Reassessing Wiretap and Eavesdropping Statutes: Making One-Party Consent the Default

*Rauvin Johl**

Introduction

The rise of smartphones, smart technology, and the internet of things has pushed society incrementally closer to the camera-laden dystopia described in George Orwell's *1984*. But rather than a surveillance network orchestrated by Big Brother, today's recordings are made by private citizens as well as the government. Smartphones have the capability to record audio and video, as do wearable devices such as GoPros and home security technologies including smart doorbells, dashboard cameras, and nanny cams. These devices have placed immense power in the hands of the public, allowing us to record and share everyday miracles, nuisances, and tragedies. As technology evolves and audiovisual recording devices become smaller, more affordable, and ubiquitous, state laws regulating the use of these devices often remain unchanged. Most states have eavesdropping and wiretapping statutes that impose one-party consent regimes, allowing the recording of audio if one party to the communication consents. But a significant minority of states have all-party consent laws, which prohibit audio recordings without the consent of all parties to a communication.[1] All-party consent statutes have led to high-profile arrests of citizens who record police officers in the performance of their duties, and cast a pall on the use of other technologies such as 'smart' home security devices and dashboard cameras.[2]

States with all-party consent recording statutes should replace those laws with one-party schemes. All-party consent laws were intended to protect privacy and preserve social bonds, but their expansive scope made little sense even in the era in which they were drafted. Changes in social attitudes, technology, and policing tactics have deepened the inconsistencies embedded in all-party consent laws. Prohibitions on audio recording without all-

* Harvard Law School, J.D. 2017. I am grateful to Professor Susan Crawford for her advice regarding this article. I would also like to thank the dedicated *Harvard Law & Policy Review* editors for their insightful editing and comments.

[1] All-party consent laws are also commonly referred to as two-party consent laws. For the purposes of this paper, I will be using the term "all-party consent" in recognition of the fact that in all-party and two-party schemes consent must be obtained from all parties to a recording for it to be lawful.

[2] *See* Annys Shin, *Traffic stop video on YouTube sparks debate on police use of Md. wiretap laws*, Wash. Post (June 16, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/06/15/AR2010061505556.html [https://perma.cc/NS85-HB7G]; *ACLU-PA Files Lawsuit on Behalf of Armstrong County Resident Arrested and Jailed for Videotaping Police*, ACLU-PA (May 3, 2016), https://www.aclupa.org/news/2016/05/03/aclu-pa-files-lawsuit-behalf-armstrong-county-resident-arres [https://perma.cc/S6E4-XED9].

party consent criminalize socially beneficial behavior in a manner that undermines the rationale behind the statutes. Moving towards a one-party system would end the chilling effect of all-party consent schemes. Lingering privacy concerns can be addressed by supplementing one-party schemes with privacy protection laws combating malicious surveillance. Moreover, if states are unwilling to shift to a purely one-party system, a split consent scheme with higher burdens placed on government and law enforcement officials can help alleviate the undesirable outcomes associated with all-party consent. Both suggestions for reform require action from state legislatures on a state-by-state basis, which can be difficult and time-consuming. However, attitudes towards privacy, recordings, and technology have shifted such that challenges to all-party consent statutes will likely continue. Rather than allowing all-party consent schemes to be altered by state judiciaries on a piecemeal basis, state legislators should strongly consider proactive reform measures.

I. Overview of Federal and State Wiretapping Statutes

A. Federal Regulation of Wiretapping

Wiretapping generally refers to "electronic or mechanical eavesdropping . . . done by law-enforcement officers under court order, to listen to private conversations."[3] The practice of wiretapping began soon after the telephone was invented and quickly became a widespread policing technique.[4] In the early days of wiretapping, it was conducted with limited judicial oversight.[5] Law enforcement officers did not seek warrants or attempt to establish probable cause before engaging in surveillance. In *Olmstead v. United States*,[6] the Supreme Court considered the Fourth Amendment implications of wiretapping for the first time, including whether the practice should be subject to warrant requirements.[7] The Court held that evidence secured by the "use of the sense of hearing" was neither a search nor a seizure as contemplated by the Fourth Amendment because it did not involve a search of material items or personal property.[8] It could therefore be conducted without a warrant.[9] Justice Brandeis dissented, arguing strongly in favor of warrant requirements on the grounds that "[c]lauses guaranteeing to the individual protection against specific abuses of power, must have a

---

[3] *Wiretapping*, Black's Law Dictionary (10th ed. 2014).

[4] *See* Anita L. Allen & Marc Rotenberg, Privacy Law and Society 1101 (3rd ed. 2015).

[5] *See id.*

[6] 277 U.S. 438 (1928).

[7] *See id.* at 455.

[8] *Id.* at 463–64 (construing the Fourth Amendment narrowly as a protection against "the use of governmental force to search a man's house, his person, his papers, and his effects, and to prevent their seizure against his will" such that when there was no entry into defendants' home or offices "[t]here was no searching. There was no seizure.").

[9] *See id.*

similar capacity of adaptation to a changing world" and that "[t]he progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping."[10] Six years after *Olmstead*, Congress agreed with Justice Brandeis and passed the Federal Communications Act of 1934, which included the first federal regulation of wiretapping.[11] The law did not impose a warrant requirement but did restrict the production of information obtained by wiretap as evidence in court.[12] This weak limitation did little to curb warrantless wiretapping, which continued to be commonplace.[13]

In 1967, the Supreme Court recognized the erosion of the property-focused conception of the Fourth Amendment, overruled *Olmstead,* and changed course. It held that wiretapping constituted a search and seizure within the meaning of the Fourth Amendment.[14] Though wiretapping did not involve a physical incursion, the results of the practice were such an intrusion on privacy and the "right to be let alone" that they raised constitutional concerns.[15] The Court further held that wiretapping by the government without a warrant violated the Fourth Amendment.[16]

Congress outlined the modern warrant requirements for wiretapping and electronic surveillance in detail a year later in the Omnibus Crime Control and Safe Streets Act of 1968.[17] Title III of the Act restricted the use of wiretaps more than prior legislation or judicial precedent. Title III protects individuals from intentional interception of wire, oral, or electronic communication by *any* person, regulating the use of surveillance technology by private citizens as well as law enforcement.[18] Private individuals can record wire, oral, or electronic communications if one of the parties consents.[19] Warrants can legitimize interceptions by law enforcement.[20] However, Title III requires law enforcement to meet several requirements before obtaining a warrant, including demonstrating that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if

---

[10] *Id.* at 472, 474 (Brandeis, J., dissenting).

[11] *See* F. Lee Bailey & Kenneth J. Fishman, Handling Narcotic and Drug Cases § 153 (2017); *see also* Communications Act of 1934, Pub. L. No. 73-416, § 605, 48 Stat. 1064, 1103–04.

[12] *See id.*

[13] *See* Paul M. Schwartz & Daniel J. Solove, Privacy Law Fundamentals 83 (1st ed. 2006).

[14] Katz v. United States, 389 U.S. 347, 353 (1967).

[15] *Id.* at 350.

[16] *See id.* at 358–59.

[17] *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended in scattered sections of 5, 18, 28, 34, 42, 47 U.S.C.).

[18] *See* 18 U.S.C § 2511 (2012) (emphasis added). The law does not address video surveillance and also contains several exceptions. Parents can vicariously consent to an interception on the behalf of minor children. *See* Newcomb v. Ingle, 944 F.2d 1534, 1535 (10th Cir. 1991). Note that this exception is limited; for example, it cannot be applied to spouses. *See* United States v. Jones, 542 F.2d 661, 670 (6th Cir. 1976). Switchboard operators can intercept communications without consent in certain circumstances as can telecommunications company employees under court orders, and persons acting under color of law with the consent of one party. *See* 18 U.S.C. § 2511 (2012).

[19] *See* 18 U.S.C. § 2511 (2012).

[20] *See* 18 U.S.C. § 2516 (2012 & Supp. III 2015).

tried or to be too dangerous."[21] If an interception occurs, and it does not satisfy any of the statutory exceptions[22] and was not conducted pursuant to a court order, the aggrieved party may be eligible for civil remedies, and the interceptor may face criminal sanctions. Title III, hereinafter referred to as the Federal Wiretap Act, has undergone numerous revisions since its original passage—including revisions under the Electronic Communication Privacy Act of 1986[23] and the Communications Assistance for Law Enforcement Act of 1994[24]—but it remains the centerpiece of federal wiretapping law.

B. State Regulation of Wiretapping

With the exception of Vermont, every state has a wiretap and surveillance statute.[25] Thirty-eight states (and the District of Columbia) have one-party consent regimes, just like the federal statute.[26] Eleven states have all-party consent schemes.[27] Unlike one-party systems, an all-party consent regime requires individuals who are recording a communication to have the consent of every party involved. If a recording or interception is made across state lines between a one-party state and an all-party state, the law of the all-party state controls.[28]

All-party consent laws vary in their scope. Some all-party consent states make it illegal to covertly record another individual or individuals. For example, Montana requires that all parties be aware that a recording is being made,[29] and Massachusetts outlaws secret recordings.[30] Other states focus on expectations of privacy rather than secrecy. In those states, recordings must

---

[21] 18 U.S.C. § 2518 (2012).

[22] *See* 18 U.S.C. § 2511 (2012).

[23] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

[24] Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103–414, 108 Stat. 4279 (codified as amended in scattered sections of 18 U.S.C.).

[25] *See* PAUL M. SCHWARTZ & DANIEL J. SOLOVE, PRIVACY LAW FUNDAMENTALS 88 (2d ed. 2015). In this article, the phrase "wiretap and surveillance statute" refers to statutes imposing criminal and/or civil penalties for electronic or mechanical eavesdropping on oral, wire, and electronic communications, with particular attention paid to how laws regulate recordings by private individuals.

[26] *Id.*

[27] *Id.* (citing California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Montana, Nevada, New Hampshire, Pennsylvania, and Washington statutes and noting that Hawaii has a split system, with two-party consent in some circumstances).

[28] *See, e.g.*, Kearney v. Salomon Smith Barney, Inc., 137 P.3d 914, 937 (Cal. 2006).

[29] "Except as provided in 69-6-104, a person commits the offense of violating privacy in communications if the person knowingly or purposely . . . records or causes to be recorded a conversation by use of a hidden electronic or mechanical device that reproduces a human conversation without the knowledge of all parties to the conversation." MONT. CODE ANN. § 45-8-213 (2017) (held unconstitutional on other grounds by State v. Dugan, 303 P.3d 755 (Mont. 2013)).

[30] "Except as otherwise specifically provided in this section any person who willfully commits an interception, attempts to commit an interception, or procures any other person to commit an interception or to attempt to commit an interception of any wire or oral communication shall be fined not more than ten thousand dollars, or imprisoned in the state prison for not more than five years, or imprisoned in a jail or house of correction for not more than two

be made with the consent of all parties unless the parties do not have a reasonable expectation of privacy, in which case recordings are legal with or without all-party consent.[31] Illinois prohibits surreptitious recordings of private conversations and defines a private conversation as one for which there is an expectation of privacy, placing it in both categories.[32]

Though the types of all-party consent schemes overlap, in practice there are meaningful distinctions between the categories. In states in which secret recordings are prohibited, a conversation recorded between two individuals in a public park could run afoul of the statute, even though the recording is made in a public space without expectation of privacy. In states requiring consent unless there is no expectation of privacy, it is likely that a normal volume conversation recorded by one-party or by a non-party in a public park or hallway would not violate the statute, even if not all parties had knowledge of the recording.

II. Legislative Rationale for One-Party and All-Party Consent Laws

A. Rationale for One-Party Consent Laws

The thirty-eight states that have adopted a one-party consent approach to the regulation of eavesdropping and wiretapping have not articulated a single unifying rationale for their approach. Common rationales include arguments based on statutory interpretation, the low level of intrusiveness of one-party recordings, and the social utility of one-party recordings.

State wiretapping and eavesdropping statutes are, on a general level, laws regulating the interception of communication. Many one-party consent systems are predicated on the assumption that a person cannot intercept his or her own oral, wire, or electronic conversation since an interception re-

---

and one half years, or both so fined and given one such imprisonment." Mass Gen. Laws ch. 272, § 99 (2017). Interception is defined as to "secretly hear." *Id.*

[31] *See, e.g.*, Fla. Stat. Ann. § 934.02 (2017) (prohibiting the interception of wire, oral, and electronic communication and defining an 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* . . .") (emphasis added). Some states have read an expectation of privacy into wiretapping statutes even where such expectations are not expressly written. *See, e.g.*, Malpas v. State, 695 A.2d 588, 595 (Md. Ct. Spec. App. 1997); Fearnow v. Chesapeake & Potomac Tel. Co. of Md., 676 A.2d 65, 70 (Md. 1996).

[32] A person commits eavesdropping when he or she knowingly and intentionally:

> (1) Uses an eavesdropping device, in a surreptitious manner, for the purpose of overhearing, transmitting, or recording all or any part of any private conversation to which he or she is not a party unless he or she does so with the consent of all of the parties to the private conversation;
>
> (2) Uses an eavesdropping device, in a surreptitious manner, for the purpose of transmitting or recording all or any part of any private conversation to which he or she is a party unless he or she does so with the consent of all other parties to the private conversation . . . ."

720 Ill. Comp. Stat. Ann. 5/141–2 (2017) (held unconstitutional in part by People v. Melongo, 6 N.E.3d 120 (Ill. 2014)).

quires the involvement of a third-party.[33] Accordingly, recordings made by a party or with a party's consent should not qualify as eavesdropping or wiretapping. One-party consent laws also rely on the assumption that a recording of a conversation made by a party to the discussion is less intrusive than a recording made by a third-party. For example, parties to a conversation are permitted to testify regarding that conversation in court, so it seems counterintuitive to make a party's recording of that same conversation illegal or inadmissible, since the recording is likely more accurate than either party's recollection. Recordings made in anticipation of legal proceedings also have social utility. They can help convict perpetrators of violent crime,[34] expose workplace misdeeds,[35] and protect victims of abuse from retribution.[36]

The Federal Wiretap Act provides further insight into the decision between one-party and all-party consent statutes. Prior to the passage of the 1968 Omnibus Crime Control Act, the issue of one-party and all-party consent was subject to significant floor debate. Some senators were concerned that one-party consent "leaves wide open the problem of industrial espionage and many other abuses of the right to privacy."[37] They also recognized that the law should protect those who record conversations "out of a legitimate desire to protect himself and his own conversations from later distortions or other unlawful or injurious uses by the other party."[38] The decision to use a one-party consent framework represents a balancing of those two concerns and a recognition that an all-party consent system would sweep the actions of well-intentioned citizens into the prohibited categories.[39]

---

[33] *See* Billeci v. United States, 184 F.2d 394, 397 (D.C. Cir. 1950) ("We think that interception of a phone call necessarily involves the idea that a speaker thinks he is talking to one person whereas in fact a third person is listening.").

[34] *See* State v. Inciarrano, 473 So. 2d 1272, 1274 (Fla. 1985) (holding that a recording made by a murder victim of his own murder was admissible despite a two-party consent regime because the defendant had trespassed in the victim's office and therefore had no expectation of privacy); *see also* State v. Lissy, 747 P.2d 345, 350 (Or. 1987) (en banc) (discussing the rationale for Oregon's one-party consent statute, which included "the example of a police officer listening in on ransom calls in a kidnapping case as a reason why the one-party consent exception to the prohibition on listening to a telephone conversation was necessary").

[35] Michael M. Grynbaum & John Koblin, *Fox Settles with Gretchen Carlson Over Roger Ailes Sex Harassment Claims*, N.Y. Times (Sept. 6, 2016), https://www.nytimes.com/2016/09/07/business/media/fox-news-roger-ailes-gretchen-carlson-sexual-harassment-lawsuit-settlement.html?_r=0 [https://perma.cc/CX6Z-BNDA] (discussing Carlson's use of secret recordings to support sexual harassment claims against Ailes).

[36] *See, e.g.*, John E.B. Myers, *California's Eavesdropping Law Endangers Victims of Domestic Violence*, 31 J. Marshall J. Info. Tech. & Privacy L. 57 (2014) (outlining circumstances in which domestic violence victims might finds themselves confronted with criminal or civil charges for recording their abusers and suggesting strategies for reforming California's wiretap law).

[37] 114 Cong. Rec. 14,694 (May 23, 1968) (statement of Sen. Hart).

[38] *Id.*

[39] *See id.* The argument was not for a strong all-party consent system like in Illinois or Massachusetts, but rather for an all-party rule with exceptions for those who wished to use the tapes to defend themselves.

B. Rationale for All-Party Consent Laws

Alan Westin, one of the foremost legal academics in the field of privacy law, succinctly summarized the fears motivating all-party consent laws in 1966, two years before the first version of the Federal Wiretap Act went into effect. He argued that a one-party consent exception would undermine the court order process for government eavesdropping and predicted that "as technology enables every man to carry his microminiaturized recorder everywhere he goes and allows every room to be monitored surreptitiously . . . permitting eavesdropping with the consent of one party would be to sanction a means of reproducing conversation that could choke off much vital social exchange."[40] Professor Westin's concerns about the impact of one-party consent laws on privacy and social interactions were shared by states as they drafted their wiretapping and eavesdropping laws.

Like Professor Westin, Pennsylvania's legislators stressed the social value of privacy and decided that preserving the privacy of conversation was more valuable than allowing those conversations to be recorded and shared. Pennsylvania's wiretap act prohibits the interception of wire, oral, or electronic communications unless all parties consent or unless there is no expectation of privacy.[41] The Pennsylvania legislature enacted the all-party consent law based on the determination that "as a matter of state public policy . . . the right of any caller to the privacy of his conversation is of greater societal value than the interest served by permitting eavesdropping or wiretapping."[42]

Legislation in Massachusetts and Illinois reflect similar concerns. Massachusetts, which has one of the most restrictive all-party consent laws, begins its wiretap statute with a preamble framing the goal of the law as protecting citizens from "grave dangers to . . . privacy" implicated by "unrestricted use of modern surveillance technology."[43] Massachusetts courts, while acknowledging the law's stringency, have explained that the law was a response to "concern over the commercial availability of electronic devices capable of intercepting wire or oral communications, and the recognition that there was no way effectively to prohibit the sale or manufacture of these devices."[44] Concerned about the impact recording devices would have on police practices and interpersonal communication, the Massachusetts legisla-

---

[40] Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's*, 66 COLUM. L. REV. 1205, 1226 (1966).

[41] *See* 18 PA. STAT. AND CONS. STAT. § 5702 (2017) (defining an "oral communication" as "any oral communications uttered by a person possessing an expectation that such communication is not subject to interception . . .").

[42] Commonwealth v. McCoy, 275 A.2d 28, 30 (Pa. 1971).

[43] MASS. GEN. LAWS ch. 272, § 99 (2017).

[44] Commonwealth v. Hyde, 750 N.E.2d 963, 966–67 (Mass. 2001); *see also* Commonwealth v. Thorpe, 424 N.E.2d 250, 255 (Mass. 1981) ("[E]lectronic surveillance is anathema except within certain narrowly prescribed boundaries.").

ture revised its one-party consent statute and replaced one-party with all-party consent.[45]

Likewise, legislators in Illinois worried that "unless we prohibit electronic eavesdropping, it could and would be used in business in connection with civil cases, not just by police."[46] The legislature further reasoned that "we must protect the citizen's right to privacy from their own government."[47] There were concerns that anything other than all-party consent would lead to surreptitious recordings by private citizens as well as police officers, and that this would discourage open communication and weaken social ties.[48] When Illinois courts narrowed the coverage of the wiretap law by holding that it did not apply to recordings made where the recorded individual lacked an expectation of privacy, the legislature reversed the judicial branch and reestablished the all-party system.[49] This pattern was repeated again in 2014, demonstrating significant legislative commitment to all-party consent requirements.[50]

III. Flaws in All-Party Consent Laws

All-party consent laws should be replaced with one-party consent statutes because all-party consent laws do not achieve their central purpose, criminalize commonplace behavior, and create a system in which private citizens are subject to warrantless surveillance but penalized for recording the police.

A. All-Party Consent Laws Do Not Achieve Their Intended Goals

All-party consent laws made little sense even at the time they were established, since they do not achieve their core goals—protecting privacy and social bonds. All-party consent statutes allegedly protect privacy by ensuring that words uttered in confidence stay in confidence. But the laws do not and cannot prevent parties to a conversation from sharing the content of

---

[45] *Hyde*, 750 N.E.2d at 966–67.

[46] *Bid to Weaken Anti-Wiretap Bill Defeated: State Senate Refuses to Reconsider Vote*, Chi. Trib., June 11, 1963, at 7.

[47] *Id.*

[48] *Id. See also* Carol M. Bast, *Eavesdropping in Florida: Beware a Time-Honored but Dangerous Pastime*, 21 Nova L. Rev. 431, 462 (1996).

[49] *Compare* People v. Beardsley, 503 N.E.2d 346, 350 (Ill. 1986) (holding that eavesdropping has occurred only where the nonconsenting participants "intended their conversation to be of a private nature under circumstances justifying such expectation") *with* People v. Nestrock, 735 N.E.2d 1101, 1107 (Ill. App. Ct. 2000) (interpreting revision of Illinois law to forbid recording of "all" conversations to prohibiting eavesdropping even where participant had no expectation of privacy).

[50] Monique Garcia, *Quinn signs new Illinois eavesdropping rules into law*, Chi. Trib. (Dec. 30, 2014, 5:53 PM), http://www.chicagotribune.com/news/ct-quinn-signs-illinois-eavesdropping-law-met-1231-20141230-story.html [https://perma.cc/26XZ-VKPX].

private conversations without the consent of all parties.[51] In all-party and one-party consent systems, a party to a conversation can share his or her recollections of its content in the press or online without the permission of all parties. Moreover, irrespective of state wiretap laws, in most circumstances individuals engaged in a private conversation can be called to testify in court as to what they uttered.[52] Because a party to a conversation can share recollections of the conversation without consent, the only functional difference between the privacy protections of one-party and all-party schemes is that all-party consent laws prevent parties from unwittingly being recorded by parties to the conversation. Though it could be argued that recordings made without consent are more intrusive than sharing without consent, audio recordings are generally more accurate versions of conversations than recollections. An audio recording cannot forget or misremember details. As a result, admitting a recording of a conversation into evidence can be more accurate than calling either party to the conversation to testify in court, and recordings are often deemed admissible where made lawfully.[53] To the extent they exist, limits on the use of out-of-court statements in court are intended to prevent "the danger that the in-court witness will inaccurately report the out-of-court statement"[54] and to ensure that parties are able to cross-examine witnesses.[55] Though recordings do not provide opportunities for cross-examination, they avoid problems of inaccuracy. Rather than protecting the privacy of parties to a conversation, all-party consent laws prevent the documentation of accurate versions of conversations that often are not protected from secondhand sharing. Conversely, one-party consent laws protect privacy by preventing parties from being unwittingly recorded by third parties, while also recognizing the potential benefits of recordings.

Defenders of all-party consent laws argue that they preserve social bonds by allowing parties to speak candidly without fear that their private words will be recorded and rebroadcasted.[56] However, laws requiring all-

---

[51] Exceptions to this general rule include privilege and confidentiality protections, such as doctor-patient confidentiality.

[52] There are rules of evidence controlling the disclosure of privileged conversations in court, but those rules protect parties to privileged conversations even in one-party consent states. *See, e.g.*, TEX. R. EVID. 503 (outlining rules of attorney-client privilege); TEX. R. EVID. 504 (outlining spousal privilege protections).

[53] *See* Bast, *supra* note 48, at 837–38 (discussing instances of conversations taped without all-party consent being admitted in criminal proceedings).

[54] Roger Park, *A Subject Matter Approach to Hearsay Reform*, 86 MICH. L. REV. 51, 56 (1987).

[55] *See id.* at 55–56 (explaining that cross-examination encourages accuracy and allows the opportunity to expose weaknesses in the declarant's memory and credibility).

[56] *See, e.g.*, Westin, *supra* note 40, at 1226; United States v. White, 401 U.S. 745, 762 (1971) (Douglas, J., dissenting) (discussing the implications of allowing warrantless surveillance when one party consents and concluding that "[m]onitoring, if prevalent, certainly kills free discourse and spontaneous utterances"); *id.* at 787 (Harlan, J., dissenting) ("Authority is hardly required to support the proposition that words would be measured a good deal more carefully and communication inhibited if one suspected his conversations were being transmitted and transcribed . . . . [I]t might well smother that spontaneity—reflected in frivolous, impetuous, sacrilegious, and defiant discourse—that liberates daily life.").

party consent are designed to solve a relationship and trust issue that existed long before cellphones and audio recording technology and that continues to exist irrespective of the laws.[57] Before recording technologies became commonplace, conversations could be transcribed and shared from memory without the consent of all parties. The constant potential for that type of sharing did not choke off social exchange. Instead, speakers used relationship strength to manage boundaries and determine how much to reveal in a conversation.[58] All-party consent laws are an additional, state-imposed boundary management tool. The government uses these types of tools to preserve certain social limits "because the alternative could have significant consequences."[59] For example, allowing surreptitious up-skirt photography could lead women to respond by shifting their boundary management mechanisms and wearing slacks rather than skirts or avoiding public transit.[60] The government has an interest in preventing those behavioral shifts, which leads to regulation of the triggering behavior.[61] But unlike circumstances in which the absence of a boundary management tool could result in a behavioral shift, in the case of wiretap laws the underlying behavior the state seeks to regulate—false friendships—existed long before the allegedly problematic technology. State regulation cannot ensure loyalty—a false friend who wishes to share a personal or intimate discussion still can—so the incentive to share or not share information will rarely hinge on the presence or absence of an all-party consent statute.[62] Accordingly, all-party consent laws are likely no more effective at preserving social bonds than one-party consent schemes. Moreover, although intuitively some might find being recorded more intrusive than an untrustworthy individual sharing the contents of a conversation, the potential for all-party consent statutes to criminalize common and socially beneficial behavior further erodes their value.

B. All-Party Consent Laws Criminalize Commonplace Behavior

Due to shifts in norms and technology since the passage of state wiretap laws, all-party consent recording laws criminalize and impose liability for commonplace actions. The social norms of today emphasize privacy from recordings and video surveillance to a lesser extent than the era in which anti-surveillance statutes were first passed. Unlike in the 1960s, the era in

---

[57] *See* Westin, *supra* note 40, at 1226; *see also* Commonwealth v. Blystone, 549 A.2d 81, 87–88 (Pa. 1988) (holding that "[h]ow, when, and to whom the confidant discloses the confidence is his choosing. He may whisper it, write it, or in modern times immediately broadcast it as he hears it"), *aff'd sub nom.* Blystone v. Pennsylvania, 494 U.S. 299 (1990); *cf.* Desnick v. Am. Broad. Cos., Inc., 44 F.3d 1345, 1351 (7th Cir. 1995) (applying false friends logic in trespassing case).

[58] *See* Margot E. Kaminski, *Regulating Real-World Surveillance*, 90 WASH. L. REV. 1113, 1152 (2015).

[59] *Id.* at 1136.

[60] *See id.* at 1137.

[61] *See id.*

[62] Moreover, one-party consent regimes can be supplemented to specifically address many of the fears cited in support of all-party consent regimes. *See infra* Part VII.

which many state wiretapping laws were drafted, people move about the world today under the assumption that their actions are subject to video and audio recording.[63] Moreover, individuals now have the ability to opt-in to environments of scrutiny via channels such as YouTube and Instagram and by agreeing to work in industries like law enforcement in which their every movement is recorded, all of which was unheard of when state surveillance statutes were first drafted.[64] Private citizens also use smartphones as a weapon against illegal and discriminatory behavior. In 2016, Gretchen Carlson made headlines when she used her iPhone to record conversations between herself and Roger Ailes, documenting instances of sexual harassment that she claimed had spanned her entire career at Fox News.[65] Ultimately, Mr. Ailes resigned and Ms. Carlson received a significant settlement from Fox.[66] Ms. Carlson's recordings of Mr. Ailes were made without his knowledge, in secret, and in his office, a space where he likely had an expectation of privacy. As a result, had the recordings been made in an all-party consent states, such as Illinois, Maryland, Massachusetts, and Pennsylvania, Ms. Carlson would have violated wiretapping laws in those jurisdictions. Ms. Carlson would have exposed herself to civil liability and the recordings would likely have been inadmissible had her suit against Mr. Ailes and Fox News gone to trial. Ms. Carlson's decision to secretly record her sexual harasser was not a unique instance of surreptitious audio recordings being used to unmask illegal or unsavory behavior. In recent years, plaintiffs in one-party consent states have recovered on civil claims after recording medical professionals mocking them during surgery[67] and after recording derogatory racial remarks made by employers.[68] Plaintiffs have also settled probate dis-

---

[63] The failure of Google Glass, a set of glasses that functioned as a hands-free computer and included a camera, may indicate society's willingness to be recorded is not without limits. *See* Jake Swearingen, *How the Camera Doomed Google Glass*, ATLANTIC (Jan. 15, 2015), https://www.theatlantic.com/technology/archive/2015/01/how-the-camera-doomed-google-glass/384570/ [https://perma.cc/4MCL-ELLF]. However, Snapchat Spectacles, a cheaper device that records up to thirty seconds of video at a time and uploads it to users' Snapchat social media accounts, have experienced recent success. *See* Anita Balakrishnan, *Snap has sold more Spectacles than Apple sold iPods in their first year, says CEO, but investors still 'fearful'*, CNBC (Oct. 3, 2017, 5:19 PM), https://www.cnbc.com/2017/10/03/snap-spectacles-how-many-have-been-sold.html [https://perma.cc/V7VU-7LAF].

[64] The Bureau of Justice Statistics reports that in 2013 a third of local police departments were using body-worn cameras. BRIAN A. REAVES, BUREAU OF JUST. STAT., LOCAL POLICE DEPARTMENTS, 2013: EQUIPMENT AND TECHNOLOGY (2015), http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5321 [https://perma.cc/89CM-RDYN]. Sixty-eight percent of local police departments used in-car video cameras. *Id.*

[65] *See* Gabriel Sherman, *The Revenge of Roger's Angels*, N.Y. MAG. (Sept. 2, 2016, 7:30 AM), http://nymag.com/daily/intelligencer/2016/09/how-fox-news-women-took-down-roger-ailes.html [https://perma.cc/8TV3-QTN8].

[66] *See id.*

[67] *See, e.g.*, Tom Jackman, *Anesthesiologist Trashes Sedated Patient – and It Ends Up Costing Her*, WASH. POST (June 23, 2015), https://www.washingtonpost.com/local/anesthesiologist-trashes-sedated-patient-jury-orders-her-to-pay-500000/2015/06/23/cae05c00-18f3-11e5-ab92-c75ae6ab94b5_story.html?utm_term=.1c7fe246bd4f [https://perma.cc/3JXG-6QCE].

[68] *See* David Koeppel, *More People are Using Smartphones to Secretly Record Office Conversations*, BUS. INSIDER (July 28, 2011, 5:43 PM), http://www.businessinsider.com/smartphones-spying-devices-2011-7 [https://perma.cc/ULD7-7A7J].

putes through the use of surreptitious recordings.[69] States, particularly those with all-party consent statutes, have been facing pressure to allow video and audio recording in nursing homes so that residents and their families can combat abusive conditions.[70]

These shifts in social attitudes towards video surveillance have been accompanied by changes in technology that make it challenging to administer wiretap laws as written. Common video and audio recording devices include:

- Nanny cameras: devices used to record children and caregivers while parents are away;
- Dashboard cameras: car-mounted cameras which are standard in police vehicles and are also available for use in personal vehicles;[71]
- Wearable cameras: examples include GoPros and Snapchat Spectacles,[72] which can be used to record audio and video footage as the user goes through her day or performs sporting and recreational activities, and;
- Smart home technologies: this category includes devices such as video doorbells which record audio and video whenever they are rung or individuals approach them.

The legality of these devices in all-party consent states is unclear. Generally, courts have analyzed the use of these devices under the same framework as any other eavesdropping device. For example, in 2010 Anthony Graber was arrested in Maryland for violating state wiretapping laws after his helmet-mounted camera recorded his experience during a traffic stop.[73] Mr. Graber uploaded the footage to YouTube, and local police responded

---

[69] *See* David Kravets, *Court OKs Covert iPhone Audio Recording*, WIRED (Aug. 18, 2010, 4:37 PM), https://www.wired.com/2010/08/covert-iphone-audio-recording/ [http://perma.cc/BRD7-2CRD].

[70] *See* Kelly Greene, *Legislative Support Grows For Nursing-Home Cameras*, WALL STREET J. (Mar. 7, 2002, 12:01 AM), http://www.wsj.com/articles/SB1015452422739779360 [http://perma.cc/Y4FM-BAKB]; Jenni Bergal, *Nursing Home Cameras Create Controversy*, PEW CHARITABLE TRUSTS: STATELINE (Sept. 25, 2014), http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2014/09/25/nursing-home-cameras-create-controversy [http://perma.cc/QZ3T-K387]; Tracey Kohl, *Watching Out for Grandma: Video Cameras in Nursing Homes May Help to Eliminate Abuse*, 30 FORDHAM URB. L.J. 2083, 2083 (2002).

[71] *See* Cleve R. Wootson Jr., *Video shows police tackling and beating a black man suspected of stealing a car. It was his.*, WASH. POST (Jan. 14, 2017), https://www.washingtonpost.com/news/post-nation/wp/2017/01/14/video-shows-police-tackling-and-beating-a-black-man-suspected-of-stealing-a-car-it-was-his/?utm_term=.39f064756a19 [http://perma.cc/K8WT-NQ2D].

[72] *See* Daniel Victor, *10-Second Videos From Your Sunglasses. Thank Snapchat.*, N.Y. TIMES (Nov. 11, 2016), https://www.nytimes.com/2016/11/12/technology/10-second-videos-from-your-sunglasses-thank-snapchat.html [https://perma.cc/5LSW-5HJJ].

[73] *See* State v. Graber, No. 12-K-10-647, 2010 Md. Cir. Ct. LEXIS 7, at *4 (Md. Cir. Ct. Sept. 27, 2010); Peter Hermann, *Judge says man within rights to record police traffic stop*, BALT. SUN (Sept. 27, 2010), http://articles.baltimoresun.com/2010-09-27/news/bs-md-recorded-traffic-stop-20100927_1_police-traffic-stop-police-officers-anthony-graber [http://perma.cc/46HY-7T36].

with an arrest.[74] The charges were eventually dismissed on the grounds that because the officers did not have an expectation of privacy, no state law violation had occurred.[75] The county judge hearing the case treated the helmet camera in the same manner he would any other surveillance device used to record the police.[76] This approach is suitable for devices that are closely analogous to standard eavesdropping devices such as tape recorders. But not all new devices can be placed squarely in the categories created by wiretap laws.

For instance, the legality of Snapchat Spectacles and smart doorbells in all-party consent states is uncertain. Snapchat Spectacles are wearable recording devices that take ten-second long audio and video recordings from the wearer's perspective.[77] The videos are automatically uploaded to the Snapchat application, where followers of the uploader can view them.[78] The devices resemble a standard pair of sunglasses, but have round camera lenses on either side of the frame that light up when the user is recording.[79] They are currently for sale nationwide, including in all-party consent states, but it is unclear whether using the Spectacles in all-party consent states is legal. In Massachusetts, "secret" audio recordings are prohibited without consent.[80] The device's indicator lights may be sufficient to make the recording open rather than secret, but the novelty of the devices may prevent subjects of video and audio recordings from understanding that they are being recorded. In California, where most of the devices have been sold, eavesdropping laws prohibit the recording of confidential conversations, which the law defines as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties."[81] Because the devices upload videos automatically after they are recorded, there is a significant likelihood that users wearing the devices during the course of their everyday lives could unintentionally record private communications, which would be automatically uploaded and publicly available.[82]

Similarly, video doorbells can record snippets of conversation by mailmen, passersby, and other residents—especially if used in a multi-family building. The devices could be considered "secret" devices in Massachusetts and Illinois, depending on their design and the courts' interpretation of

---

[74] *See Graber*, 2010 Md. Cir. Ct. LEXIS 7, at *4.
[75] *See id.* at *19.
[76] *See id.* at *7–8.
[77] FEATURES, https://www.spectacles.com/features/ [http://perma.cc/X7KW-PM4L].
[78] *See id.*
[79] *See id.*
[80] *See* MASS. GEN. LAWS ch. 272, § 99 (2017).
[81] CAL. PENAL CODE § 632 (West, Westlaw with urgency legislation through Ch. 859 of 2017 Reg. Sess.).
[82] The glasses record up to thirty seconds of video at a time. *See* FEATURES, *supra* note 77. The unintentional recording of private communication could occur if, while using the device, someone near the recorder utters a confidential communication picked up by the Spectacles' microphone. The communication would be recorded and uploaded to the user's account, where it could be viewed publicly. *See id.*

the word "secret."[83] The device may also violate one-party wiretap consent statutes because it records whenever there is motion near the device, even if the owner of the device is not a party to the conversations or actions triggering the device. Spying devices are not a new concept, but smart-home technologies differ from spying devices in that their purchasers generally are not intending to eavesdrop. They are often concerned about whether their packages are arriving as scheduled and whether their home is secure while they are away. Moreover, the packaging and websites accompanying Snapchat Spectacles and standard smart doorbell devices do not mention the potential wiretap and eavesdropping implications of the devices, making it unlikely that a standard consumer is even aware of the potential legal implications of her recordings.[84] New recording devices seem to be Professor Westin's worst nightmare made real, but they also demonstrate an evolution in social norms and expectations. Consumers are now demanding technologies that scholars and legislatures framed as intrusive and undesirable when wiretapping laws were drafted. In light of this development, do legal frameworks designed to suppress the use of those technologies make sense?

C. All-Party Consent Laws Facilitate Police Surveillance while Undermining Accountability

Wiretapping statutes were passed in response to a specific fear and a specific problem. The fear—that surveillance technology would lead to extensive recording of private conversations without participant consent and for malicious purposes—has not come to fruition. Criminal sanctions designed to prevent malicious recordings have protected civilian privacy in one-party consent states. In fact, recording devices have been used as a tool for justice and transparency in many instances. Meanwhile, wiretapping statutes in all-party consent states are failing to address the problem that they were designed to solve—the persistent use of wiretapping by law enforcement officials without a warrant. Legislators drafting all-party consent statutes worried that police officers could use one-party consent as an end-run around warrant requirements by getting the consent of informants and using them as a means to record others without probable cause.[85] Though all-party consent laws criminalize warrantless wiretapping, advancements in policing technology have introduced inconsistencies into all-party consent schemes, creating a framework in which private citizens are subject to constant war-

---

[83] The legality of the doorbells would likely hinge on whether its design makes it easy for passersby to discern that they are being recorded. A device that closely resembles a normal doorbell could be considered a "secret" recording device under Illinois or Massachusetts law. *See* MASS. GEN. LAWS ch. 272, § 99 (2017); 720 ILL. COMP. STAT. ANN. 5/141–2 (2017).

[84] *See* FEATURES, *supra* note 77; RING, https://www.ring.com/ [https://perma.cc/KQ8Y-4ZK6].

[85] *See, e.g.*, Commonwealth v. Blood, 507 N.E.2d 1029, 1035 (Mass. 1987) (writing that the "consent exception puts the conversational liberty of every person in the hands of any officer lucky enough to find a consenting informant").

rantless surveillance and penalized for attempting to record the police in turn.

Today, most police vehicles are equipped with audio and visual recording technologies that activate whenever officers are on duty.[86] An increasing number of police departments are also investing in wearable cameras.[87] Putting aside the legality of those devices under all-party consent wiretapping statutes, the use of wearable and vehicular recording devices create inconsistencies within all-party consent surveillance schemes.[88] Law enforcement officers wearing body cameras record anyone they encounter while on-duty and have the potential to record the conversations of third-parties as well as conversations between officers and civilians. This directly violates the intent of all-party consent statutes designed to curtail the use of warrantless surveillance measures.

Meanwhile, the legality of civilian recordings of police encounters remains hazy. Some states expressly allow the recording of on-duty police officers, others have been pushed in that direction by judicial decisions, and still others have continued to prosecute individuals who record the police, even while allowing the police to make frequent recordings of civilians. State wiretap laws and judicial precedent controlling the legality of police recordings raise two questions. First, can citizens lawfully record police officers in the course of their duties? Second, if recordings can be made lawfully, is the right clearly established? If recordings are lawful then officers cannot arrest citizens for filming them. If there is a clearly established right to record the police then individuals who record the police and are forced to stop recording by law enforcement officers can bring civil claims against police departments. If no clearly established right exists, officers are granted qualified immunity.[89]

The tension between the legality of recording and qualified immunity is illustrated by the Third Circuit's decision in *Kelly v. Borough of Carlisle*.[90] Brian Kelly was arrested for violating the Pennsylvania Wiretap Act after he recorded a traffic stop using a small handheld camera.[91] Mr. Kelly was a passenger in the vehicle and recorded the encounter between the driver and

---

[86] *See* REAVES, *supra* note 64.

[87] *See id.*

[88] The legality of these devices, particularly wearable body cameras, and their interactions with wiretap laws is unclear. Some all-party consent states, such as New Hampshire, have specifically amended their wiretap and recording statutes to allow the use of body cameras by police officers. *See* N.H. REV. STAT. ANN. § 570-A:2 (West, Westlaw through Ch. 258 (End) of 2017 Reg. Sess., not including changes and corrections made by State of N.H., Off. of Legisl. Services). States without amendments may unwittingly be violating their own laws by installing wearable recording devices on their officers.

[89] *See* Harlow v. Fitzgerald, 457 U.S. 800, 818 (1982) (explaining that the doctrine of qualified immunity protects government employees "from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known").

[90] 622 F.3d 248 (3d Cir. 2010).

[91] *See id.* at 251.

the police officer.[92] The charges against Mr. Kelly were eventually dropped, but he sued the police department, alleging that his First and Fourth amendment rights were violated.[93] The court held that qualified immunity would protect the officer and the department as long as "their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known."[94] At the time of Mr. Kelly's arrest, two Pennsylvania Supreme Court cases had held that covert recordings of the police do not violate the Pennsylvania Wiretap Act, and Pennsylvania case law had also established that police officers do not have a reasonable expectation of privacy while conversing with suspects.[95] The court remanded the case for additional fact finding on the Fourth Amendment issue and whether the officers violated a clearly established right.[96] On the First Amendment claim, the Court held that if a right to record existed, it would be subject to reasonable time, place, and manner restrictions.[97] The Court ultimately held that although Mr. Kelly's recording had not violated the Pennsylvania Wiretap Act, he could not recover on his First Amendment claim because there was insufficient case law demonstrating that there was a right to videotape police officers during a traffic stop.[98] Since a reasonably competent officer would not be on notice that seizing Mr. Kelly's camera or arresting him for videotaping during the stop would violate the First Amendment, the arresting officers were protected by qualified immunity.[99]

Beyond the Third Circuit, other jurisdictions also have considered the legality of arrests under state wiretap laws and the ability of citizens to recover civilly when officers arrest them for recording or otherwise force them to cease recording. In *Glik*, the First Circuit held that a recording made by a bystander of a police officer arresting a suspect did not violate the Massachusetts Wiretap Act, an all-party consent statute, because it was not a secret recording.[100] This meant that the recorder, Simon Glik, could recover on his Fourth Amendment claim.[101] Moreover the Court held that a citizen's right to film law enforcement officers discharging their duties in a public space was

---

[92] *See id.*

[93] *See id.* at 252.

[94] *Id.* at 253 (quoting *Harlow*, 457 U.S. at 818).

[95] *See id.* at 258 (citing Agnew v. Dupler, 717 A.2d 519, 522 (Pa. 1998) and Commonwealth v. Henlen, 564 A.2d 905, 906 (Pa. 1989)).

[96] The officer was ultimately granted qualified immunity because he had consulted with an assistant district attorney before arresting Mr. Kelly, and the good faith reliance on objectively reasonable advice entitled him to immunity. Kelly v. Borough of Carlisle, 544 F. App'x 129, 135 (3d Cir. 2013). The court did not rule on the substantive Fourth Amendment issue. *Id.*

[97] *See id*. at 262.

[98] *See id.* (concluding "there was insufficient case law establishing a right to videotape police officers during a traffic stop" when some cases existed announcing a broad right to videotape police while others suggested a narrower right).

[99] *See id.*

[100] Glik v. Cunniffe, 655 F.3d 78, 87 (1st Cir. 2011) ("The complaint alleges that Glik 'openly record[ed] the police officers' with his cell phone, and further that 'the police officers admitted Mr. Glik was publicly and openly recording them.' On its face, this conduct falls plainly outside the type of clandestine recording targeted by the wiretap statute.").

[101] *Id.* at 88.

well-established, such that Mr. Glik could also recover on his First Amendment claim.[102] In instances in which recordings of the police are made secretly, they likely are not protected in the First Circuit.[103] The Ninth and Eleventh Circuits have also weighed in on the issue, with the Ninth Circuit holding in a case involving the filming of police that the First Amendment protected the right to film matters of public interest.[104] The Eleventh Circuit ruled similarly, stating that petitioners "had a First Amendment right . . . to photograph or videotape police conduct," but that the right was "subject to reasonable time, manner and place restrictions."[105] The absence of uniform recognition of the right to record is troubling. If the right to record were clearly established, it would encourage witnesses of police misconduct to make recordings and discourage law enforcement from unlawfully arresting those recorders, since the officers could face civil liability. In the absence of a clearly established First Amendment right to record, one-party consent schemes would protect those who record the police and discourage unlawful arrests. Each of the cases cited above took place in an all-party consent regime, and would have been conclusively lawful in the many one-party consent states. Moreover, if the recordings had occurred in one-party consent states, the recorders may have been able to avoid the problem of qualified immunity in the Fourth Amendment context, despite the lack of a universally recognized right to record.[106]

The dissonance between allowing near-constant surveillance by the government, in the form of police dash-cams and body cameras, while limiting the ability of individuals to record their interactions with one another or with the police calls into question the necessity of all-party consent laws. Given the frequency with which stories of officer abuse of minority and low-income individuals have been recorded by phones and other handheld devices and then shared via social media and traditional news outlets,[107] it is in

---

[102] *Id.* at 85.

[103] *See* Commonwealth v. Hyde, 750 N.E.2d 963, 971 (Mass. 2001) (holding that a secret recording of a police officer during a traffic stop violated the Massachusetts Wiretap Act). The right to record is also limited based on the time, place, and whether the recording interferes with an officer's performance of job duties. *See* Gericke v. Begin, 753 F.3d 1, 8 (1st Cir. 2014) ("[A] police order that is specifically directed at the First Amendment right to film police performing their duties in public may be constitutionally imposed only if the officer can reasonably conclude that the filming itself is interfering, or is about to interfere, with his duties.").

[104] *See* Fordyce v. City of Seattle, 55 F.3d 436, 439 (9th Cir. 1995). However it is worth noting that the Court did not explain why the First Amendment right to record matters of public interest specifically protected recordings of the police.

[105] Smith v. City of Cumming, 212 F.3d 1332, 1333 (11th Cir. 2000).

[106] The Fourth Amendment requires that an arrest be grounded in probable cause. *See* Beck v. Ohio, 379 U.S. 89, 91 (1964). If state law permits one-party consent recordings, officers would not have probable cause to arrest bystanders who record them. As a result, such arrests would violate the Fourth Amendment and arrestees who bring civil suits against officers would be able to avoid qualified immunity and recover.

[107] *See, e.g.*, Catherine E. Shoichet, *Facebook Live Video Offers New Perspective on Police Shootings*, CNN (July 7, 2016), http://www.cnn.com/2016/07/07/us/facebook-live-video-minnesota-police-shooting/ [https://perma.cc/LB62-6ZU4]; Julie Bosman & Mitch Smith, *Chicago Police Routinely Trampled on Civil Rights, Justice Dept. Says*, N.Y. TIMES (Jan. 13,

the interest of justice to encourage recordings of the police. However, the uncertain legality of citizen recordings of the police could stifle such recordings. Additionally, as body cameras become commonplace, it is now possible for a police officer to record a citizen while the civilian is unable to simultaneously record the officer. That scenario seems to directly violate the central goal of all-party consent statutes—protecting private citizens from the prying eye of the government.

IV. Legal Challenges to State Wiretap Laws

The First Circuit's reasoning in *Glik* is an indicator that the constitutionality of all-party consent laws is eroding. In *Glik*, the First Circuit held that Mr. Glik's non-secret recording of an on-duty police officer in a public park was protected by the First Amendment because his actions fit "comfortably within [First Amendment] principles."[108] The Court framed First Amendment principles broadly, stating that "the First Amendment's aegis extends further than the text's proscription on laws 'abridging freedom of speech, or of the press,' and encompasses a range of conduct related to the gathering and dissemination of information."[109] This broad framing of the First Amendment as a protection on the flow of information has its roots in Supreme Court precedent dealing with commercial speech and obscenity laws.

The Supreme Court has protected the rights of businesses to make campaign expenditures and the right of consumers to access prescription drug cost information on the grounds that "the First Amendment goes beyond protection of the press and the self-expression of individuals to prohibit government from *limiting the stock of information* from which members of the public may draw."[110] In *First National*, the Court scrutinized a criminal statute in Massachusetts making expenditures by banks for the purposes of influencing referendum votes illegal.[111] Like the First Circuit in *Glik*, the Court in *First National* applied an expansive view of the First Amendment, explaining that "the press does not have a monopoly on . . . the ability to enlighten."[112] Corporations had a role in "affording the public access to discussion, debate, and the dissemination of information" as much as the traditional press, making the limit on corporate contributions subject to strict scrutiny and ultimately unconstitutional.[113] In *Virginia State Board of Phar-*

2017), https://www.nytimes.com/2017/01/13/us/chicago-police-justice-department-report.html [https://perma.cc/T6M8-NG4E] (reporting on a recent Justice Department investigation that found significant and recurring incidences of officer aggressions towards city residents, particularly minorities).

[108] Glik v. Cunniffe, 655 F.3d 78, 82 (1st Cir. 2011).

[109] *Id.*

[110] First Nat'l Bank of Bos. v. Bellotti, 435 U.S. 765, 783 (1978) (emphasis added); *see also* Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 764 (1976).

[111] *First Nat'l Bank of Bos.*, 435 U.S. at 767.

[112] *Id.* at 782.

[113] *Id.* at 783, 796.

macy, the Court struck limits on advertising prescription drug prices on the grounds that consumer interest in the flow of information "may be as keen, if not keener by far, than his interest in the day's most urgent political debate."[114] Similarly, in the obscenity context, the Court has held that "the Constitution protects the right to receive information and ideas . . . regardless of social worth."[115]

Like limits on commercial election expenditures, pharmaceutical advertising, and the distribution of lewd materials, all-party consent laws limit the stock of information from which the public draws. All-party consent statutes can prevent the dissemination of information regarding workplace abuses, malfeasance by public servants, and other matters of public interest.[116] The First Circuit's application of the Supreme Court's "stock of information" reasoning could lead to more challenges to all-party consent laws—particularly in the context of limits on workplace recordings, recordings of sexual harassers, and recordings of government officials. The First Circuit is not alone in its approach. The Seventh Circuit cited "stock of information" principles in a 2014 decision acknowledging that Illinois's all-party consent eavesdropping law had First Amendment implications. The Seventh Circuit held the state's all-party consent laws had "far from incidental" effects on the First Amendment. The Court reasoned that by specifically targeting a medium of expression, the use of an audio recorder, "[t]he law's legal sanction is directly leveled against the expressive element of an expressive activity. As such, the statute burdens First Amendment rights directly, not incidentally."[117] Illinois responded by continuing to use its wiretap law as grounds for prosecuting individuals making recordings of the police in public until the Illinois Supreme Court held the law unconstitutional in 2014. The legislature subsequently amended the eavesdropping statute, adding language limiting the prohibition to cover only recordings of private conversations made surreptitiously. This new statute makes non-surreptitious recordings of on-duty police officers lawful, but like in Massachusetts the law could still be used to penalize secret recordings of on-duty officers and recordings made in circumstances similar to the Gretchen Carlson–Roger

---

[114] *Va. State Bd. of Pharmacy*, 425 U.S. at 763.

[115] Stanley v. Georgia, 394 U.S. 557, 564 (1969).

[116] *See, e.g.*, Ben Botkin, *Taxicab authority can't be 'heavy-handed,' chief says in secret recording*, Las Vegas Rev. J. (Feb. 15, 2014, 4:47 P.M.), https://www.reviewjournal.com/news/taxicab-authority-cant-be-heavy-handed-chief-says-in-secret-recording/ [https://perma.cc/U243-46JH] (detailing wiretap charges brought against employee who recorded his supervisor engaging in allegedly corrupt practices). *Compare* Knight v. Dep't of Police, 619 So. 2d 1116 (La. Ct. App. 1993), *writ denied*, 625 So. 2d 1058 (La. 1993) (recording of phone call in which police captain made racially derogatory remarks did not violate Louisiana's one-party consent statute where both parties knew that incoming calls to police headquarters were regularly monitored) *with* Coulter v. Bank of Am. Nat'l Tr. & Sav. Ass'n, 33 Cal. Rptr. 2d 766, 771 (Cal. Ct. App. 1994) (affirming award of $132,000 in damages to coworkers whom Coulter recorded without consent as part of his attempt to build a sexual harassment claim against the bank).

[117] ACLU of Ill. v. Alvarez, 679 F.3d 583, 602–03 (7th Cir. 2012).

Ailes tapes, both of which could fall under the Supreme Court's "stock of information" principle.

The National Labor Relations Board (NLRB) has also made moves to strike down limits on workplace recordings instituted via workplace policies. In December 2015, the NLRB held that Whole Foods's prohibition on workplace recordings violated the National Labor Relations Act, since the broad policy could prevent employees from engaging in protected workplace activities.[118] Company rules prohibited recordings of meetings or aspects of the work environment without company approval and did not include exceptions for organizing activities.[119] By acknowledging that recordings in the workplaces can be a potential organizing tool, the decision reframes recordings as tools of information dissemination, rather than infringements on privacy. This reframing has the potential to place workplace recordings in the ambit of First Amendment protection. It remains to be seen how the decision will interact with all-party consent laws, but it is another indicator that all-party consent statutes will face increased First Amendment scrutiny as the practice of recording daily interactions becomes more and more commonplace.

Challenges to all-party consent laws based on First Amendment arguments have their limits—for example freedom of the press arguments against all-party consent laws often fail since reporters cannot use the First Amendment as an excuse to disobey laws of general applicability.[120] However the Supreme Court's rationale in the commercial speech, election speech, and obscenity contexts has framed the First Amendment as a broad protection on the public's access to information, and circuit court precedent has framed all-party consent laws as limits on access to information in several contexts. This, coupled with litigation directly challenging the First Amendment implications of all-party consent laws, indicates that reform may be forthcoming. As a result, reevaluating all-party consent laws will help states avoid costly litigation based on free speech arguments while also protecting privacy. Simultaneous to the rollback of all-party consent laws, legislatures should consider fortifying existing laws that protect important facets of privacy and relate to surveillance.

V. The Path Forward: Recommendations for Reform

In response to the inconsistencies inherent in all-party consent wiretapping and surveillance laws, all-party consent states should revise their statutes and shift to a one-party consent framework. This shift can be

---

[118] *See* Whole Foods Mkt. Grp., Inc. and United Food and Commercial Workers, Local 919 and Workers Org. Comm. of Chi., 363 N.L.R.B. 87 (2015).

[119] *See id.* at 3.

[120] *See* Branzburg v. Hayes, 408 U.S. 665, 684 (1972) (holding that "the First Amendment does not guarantee the press a constitutional right of special access to information not available to the public generally . . ."); *see also Alvarez,* 679 F.3d at 602 (exploring the relationship between *Branzburg* and citizen recordings of the police).

accompanied by strengthened criminal sanctions for malicious recordings, such as those made in violation of voyeurism and peeping Tom statutes[121] or recordings made consensually but distributed without all-party consent (for example "revenge porn").[122] This would protect the rights of citizens as well as their privacy. If states are unwilling to shift to a fully one-party consent system, a compromise position exists. Rather than adopting a one-party consent system in its entirety, state legislatures could draft a two-track system. This system would require law enforcement officials to seek warrants before engaging in communications interception, regardless of whether the officers have the consent of a party to the communication. Private citizens would be subject to a one-party consent regime, free to record their own conversations so long as they are not doing so maliciously or at the direction of law enforcement.

To date, no state has moved from an all-party consent regime to a one-party consent framework. Though there have been occasional proposals for a movement from one-party consent to all-party consent, few states have altered their schemes in that direction either.[123] Instead, amendments occur primarily via changes to the exceptions provided in all-party consent laws or judicial narrowing of all-party consent laws. Neither option is a comprehensive fix to the over-inclusivity of all-party consent laws and the tension between those laws and new technologies.

A. Shortcomings of Recent Reforms of All-Party Consent Statutes

Illinois revised its wiretap law after the Illinois Supreme Court unanimously held that the existing law unconstitutional in *People v. Clark*[124] and *People v. Melongo.*[125] In *Melongo*, the court addressed whether private citizens had the right to record a phone conversation with a city clerk,[126] while *Clark* involved a defendant in a child support matter recording opposing

---

[121] Voyeurism and peeping Tom laws are not well adapted to the era of video surveillance, leaving victims of 'up-skirt' filming and other invasive video intrusions without remedy. *See* Lance E. Rothenberg, *Re-Thinking Privacy: Peeping Toms, Video Voyeurs, and the Failure of Criminal Law to Recognize A Reasonable Expectation of Privacy in the Public Space*, 49 AM. U.L. REV. 1127, 1131 (2000).

[122] For a discussion of current and potential criminal and tort remedies for revenge porn, *see* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345 (2014).

[123] *See* Ryan J. Brown, *Watch What You Record: Proposed N.J. Legislation Aims to Change State Wiretapping Law*, RUTGERS UNIV. J. L. PUB. POL'Y (July 10, 2014); Lou Ann Anderson, *Accurate news may be at stake with one-party consent ban facing Texas,* WATCHDOG.ORG (May 14, 2015), http://watchdog.org/218789/one-party-consent-texas/ [https://perma.cc/9FSM-ZTQT]. *But see* Commonwealth v. Hyde, 750 N.E.2d 963, 967 (Mass. 2001) (discussing legislature's decision to alter statutory scheme from one-party to all-party consent in 1968).

[124] 6 N.E.3d 154 (Ill. 2014).

[125] 6 N.E.3d 120 (Ill. 2014).

[126] *See id.* at 122.

counsel and the judge without their knowledge.[127] In both cases, the court held that the Illinois law was overbroad, as it sought to protect the privacy of citizens but did not differentiate between recordings in private and non-private settings.[128] As a result, a substantial number of the law's applications were unconstitutional.[129] For instance, the court took issue with the fact that the law could be read to criminalize conduct such as recording loud arguments in the street, recording political debates in a public space, and recording fans at sporting events without regard for whether the speech was considered private or the recording was surreptitious.[130] The Illinois legislature amended the law shortly after the decisions, adding language making recordings illegal only where the recordings are of private conversations and made in a surreptitious manner.[131]

The Illinois legislature's amendments do not remedy the full range of concerns expressed by the Illinois Supreme Court, nor does the new law position the state to adapt to changes in technology and the ubiquity of recording devices. Even as amended, the definitions of surreptitious and private have the potential to cause confusion and lead to outcomes similar to the original law. In *Melongo*, the defendant recorded a conversation with a city clerk over the phone. Because the clerk could not see the recording device, the only way to conform to the new law would be to disclose the recording. If a person is recording in an attempt to gather evidence of bad acts, disclosure would undermine that goal. The definition of private can likewise be problematic. In *Clark*, the defendant recorded a conversation between himself and opposing counsel in a public courtroom hallway, an environment that is neither clearly public nor clearly private. The new law narrows the scope of situations in which the permissibility of recording is unclear, but does not provide guidance for the specific fact patterns of *Clark* and *Melongo*.[132] Rather than attempting to narrow its wiretapping statute for a second time in order to conform to judicial holdings, the Illinois legislature should have shifted the wiretapping scheme into a one-party framework.

B. Shortcomings of Judicial Narrowing of All-Party Consent Statutes

Courts have not been more effective than legislatures at narrowing the scope of all-party consent laws to avoid counterintuitive or unconstitutional applications of the statutes. For example, state courts in Maryland and Nevada have both interpreted their wiretap statutes in a manner not clearly linked to the plain language of the statute. The Maryland statute prohibits the willful interception of any wire, oral, or electronic communication unless all

---

[127] *See Clark*, 6 N.E.3d at 156.
[128] *See id.* at 161; *Melongo*, 6 N.E.3d at 126.
[129] *See Clark*, 6 N.E.3d at 162.
[130] *See Melongo*, 6 N.E.3d at 126.
[131] *See* 720 ILL. COMP. STAT. ANN. 5/141–2 (2017).
[132] It is not clear whether a dash cam, helmet camera, or smart doorbell would be considered surreptitious, and the portability of the latter two devices makes the distinction between private and public recordings a challenge to administer.

parties consent.[133] The statute defines an oral communication as "any conversation or words spoken to or by any person in private conversation."[134] Maryland state courts have interpreted the use of "private conversation" in the definition of oral communication to mean that the Act only applies if the parties to the communication have a reasonable expectation of privacy.[135] The phrase "expectation of privacy" never appears in the statute. The court's decision to read that meaning into the statute and to define it pursuant to the Supreme Court's Fourth Amendment precedent narrows the statute and renders it constitutional. It also makes it difficult for a lay reader of the statute to accurately parse its scope. This could discourage Maryland residents seeking to record a conversation for socially desirable reasons—such as documenting questionable police conduct during a traffic stop—from making those recordings.

The Nevada state courts have acted in the opposite manner as the Maryland courts, but to the same effect. Nevada's wiretapping statute addresses wire and oral communications in different statutory sections. The section of the Nevada statute controlling the interception of oral communication is a standard one-party consent scheme. The interception is lawful if one party consents to the recording.[136] The section governing wire communication reads as follows:

> Except as otherwise provided . . . it is unlawful for any person to intercept or attempt to intercept any wire communication unless:
>
> (a) The interception or attempted interception is made with the prior consent of one of the parties to the communication; and
> (b) An emergency situation exists and it is impractical to obtain a court order.[137]

The Supreme Court of Nevada interprets this statutory language to prohibit the recording of a wire communication, such as a phone call, unless all parties consent.[138] The exception is relevant only in the case of an emergency and even then must be ratified by a court after the fact in order to be lawful. No special exception is made for individuals opting to record their own conversations with other parties; private citizens are lumped in with law enforcement. This decision was contentious. Four justices dissented on the

---

[133] *See* MD. CODE ANN., CTS. & JUD. PROC. § 10-402 (West, Westlaw through all legis. from the 2017 Reg. Sess. of the Gen. Assemb.).

[134] MD. CODE ANN., CTS. & JUD. PROC. § 10-401 (West, Westlaw through all legis. from the 2017 Reg. Sess. of the Gen. Assemb.).

[135] *See* Malpas v. State, 695 A.2d 588, 595 (Md. Ct. Spec. App. 1997); Fearnow v. Chesapeake & Potomac Tel. Co. of Md., 676 A.2d 65, 70 (Md. 1996).

[136] *See* NEV. REV. STAT. ANN. § 200.650 (West, Westlaw through 79th Reg. Sess. (2017) of Nev. Leg. with all legis. operative or effective up to and including October 1, 2017 subject to change from reviser of Legis. Counsel Bureau.).

[137] NEV. REV. STAT. ANN. § 200.620 (West, Westlaw through the 79th Reg. Sess. (2017) of Nev. Leg. with all legis. operative or effective up to and including October 1, 2017 subject to change from reviser of Legis. Counsel Bureau.).

[138] *See* Lane v. Allstate Ins. Co., 969 P.2d 938, 940 (Nev. 1998).

grounds that it was illogical to classify the recording of one's own conversation as an "interception" and that the statute was clearly designed to prevent law enforcement officers from recording conversations with private citizens, rather than private citizens from recording conversations with one another.[139] Like in Maryland, the Nevada courts have interpreted the statutory language in a manner that may not be intuitive to lay interpreters.

This is not without consequence. In 2014 Joseph Morgan, an investigator with the Nevada Taxicab Authority, called the Chief Investigator on his cell phone.[140] The Chief inadvertently answered the phone, and Morgan was able to overhear a conversation between the Chief and another employee, in which the two made possibly incriminating statements indicating corruption and favoritism between the office and business owners.[141] Morgan recorded a portion of the conversation and was charged with violating the Nevada Wiretap Act.[142] Inconsistencies and a lack of clarity in state wiretap laws affect people, and judicial attempts to bring order to the statutory schemes do not do enough to remedy inconsistencies. Indeed, they often make the situation worse by interpreting statutes in a manner not clearly evident from a plain reading of the text.

C. Shortcomings of Other Proposals for Reform

The idea of limiting the scope of all-party consent laws is not new. Proposals to end all-party consent schemes have been articulated with increasing frequency in recent years. One suggestion involves creating an exception to all-party consent requirements for circumstances in which recordings are made in public places of public officials engaged in a public duty.[143] This type of limited exception to all-party consent statutes would protect individuals like Anthony Graber who are charged with wiretapping after recording encounters with the police. Unfortunately, it would leave individuals who seek to promote transparency and accountability in other circumstances unprotected. Moreover, designing an increasing number of carve-outs to all-party consent statutes based on motives and circumstance will ultimately leave the statutes eviscerated. The most straightforward manner of remedying complicated all-party consent wiretapping schemes is to move away from the all-party system completely. One-party consent laws form the majority of wiretapping schemes for a reason. Unlike all-party laws, they balance the privacy rights of individuals against the many reasons people opt to record conversations. They also have the flexibility to incorporate new technologies and evolving social norms. Legislatures should move

---

[139] *Id.* at 944 (Rose, J., dissenting).
[140] *See* Botkin, *supra* note 116.
[141] *See id.*
[142] *See id.*
[143] *See* Jake Tracer, *Public Officials, Public Duties, Public Fora: Crafting an Exception to the All-Party Consent Requirement*, 68 N.Y.U. ANN. SURV. AM. L. 125, 131 (2012).

towards reshaping state wiretapping laws now, before they are forced to do so by the courts.

VI. Benefits of A Two-Tier Consent Scheme

States with all-party statutes should replace their current provisions with one-party consent obligations based on the statutes in a majority of the states.[144] If state legislators are wary of completely one-party consent systems, a hybrid statutory framework could help bridge the gap between the problematic aspects of all-party consent laws and the privacy concerns of legislators and constituents.

A hybrid wiretapping statute would divide coverage into two tiers. Private citizens would be subject to a one-party consent framework. This framework would allow parties to a communication to record or intercept the communication or to grant third parties the right to do so. Law enforcement officials would remain subject to an all-party consent regime. Specifically, the statute would prohibit law enforcement officials from obtaining the consent of a party to a communication and using that consent to record other, non-consenting parties. This exception to the one-party consent scheme would address one of the concerns articulated during the drafting of one-party consent laws—the potential for warrantless interceptions by law enforcement officers based on the consent of a party to a communication.[145] The system would protect individuals seeking to record their own communications for administrative, legal, or journalistic purposes while drawing a line between the use of recordings by private citizens and interceptions by law enforcement. The distinction between law enforcement and private citizens could be problematic—for instance if a victim of domestic abuse wants a law enforcement officer to listen in on a call with her abuser. However, given the concerns articulated by legislators and the courts, the ultimate balance of harms is closer to equilibrium under a two-tier system. For an example of the potential language a two-tier consent scheme could include, see Appendix I.

VII. Strategies for Protecting Privacy in One-Party Schemes

There are strategies that can mitigate many of the concerns expressed by advocates of all-party consent laws even in one-party consent regimes. Legislatures could end criminal and civil liability for audio recordings made with one-party consent while also encouraging state advisory committees on

---

[144] *See, e.g.*, N.Y. Penal Law § 250.00 (McKinney 2003, Westlaw through L.2017, chapters 1 to 332.); N.Y. Penal Law § 250.05 (McKinney 2003, Westlaw through L.2017, chapters 1 to 332.).

[145] *See e.g.*, Commonwealth v. Blood, 507 N.E.2d 1029, 1035 (Mass. 1987) (worrying that a "consent exception puts the conversational liberty of every person in the hands of any officer lucky enough to find a consenting informant").

the rules of evidence to make inadmissible one-party consent recordings unless they are more probative than prejudicial.[146] This prevents the use of one-party consent recordings as tools to embarrass participants in family law disputes or other civil settings where the goal of the recording is less socially desirable than investigative reporting or exposing sexual harassment.

Moreover, existing tort claims protect private citizens from being the subjects of unwanted audio recordings. Trespass laws or claims of fraud can be used to hold civilly liable those who enter a private area under false pretenses for the purposes of making surreptitious recordings.[147] These doctrines impose context-based liability and take into account the purposes of surreptitious recordings. For example, in *Dietemann v. Time*, the Ninth Circuit held that the photographing and secret audio-recording by reporters of a healer while he was treating patients in his home constituted an invasion of privacy.[148] In determining if there was an invasion of privacy, the court considered the location of the recording and whether the healer had an expectation of privacy in the location.[149] The court relied on the specific facts of the case in making its determination, rather than on whether either party consented to the recordings and photography.[150] In addition to protecting against audio-recordings, invasion of privacy claims allow individuals to recover from the publication of personal facts "that while true and not misleading are so intimate that their disclosure to the public is deeply embarrassing. . . and is perceived as gratuitous by the community."[151]

The final subset of privacy protections for individuals even in the absence of all-party consent laws is laws against surreptitious recordings of sexual encounters or nudity. These laws protect against peeping Toms, the creation of footage for blackmail purposes, and the use of surveillance equipment to unknowingly record guests. Most protect against video, rather than audio, recordings. Nevertheless, these laws are critical supplements to eavesdropping statutes especially given that many new technologies such as Snapchat Spectacles and video doorbells combine audio and video recordings. Even in states like New York, which has long had a one-party consent scheme, it is illegal to use a secret device to record someone dressing or

---

[146] Legislatures do not control the rules of evidence, which are established by the judiciary and advisory committees.

[147] *See* Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz, 82 F. Supp. 3d 344, 359 (D.C. Cir. 2015).

[148] 449 F.2d 245, 248 (9th Cir. 1971) ("[W]e have little difficulty in concluding that clandestine photography of the plaintiff in his den and the recordation and transmission of his conversation without his consent resulting in his emotional distress warrants recovery for invasion of privacy in California.").

[149] *See id.* at 248–249.

[150] *See id.* This fact specific analysis does not always work out in favor of the recorded party. *See* Desnick v. Am. Broad. Cos., Inc., 44 F.3d 1345, 1353 (7th Cir. 1995) (holding that recordings of conversations made by reporters in an ophthalmic office which was open to the public did not constitute an invasion of privacy).

[151] Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222, 1229 (7th Cir. 1993).

undressing in a place where that individual has an expectation of privacy.[152] Statutes like the New York voyeurism prohibition ensure that the most damaging invasions of privacy are subject to criminal, as well as civil, sanction. Further, like trespass and invasion of privacy claims, they allow for a more careful weighing of circumstances than traditional all-party consent laws. Proponents of all-party consent laws with concerns about the impact of new one-party consent schemes on privacy should consider advocating for stronger protections against voyeurism and non-consensual video recordings. Like eavesdropping laws, existing statutory frameworks in the video voyeurism realm have not kept up with advancements in recording technology.[153] But unlike eavesdropping statutes, the laws are too narrow in their scope. They fail to address new transgressions rather than criminalizing socially beneficial activities.[154]

Conclusion

We live in a world where "technology enables every man to carry his microminiaturized recorder everywhere he goes" and in which we are increasingly demanding that our law enforcement officers wear video and audio recording devices whenever they are on duty.[155] However, in eleven states a citizen who records an encounter with a police officer, sexual harasser, or domestic abuser could find herself charged with violating a wiretap law or be told her evidence is inadmissible. All-party consent laws have outlived their value. As written, they do little to satisfy their original purpose, instead sweeping up well-intentioned citizens and users of new technologies. States with all-party consent laws should shift to one-party schemes, which are much more flexible in the face of new technologies and friendlier to private citizens making recordings of their daily lives. There are other privacy-protective measures beyond wiretapping statutes which are already used to protect individual privacy and which can be bolstered in the absence of an all-party consent framework. Continuing to complicate all-party systems by adding exceptions for certain types of recordings either via

---

[152] *See* Danielle Citron, *Nonconsensual Taping of Sex Partner is a Crime*, Forbes: Tech (May 15, 2014, 5:11 P.M.), http://www.forbes.com/sites/daniellecitron/2014/05/15/nonconsensual-taping-of-sex-partners-is-a-crime/#5aa2261b30ed [https://perma.cc/WPZ6-CZ2L].

[153] *See* Lance E. Rothenberg, *Re-Thinking Privacy: Peeping Toms, Video Voyeurs, and the Failure of Criminal Law to Recognize A Reasonable Expectation of Privacy in the Public Space*, 49 Am. U.L. Rev. 1127, 1132 (2000) ("[N]either criminal nor civil law acknowledges an individual's expectation of privacy in public places as reasonable. Therefore, society is simply ill-prepared to combat fully the new-technology crime of video voyeurism.").

[154] *See id.* at 1151 (discussing how video surveillance laws fail to protect the public for up-skirt photography, the non-consensual videotaping of nude individuals in tanning salons, and other instances in which laws "fail[ ] to recognize that today's voyeur, equipped with modern surveillance technology, can violate the privacy of a fully-clothed individual in a public setting almost as easily as it can be to intrude upon the privacy of a naked individual behind the traditionally understood closed door").

[155] Westin, *supra* note 40, at 1226.

legislative amendments or the courts is insufficient to address the shortcomings of all-party consent. Instead, those attempts muddle an already complex legal framework and make it more likely that those who seek to record others for their own defense will choose not to do so out of compliance concerns.

Appendix I: Draft Language

The text of a hybrid one-party and all-party consent statute could read as follows. The hybrid language is bolded:[156]

Sec. XX.XX. UNLAWFUL INTERCEPTION, USE, OR DISCLOSURE OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS.

(a) In this section, "computer trespasser," "covert entry," "communication common carrier," "contents," "electronic communication," "electronic, mechanical, or other device," "immediate life-threatening situation," "intercept," "investigative or law enforcement officer," "member of a law enforcement unit specially trained to respond to and deal with life-threatening situations," "oral communication," "protected computer," "readily accessible to the general public," and "wire communication" have the meanings given those terms in Article XX.XX, Code of Criminal Procedure.

(b) A person commits an offense if the person:
(1) intentionally intercepts, endeavors to intercept, or procures another person to intercept or endeavor to intercept a wire, oral, or electronic communication;
(2) intentionally discloses or endeavors to disclose to another person the contents of a wire, oral, or electronic communication if the person knows or has reason to know the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
(3) intentionally uses or endeavors to use the contents of a wire, oral, or electronic communication if the person knows or is reckless about whether the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
(4) knowingly or intentionally effects a covert entry for the purpose of intercepting wire, oral, or electronic communications without court order or authorization; or
(5) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when the device:
(A) is affixed to, or otherwise transmits a signal through a wire, cable, or other connection used in wire communications; or
(B) transmits communications by radio or interferes with the transmission of communications by radio.

(c) It is an affirmative defense to prosecution under Subsection (b) that:

---

[156] This draft language is based closely on the Texas Wiretap Act, with changes made to exceptions for interceptions by persons acting under color of law. *See* TEX. PENAL CODE ANN. art. § 16.02 (West, Westlaw through end of 2017 Reg. and First Called Sess. of 85th Leg.).

(1) an operator of a switchboard or an officer, employee, or agent of a communication common carrier whose facilities are used in the transmission of a wire or electronic communication intercepts a communication or discloses or uses an intercepted communication in the normal course of employment while engaged in an activity that is a necessary incident to the rendition of service or to the protection of the rights or property of the carrier of the communication, unless the interception results from the communication common carrier's use of service observing or random monitoring for purposes other than mechanical or service quality control checks;

(2) an officer, employee, or agent of a communication common carrier provides information, facilities, or technical assistance to an investigative or law enforcement officer who is authorized as provided by this section to intercept a wire, oral, or electronic communication;

(3) **a person acting under color of law intercepts:**

(A) a wire, oral, or electronic communication, if the person is a party to the communication.

(B) a wire, oral, or electronic communication, if the person is acting under the authority of Article XX.XX, Code of Criminal Procedure; or

(4) **a person not acting under color of law intercepts a wire, oral, or electronic communication, if:**

(A) the person is a party to the communication; or

(B) one of the parties to the communication has given prior consent to the interception, unless the communication is intercepted for the purpose of committing an unlawful act;

(i) A party may not give prior consent to an interception by a person acting under color of law unless all other parties also consent or unless the person is acting under the authority of Article 18.20, Code of Criminal Procedure;

(5) a person acting under color of law intercepts a wire, oral, or electronic communication if:

(A) oral or written consent for the interception is given by a magistrate before the interception;

(B) an immediate life-threatening situation exists;

(C) the person is a member of a law enforcement unit specially trained to:

(i) respond to and deal with life-threatening situations; or

(ii) install electronic, mechanical, or other devices; and

(D) the interception ceases immediately on termination of the life-threatening situation;

(6) an officer, employee, or agent of the Federal Communications Commission intercepts a communication transmitted by radio or discloses or uses an intercepted communication in the normal course of employment and in the discharge of the monitoring responsibilities ex-

ercised by the Federal Communications Commission in the enforcement of Chapter 5, Title 47, United States Code;

(7) a person intercepts or obtains access to an electronic communication that was made through an electronic communication system that is configured to permit the communication to be readily accessible to the general public;

(8) a person intercepts radio communication, other than a cordless telephone communication that is transmitted between a cordless telephone handset and a base unit, that is transmitted:

(A) by a station for the use of the general public;

(B) to ships, aircraft, vehicles, or persons in distress;

(C) by a governmental, law enforcement, civil defense, private land mobile, or public safety communications system that is readily accessible to the general public, unless the radio communication is transmitted by a law enforcement representative to or from a mobile data terminal;

(D) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(E) by a marine or aeronautical communications system;

(9) a person intercepts a wire or electronic communication the transmission of which causes harmful interference to a lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of the interference;

(10) a user of the same frequency intercepts a radio communication made through a system that uses frequencies monitored by individuals engaged in the provision or the use of the system, if the communication is not scrambled or encrypted; or

(11) a provider of electronic communications service records the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service towards the completion of the communication, or a user of that service from fraudulent, unlawful, or abusive use of the service.

(d) An offense under this section is a felony of the second degree, unless the offense is committed under Subsection (d) or (g), in which event the offense is a state jail felony.

(e) A person commits an offense if, knowing that a government attorney or an investigative or law enforcement officer has been authorized or has applied for authorization to intercept wire, electronic, or oral communications, the person obstructs, impedes, prevents, gives notice to another of, or attempts to give notice to another of the interception.