "automatic tone warning" requiring a distinct signal repeated at intervals of approximately fifteen seconds during use).

photooptical system that affects intrastate, interstate, or foreign commerce."[69] Communications recorded by a communications-capturing technology qualify under this definition of "electronic communication" since the data, traveling over wireless signals, would be transmitted in part by radio.[70]

We must then ask whether these oral or electronic communications have been "intercepted" by the company producing the communications-capturing technology. The statute defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[71] Communications-capturing technologies neatly fit the definition of "electronic, mechanical, or other device" which acquires the contents of electronic or oral communications, so I would also conclude that the producers of communications-capturing technologies "intercept" secondary user communications as defined under the statute.[72] However, two exceptions to the prohibition on intercepting communications may apply: the all-party consent exception and what I refer to as the "normal course of business" exception. If either of these exceptions apply, then secondary users would no longer have a cause of action under the statute.

The all-party consent exception permits interception "when all of the parties to the communication have given prior consent to such interception."[73] As stated in Part II, secondary users do not appear to consent to expansive data use clauses stated in privacy policies, especially when secondary users were never afforded an opportunity to read the terms. However, the language of the statute refers to consent in the context of the "interception."[74] Courts might infer consent to the initial *interception* solely from the secondary user's use of the product even where the secondary user did not consent to all of the terms of the privacy policy. Companies that require the push of a button before recording, such as the Samsung SmartTV or Hello

---

69 FLA. STAT. ANN. § 934.02(12).

70 *Cf.* Joffe v. Google, Inc., 746 F.3d 920, 927–30 (9th Cir. 2013) (interpreting the Wiretap Act's definition of "radio communication" to exclude data transmitted over Wi-Fi, but recognizing that the Wiretap Act's definition of "electronic communication" would include any communication by radio waves, thus including Wi-Fi).

71 FLA. STAT. ANN. § 934.02(3).

72 *See, e.g.*, United States v. Szymuszkiewicz, 622 F.3d 701, 706–07 (7th Cir. 2010) (describing the expansive approach to defining "electronic, mechanical, or other device[s]" adopted by the Seventh Circuit). *But see* Bruce E. Boyden, *Can a Computer Intercept Your Email?*, 34 CARDOZO L. REV. 669, 689 (2012) (arguing that the Wiretap Act, as part of the Electronic Communications Privacy Act, would not interpret "interception" to include machine-based collection and acquisition of communications).

73 FLA. STAT. ANN. § 934.03(2)(d).

74 *Id.*

Barbie, would argue that secondary users consent to the *interception* when they push the recording button, even if they do not consent to all of the terms of the privacy policies, and therefore they have consented for the purpose of the eavesdropping statute.[75] If this exception applies as described, then secondary users would not have access to the statutory remedies available under all-party consent state regimes.

The second relevant exception found in the statute reads as follows:

> It is lawful under §§ 934.03-934.09 for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his or her employment while engaged in any activity which is a necessary incident to the rendition of his or her service . . . .[76]

Interestingly, this statute refers to companies as an "electronic communication service," as opposed to other statutes that limit this exception to common carriers.[77] This statute defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications," which seems to include providers of communications-capturing technologies. However, the term is elsewhere defined at the federal level,[78] and has been interpreted by several courts not to include companies like the producers of communications-capturing technologies, which merely utilize electronic communications services to receive and transmit data.[79] These courts suggest that the term only applies to

---

[75] *Cf.* RESTATEMENT (SECOND) OF CONTRACTS § 19 cmt. a (1981) (describing the effectiveness of non-verbal conduct as a form of assent).

[76] FLA. STAT. ANN. § 934.03(2)(a)(1).

[77] *See, e.g.*, LA. REV. STAT. ANN. § 15:1303(C)(1) (2015) (creating an exception for officers, employees, or agents of communications common carriers acting in the normal course of employment); TEX. PENAL CODE ANN. § 16.02(c)(1) (West 2011 & Supp. 2015) (same).

[78] 18 U.S.C. § 2510(15) (2012) (defining "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications").

[79] *See, e.g.*, *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 307 (E.D.N.Y. 2005) (concluding that while the Electronic Communications Privacy Act defines "electronic communication services" as "any service which provides to users thereof the ability to send or receive wire or electronic communications," 18 U.S.C. § 2510(15), and thus might appear to cover JetBlue, the text instead refers to direct providers of electronic communication services, like ISPs, and not companies like JetBlue that simply consume these services in order to receive and transmit data to and from its customers). *But see* United States v. Mullins, 992 F.2d 1472, 1474, 1478 (9th Cir. 1993), *cert. denied,* 510 U.S. 994 (1993) (finding American Airlines, through its computerized reservation system, which enables travel agents to gather flight information and directly input travel reservations, to be "a provider of wire or electronic communication service").

companies like internet service providers, which directly provide electronic communications services to consumers.[80] Under this interpretation, the state definition also may be much narrower than it appears on its face. Whether this exception applies, and thus whether secondary users can bring a cause of action under the statute, will in part depend on whether state courts adopt a definition of "electronic communication service" that only applies to direct communication service providers or an interpretation more closely based on the definitions directly provided by the state legislature which would include providers of communications-capturing technologies.

If companies successfully argue that they are "electronic communication services" under the statute in order to qualify for the exception, they would also need to argue that the recording of secondary user data is a "necessary incident to the rendition of his or her service."[81] Here, companies would argue that the "service" being rendered is the provision of consumer products which feature speech- and voice-recognition technology, and the capturing of secondary-user communications is necessarily incidental to improving that service.[82] If successful, the argument that collecting secondary user communications is necessary to improve voice-recognition services would again prevent secondary users from enjoying any statutory protections available under all-party consent state regimes, even where the data collection and use is far beyond what secondary users expected upon pushing a button.

2. Single-Party Consent Statute: Delaware

The Delaware eavesdropping statute similarly prohibits the intentional interception of any wire, oral, or electronic communication.[83] "Oral communications" as defined by the Delaware statute face the same problem as in the Florida statute: Companies may argue that secondary users expect their communications to be subject to interception solely through use of products featuring voice recognition, thus removing any claims by secondary users that their "oral communications" are protected under the statute.[84] The statute defines "electronic communication" as "any transfer of signs, signals, writing,

---

[80] *E.g.*, *In re* JetBlue Airways Corp., 379 F. Supp. 2d at 307.

[81] FLA. STAT. ANN. § 934.03(2)(a)(1).

[82] *See, e.g.*, *Samsung Privacy Policy—SmartTV Supplement*, *supra* note 2 ("To provide you the Voice Recognition feature, some interactive voice commands may be transmitted (along with information about your device, including device identifiers) . . . to the extent necessary to provide the Voice Recognition features to you.").

[83] DEL. CODE ANN. tit. 11 § 2402(a)(1) (2015).

[84] *Id.* § 2401(13).

images, sounds, data or intelligence of any electromagnetic, photoelectronic or photooptical system."[85] Secondary-user communications are transferred through an electromagnetic system—specifically, through Wi-Fi—and would thus arguably be protected under the statute as "electronic communications."[86]

But does the protection of these electronic communications survive Delaware's single-party consent exception? Delaware's consent exception applies where only one party consents, and reads as follows: "It is lawful . . . [f]or a person to intercept a wire, oral or electronic communication where the person is a party to the communication or where one of the parties to the communication has given prior consent to the interception . . . ."[87] Companies facing suits in single-party consent states would argue that because the company itself consented to the recording as "a party to the communication,"[88] the recording is lawful under the statute, even though secondary users never consented.[89] If successful, this application of the consent exception would remove any protections afforded to communications-capturing technology users under state eavesdropping statutes in single-party consent regimes.

As shown, back-end protections under state eavesdropping laws likely do not cover secondary users based on either the plain language, which may not cover secondary user communications to communications-capturing technologies, or the statutory exceptions. Given the lack of contract-based protections under privacy policies and the lack of statutory back-end protections under state eavesdropping statutes, secondary users must instead look to federal privacy statutes for protection.

B. Federal Protection: Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA) similarly prohibits persons from "intentionally intercept[ing] . . . any wire, oral,

---

[85] *Id.* § 2401(5).

[86] *Cf.* Symbol Tech., Inc. v. Janam Tech. LLC, 729 F. Supp. 2d 646, 656 (D. Del. 2010) (referring to a Wi-Fi transceiver as an "electromagnetic transceiver").

[87] DEL. CODE ANN. tit. 11 § 2402(c)(4).

[88] *Id.*

[89] *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 510–12 (S.D.N.Y. 2001) (finding that websites could "consent" as parties to a communication, thus removing the interception of user communications by DoubleClick from the protections of the Electronic Communications Privacy Act); *see also In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *7 (N.D. Cal. Oct. 9, 2001) (finding that a third party company's collection of consumer data did not violate the Electronic Communications Privacy Act because Toys R Us consented to the interception of electronic communications as one of the parties to the communication).

or electronic communication" unless either the person intercepting the communication is also a party to the communication or one party to the communication consented prior to the recording.[90] Federal case law supports an interpretation of the Act that would include communications-capturing technologies as capable of "intercept[ing]" "wire, oral, or electronic communication[s]" under the plain text of the statute.[91] However, for the same reasons stated above with respect to state eavesdropping statutes, secondary users will not be able to prevail under this statute where communications-capturing technology producers successfully argue that (a) they are a party to the communication or (b) secondary users consented to the interception prior to the recording, thus removing them from the purview of the statute. The latter argument depends on courts accepting the premise that a secondary user can consent to the initial interception, without having received notice of all of the data collection and use terms described in the privacy policy. If this argument succeeds, then secondary users would not be protected under § 2511 of the Electronic Communications Privacy Act.

However, the Electronic Communications Privacy Act does much more than simply create a federal floor below which state eavesdropping statutes may not fall. The Act also prohibits divulging stored communications without consent.[92] Specifically, the Act states: "[A] person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service . . . ."[93] The first question we must consider is whether communications-capturing technology companies qualify as "electronic communication services." While communications-capturing technologies appear to fit within the plain meaning of electronic communication services as defined in the statute,[94] the term has been interpreted by several federal courts which arrived at different conclusions. In *In re JetBlue Airways Corp. Privacy Litigation*, the court held that the airline was

[90] 18 U.S.C. § 2511(1)(a), (2)(d) (2012).

[91] *See, e.g.*, United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992) (declaring that an interception occurs "when the contents of a wire communication are captured or redirected in any way," thus eliminating the argument that human listening is required in order to intercept); United States v. Turk, 526 F.2d 654, 658 n.2 (5th Cir. 1976) (concluding that the aural acquisition occurs when a recording is made, with the recorder serving as "the agent of the ear").

[92] 18 U.S.C. § 2702(a)(1), (2) (2012).

[93] 18 U.S.C. § 2702(a)(1).

[94] ECPA defines "electronic communication services" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (2012).

not an electronic communication service under the statute because it did not directly provide users the ability to send or receive wire or electronic communications.[95] However, more than a decade earlier, the Ninth Circuit in *United States v. Mullins* held that American Airlines was a provider of "wire or electronic communication service[s]" through its computerized reservation system.[96] Given the conflicting interpretations of the statute, it is not unreasonable to consider the possibility that communications-capturing technology producers could be considered "electronic communication services" under the statute.

One question not yet considered by the federal courts in interpreting ECPA is whether secondary users qualify as "users" under the statute at all. The statute defines "user" as any person or entity who (A) uses an electronic communication service, and (B) is duly authorized by the provider of such service to engage in such use.[97] Especially where communications-capturing technologies have the ability to distinguish between users based on voice commands and still permit use by individuals other than the primary user,[98] it would be difficult for communications-capturing technology producers to argue that secondary users are not "duly authorized" to engage in use of the service.[99] Given the ease with which companies could distinguish between users either through voice recognition or other simple authentication methods, I argue that secondary users qualify as "duly authorized" users under the statute.

Though communications-capturing technologies appear to meet the definition of "electronic communication services" and secondary users appear to be "duly authorized" users, two statutory exceptions under § 2702 may apply to disclosures by communications-capturing technology producers, thus eliminating federal statutory protection

---

[95] *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 307 (E.D.N.Y. 2005) ("JetBlue is more appropriately characterized as a provider of air travel services and a consumer of electronic communication services."). This holding must be considered in light of the fact that the court was reconciling an expansive federal scheme for regulating airlines with a federal privacy statute which did not seem to specifically cover airlines.

[96] United States v. Mullins, 992 F.2d 1472, 1474, 1478 (9th Cir. 1993), *cert. denied*, 510 U.S. 994 (1993).

[97] 18 U.S.C. § 2510(13) (2012).

[98] *See, e.g.*, Matt Warman, *Say Goodbye to the Pin: Voice Recognition Takes Over at Barclays Wealth*, THE TELEGRAPH (May 8, 2013), http://www.telegraph.co.uk/technology/news/10044493/Say-goodbye-to-the-pin-voice-recognition-takes-over-at-Barclays-Wealth.html (describing Barclays's adoption of Nuance technology to identify and authenticate users on the phone).

[99] Of course, communications-capturing technology producers and sellers may include a clause in their terms of use or privacy policies attempting to forbid secondary users from using the product in order to disqualify them as "duly authorized" users. However, current privacy policies accompanying communications-capturing technologies do not make this attempt.

for secondary users under ECPA. First, ECPA creates an exception based on either "originator" or "intended recipient" consent.[100] As long as communications-capturing technology producers can argue that they were the intended recipient of the communication, as would be the case with both the Samsung SmartTV and the Hello Barbie doll, secondary users would no longer be able to make claims against the producer.[101] This would hold true even where secondary users did not consent to the collection or disclosure of their communications.

The second relevant exception under § 2702 states that "[a] provider described in subsection (a) may divulge the contents of a communication . . . as may be necessarily incident to the rendition of the service . . . ."[102] As described above with respect to state eavesdropping statutes, communications-capturing technology producers will likely argue that secondary user data collection is "necessarily incident" to the rendition of both voice-recognition and personalization services provided by the company.[103] If this argument succeeds, then secondary users would not be able to bring suit against communications-capturing technology producers under § 2702.

IV
Designing Privacy Protections for Secondary Users

Part II and Part III provide evidence that secondary users lack protection under the current legal regimes for protecting user privacy. Part IV considers particular privacy harms that might result from that lack of protection and proposes a framework for designing secondary user protections that balances innovation and utility of communications-capturing technologies with prevention of unwanted data collection and use.

As described above, secondary users lack both front-end protection, in the form of notice-and-choice,[104] and back-end protection, in

---

100 18 U.S.C. § 2702(b)(3) (2012).

101 *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 510, 513–14 (S.D.N.Y. 2001) (dismissing claims against DoubleClick because their actions fell under the consent exceptions of the Stored Communications Act and Wiretap Act); Yunker v. Pandora Media, Inc., No. 11-CV-03113 JSW, 2013 WL 1282980, at *9 n.6 (N.D. Cal. Mar. 26, 2013) (explaining that plaintiff may have pleaded himself out of a Stored Communications Act claim by alleging that Pandora was the intended recipient of plaintiff's personally identifiable information, since intended recipients can consent to third party disclosure under the Stored Communications Act without originator consent).

102 18 U.S.C. § 2702(b)(5).

103 *See supra* note 82 and accompanying text (describing Samsung's privacy policy, which notes that it will capture voice data to the extent necessary to provide voice-recognition services).

104 *Supra* Part II.

the form of a civil cause of action or other means of changing a company's data collection and use policies.[105] The system I propose for secondary users removes any attempt to provide secondary users with notice-and-choice, recognizing that to do so would impose unreasonable costs on the company and friction in the user experience without providing any meaningful benefit to secondary users. Instead, I argue for back-end protection that distinguishes between primary and secondary users, providing secondary users with stronger protections than primary users based on the notion that they never consented to the expansive data collection and use terms in privacy policies.

The most cumbersome system design would require upfront notice-and-choice for secondary users every time a new secondary user attempts to use the product, even though they did not purchase the product. Before explaining why requiring upfront notice would not be the ideal outcome for both sellers and secondary users, I will lay out the best case for notice-and-choice in these products. Consider, for example, the Hello Barbie product described above. If Mattel authenticates the primary user through voice recognition—a simple process already used in high-security financial settings[106]—then they would be able to identify secondary users and provide those users with notice and an opportunity to consent to the privacy policy. Note, however, that because the Hello Barbie and other communications-capturing consumer products like it do not have a visual display, the user will not have a simple means of viewing the privacy policy. Mattel could require the user to go to a website, read and consent to the privacy policy, and then provide a voice baseline with which to later authenticate the secondary user when using the product. This notice-and-choice scheme creates an absurd requirement in the fast-paced environs in which these products will be used.[107]

---

[105] *Supra* Part III.

[106] *See* Penny Crosman, *U.S. Bank Pushes Voice Biometrics to Replace Clunky Passwords*, AM. BANKER (Feb. 13, 2014), http://www.americanbanker.com/issues/179_31/us-bank-pushes-voice-biometrics-to-replace-clunky-passwords-1065608-1.html ("When U.S. Bank announced Wednesday that it's testing voice biometrics for possible use by customers to access account information, it joined a line of banks that have been testing this technology, including Wells Fargo (WF) and Barclays.").

[107] Note that Mattel's Hello Barbie, as well as other communications-capturing technologies that collect communications from children under the age of thirteen, may be subject to the Children's Online Privacy Protection Act (COPPA). *See* 5 U.S.C. §§ 6501–6505 (2012); 16 C.F.R. § 312 (2015). COPPA requires operators of online services that collect data from children under the age of thirteen to present notice of the privacy practices on the website or online service in the same place that the childrens' data is collected. 16 C.F.R. § 312.4(d) (2015). This may pose particular problems for

Moreover, disclosure as described above will not provide meaningful benefits to secondary users. Upfront disclosure works best where there is a simple means to communicate the terms, like on the back of a ticket,[108] or through a prominent hyperlink on the website,[109] or in the context of a subtle nudge to the user requiring little reading.[110] But with communications-capturing technologies, there may be no direct connection to an easily-accessible website during use, and requiring notice to be posted or stated by the product itself every time a secondary user uses the product would create unreasonable transaction costs. Beyond the fact that presenting notice will create significant difficulties for products without visual displays, several authors suggest that upfront disclosure of privacy practices does not increase privacy policy readership, and thus does not have a meaningful impact on user choice.[111] Given that the implementation of a notice-and-choice scheme would be unreasonably inefficient and ineffective, I conclude that communications-capturing technologies should not be mandated to provide notice-and-choice to secondary users before use. The case proves different for primary users, who may be more easily directed to an application or to the terms directly before initial use of the product.[112] While primary users may still initially choose not to read the terms,[113] the one-time transaction costs would

communications-capturing technologies that lack displays and are potentially covered by COPPA, such as the Hello Barbie.

108 *See, e.g.*, Carnival Cruise Lines, Inc. v. Shute, 499 U.S. 585 (1991) (holding a forum selection clause enforceable even though it appeared in a standard form contract appended to a cruise ticket).

109 *See supra* note 43 and accompanying text (describing Hello Barbie's likely sign-up process).

110 *See* Wang et al., *supra* note 30 (describing privacy "nudges" in the disclosure context).

111 *See, e.g.*, Omri Ben-Shahar & Carl Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647 (2011) (explaining why mandatory disclosure regimes not only fail their stated goal of increasing awareness of contract terms, but also unintentionally harm consumers by creating a situation in which a contract that they did not read will be more likely to be enforced against them due to the initial disclosure); Marotta-Wurgler, *supra* note 6 (finding that mandatory disclosure does not significantly increase readership of online contracts). *But see* Calo, *supra* note 30, at 1036–37 (suggesting that unwritten forms of disclosure may be more effective at communicating privacy practices to consumers); Robert A. Hillman & Maureen O'Rourke, *Defending Disclosure in Software Licensing*, 78 U. CHI. L. REV. 95 (2011) (suggesting that disclosure may be justified in terms of economic efficiency, among other normative grounds).

112 *See supra* note 43 and accompanying text (describing how ToyTalk and Mattel will likely require parents (as primary users) to download an app and affirmatively consent to their and their children's data collection before enabling the voice-recognition software on the doll).

113 *See* Marotta-Wurgler, *supra* note 6, at 173–77 (measuring reading rates for end user license agreements).

likely prove low enough to support the practice for those primary users who would benefit from front-end notice.

In terms of back-end protection, I propose an approach in which companies are legally required to treat primary and secondary user communications differently. If we assume, as suggested in Part III, that secondary users at best consent to the *interception* of their data for voice recognition purposes, but not to any more expansive data use practices described in a privacy policy, then companies should be required to treat secondary user communications differently on the back end based on this lack of consent, providing secondary users much stronger protection than currently provided.

What would this back-end protection look like? It could look like shorter data retention periods for secondary user data, a ban on sale and disclosure to third parties, and anonymization techniques currently implemented by several companies that collect voice data.[114] All of these practices would allow companies to collect the data without upfront notice and consent while protecting secondary user data through heightened back-end treatment.

The back-end approach suggested above requires that companies be able to distinguish between primary and secondary users at some stage of the data collection process. While complying with the proposed legal requirement would prove much easier for those companies already utilizing voice-recognition software,[115] we can also design additional legal requirements to incentivize companies who have yet to adopt the necessary technology to do so in order to distinguish between primary and secondary users. For example, companies that use voice-recognition technology and are thus able to distinguish between primary and secondary user communications can use primary user communications in accordance with the terms of their privacy policy, but would still need to treat secondary user communications according to the use restrictions described above. Companies that are *unable* to distinguish between primary and secondary user communications would be required to treat *all* communications according to the restrictions on secondary user communications. This legal requirement would serve as a strong incentive to adopt technologies, such as voice-recognition technology, that facilitate the ability to distinguish

[114] *See* Matyszczyk, *supra* note 2 ("[F]or example, Google creates random identifiers to block its servers from knowing that it's you making the voice request."). I acknowledge that this process would be different where attempting to collect data about one subgroup while anonymizing the other subgroup, but cite Google's method as one anonymization method currently used by a communications-capturing technology.

[115] *See* Crosman, *supra* note 106 and accompanying text (describing adoption of voice recognition technologies across sectors, including the financial sector).

between primary and secondary users, thus increasing the likelihood that the bifurcated approach to primary and secondary user data will be effective. Under this proposed reform, the very voice-recognition technology that captures secondary user communications and creates the privacy issues discussed in this Note could be used to protect secondary users on the back end by filtering their communications and treating them differently from primary user communications.

Some may argue that the costs of implementing voice recognition technology will be too high, and that those costs will be inevitably passed on to consumers. Similarly, if critics view the harms to secondary users caused by communications-capturing technologies as insignificant, then critics may also argue that the costs to consumers outweigh the benefits to secondary users. This argument does not fully consider the argument that companies will also experience economic benefit from the introduction of voice recognition technology into communications-capturing technologies. Products utilizing voice recognition can improve targeted advertisements to primary users, providing an improved source of revenue for the company, and can also improve the individualized content and recommendations provided to the primary users, a benefit for which primary users would arguably pay a premium. While there are no doubt costs associated with developing and implementing voice recognition technology, many of the features of communications-capturing technologies dramatically improve with the implementation of voice recognition.

Critics may also argue that the addition of voice-recognition technology would be net privacy-diminishing, as it would enable companies to identify specific secondary users and connect them with their communications. This is not necessarily the case. While this proposal does call for the adoption of voice-recognition technology to distinguish the primary user from secondary users, the proposal does not mandate (or even invite) companies to require secondary users to *identify* themselves in order to use communications-capturing technologies. Instead, this proposal only incentivizes companies to incorporate voice recognition technology sufficient to distinguish between the voice of the primary user and secondary users without identifying individual secondary users.

Finally, my goal is not to impose burdensome notice requirements on sellers engaging in mass consumer transactions where communications-capturing technologies could be used by secondary users. Nor is my goal to stymie these innovative products, which can benefit primary users by providing more personalized user experiences. Instead, I hope to reorient the privacy discourse in an age where individuals can purchase communications-capturing technolo-

gies that affect the privacy of more than just themselves, and incentivize companies to design these technologies with secondary users in mind.

Conclusion

As the world of communications-capturing technologies grows, privacy concerns for secondary users will grow as well. This Note demonstrates that secondary user privacy protections lag behind the development of innovative communications-capturing technologies. Because secondary users are not protected by privacy policies, secondary users lack meaningful front-end protections provided by notice-and-choice. Also, because secondary users arguably consent to the *interception* of their data by using these products or because of other statutory exceptions, they may not be able to bring claims under state and federal privacy statutes. This creates a significant problem: Secondary users, who never consented to expansive data use policies, will have their data collected and treated in the same way as primary users despite being in very different positions—and lacking similar protections—than primary users. In designing secondary user protection, companies and regulators should consider ways to preserve the utility of these technologies while protecting secondary users from expansive data use practices that they never agreed to under privacy policies. My proposed approach will encourage the adoption of innovative voice-recognition technologies and communications-capturing technologies more broadly while protecting secondary user communications.