The Wiretapping of Things

Eldar Haber[*]

TABLE OF CONTENTS

INTRODUCTION

Investigating and solving crimes often requires access to data. In the pre-digital era, law enforcement agencies used various techniques to spy

 Senior Lecturer, Faculty of Law, University of Haifa; Visiting Professor, Bocconi University, Italy (2018-2019); Faculty member, Center for Cyber, Law and Policy (CCLP), and Haifa Center for Law and Technology (HCLT), University of Haifa. I am much grateful to Gabriel Focshaner and Naama Shiran for their excellent assistance in research. I also wish to thank participants of Tilting 2019 at Tilburg University (May 2019) for their helpful comments and suggestions. This work was supported by the Center for Cyber Law & Policy at the University of Haifa in conjunction with the Israel National Cyber Directorate in the Prime Minister's Office.

on those who were, at the very least, suspected of engaging in criminal activity. They might have applied investigatory techniques such as using informants, undercover agents or stakeouts, or simply have questioned or interrogated individuals. Throughout history, the state has sought to gain access to new technologies that would advance their investigation or even suspicion of criminal activities — whether by telegraph, by mail or by telephone. As long as the state did not prohibit governmental access to such communication technologies, law enforcement agencies could intercept them in transit, access the acquired data at rest, and use any gathered evidence to arrest, indict, and convict suspects of crimes.

While criminal enforcement might be vital for society, these practices could be highly intrusive for individuals and might jeopardize their human rights and liberties, such as their right to privacy. Responsive to such fears, the Supreme Court's decisions in *Katz v. United States* and *Berger v. New York* reversed the permissible scope of wiretapping under the Constitution.[1] Congress followed suit and regulated wiretapping by enacting the Wiretap Statute under Title III of the 1968 Omnibus Crime Control and Safe Streets Act.[2] With the growth of computer technology, Congress further protected individuals' privacy by enacting the Electronic Communications Privacy Act, which besides revising the Wiretap Act added two more acts to deal with new technological developments: the Stored Communications Act, regulating access to content and metadata stored by electronic communications services, and the Pen Register Act, regulating devices that obtained information about calls.[3] Finally, as technology kept evolving, Congress enacted, and later revised, the Communications Assistance for Law Enforcement Act, by which some telecommunications companies are required to ensure that enforcement agencies will be able to wiretap their networks upon issue of a legal order.[4]

But since the last revision in federal regulation of wiretapping and access to stored communications, technology — together with social changes and digital consumption habits — has rapidly changed. Many individuals in modern society have become almost constantly connected to some type of a network — mostly the internet — whereby their daily activity can be captured, analyzed, and stored by private companies. These technological capabilities have been further expanded due to the invention of the so-called smartphone — a device

[1] *See infra* Part I.A.

[2] *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82. Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2510-22 (2019)).

[3] *See infra* Part I.A.

[4] *Id.*

which, *inter alia*, can potentially track and store mass amounts of data on individuals, such as their locations and movements. Presently a new form of technology is expected to broaden the potential scope of wiretapping and access to stored communication through what is usually termed the *Internet of Things* ("IoT").[5]

The potential technological changes that IoT might bring could be substantial. Many IoT devices are equipped with microphones, cameras, and other sensors and might operate in an "always-on" mode, i.e., constantly collecting and retaining data. The use of sensors combined with internet connectivity could reveal individuals' locations, any information they have conveyed near the IoT device, their images and videos, their vital signs, and much more about people's lives.

Naturally, there is little doubt IoT could become a goldmine for enforcement agencies. Not surprisingly then, IoT devices have in fact already begun to assume a role in criminal enforcement, especially when dealing with stored communications. But while the current governmental use of stored data acquired from IoT is evident, these IoT devices could potentially also be accessed in real time. Equipped with powerful sensors, such as microphones, IoT devices might enable real-time surveillance of individuals in their living rooms, bedrooms, and potentially anywhere they go, depending on the device's type, location, and an individual's proximity to the device. Moreover, rapid technological changes in the field of artificial intelligence and machine learning, along with capabilities in storing and analyzing biometric data such as voices and images, might further expand enforcement agencies' abilities.

Obviously, there is tradeoff between enforcement needs and capabilities and privacy. Allowing government agencies to wiretap IoT, or access its stored communication, is by nature an intrusive form of enforcement that might jeopardize the right to privacy and thus must be further scrutinized prior to any use. The move toward a potential "always-on" era — when most individuals are constantly surrounded by IoT devices — raises several normative questions that must be

[5] The term Internet of Things ("IoT") is attributed to Kevin Ashton, and describes devices or sensors that "connect, communicate or transmit information with or between each other through the Internet." FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 6 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [hereinafter PRIVACY & SECURITY IN A CONNECTED WORLD]; *see* Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (June 22, 2009), http://www.rfidjournal.com/articles/view?4986. For various definitions of IoT, see Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 BERKELEY TECH. L.J. 997, 1008-09 (2016).

further scrutinized prior to the use of IoT by enforcement agencies. Is the current legal framework that governs stored communications and wiretapping, originally designed for computers and telephones, still relevant for these new technological developments? Could the state gain access to IoT devices in real time — and "wiretap" them? Do the current requirements of obtaining a wiretap warrant change in light of IoT capabilities? How should policymakers balance the potential need to acquire such data against safeguarding privacy? And what does the digital future of biometric identification entail regarding the lawful use of enforcement agencies and its potential impact on society?

This Article approaches these and related timely questions by analyzing the current legal framework that governs lawful access to stored communications and wiretapping. Part I introduces the movement from analog to digital enforcement, while addressing the general collision between law enforcement needs and the right to privacy. It then turns to introduce new technologies — namely IoT and always-on devices — and their potential data mining capabilities. Part II scrutinizes wiretapping and datafication in the age of IoT. It discusses the constitutional protection and the regulatory framework that governs both access to stored communication and wiretapping in the age of IoT. Then it discusses the practical challenges of applying the current framework to IoT in the context of access to stored communications and wiretapping. Part III evaluates and discusses the implications of applying the current legal framework to the right to privacy. This Part argues that the current regulatory framework is ill-suited to properly protect privacy, and suggests amendments to this framework. Finally, this Part raises further challenges to privacy under the potential use of technological innovation in the "always-on" era while further warning against the misuse of such technologies without proper regulatory safeguards that would protect against misuse. The Conclusion summarizes the discussion and concludes that while wiretapping could be a necessity in law enforcement, without proper safeguards, allowing the *Wiretapping of Things* might result in mass-surveillance of everything and the demise of our right to privacy.

I. LAW ENFORCEMENT AND TECHNOLOGY

Law enforcement necessitates some form of control and access to what individuals in society are doing. Enforcement agencies might require access to various types of data to detect and prevent crimes, arrest suspects, and eventually use the acquired data as evidence. Accordingly, they would seek to gain as much access as possible to any relevant data on any individual, at any given time. Obviously, however,

lacking judicial oversight, such practices are neither pragmatic nor desirable in a liberal society. From a pragmatic aspect, it would be nearly impossible to know what data is required for a criminal investigation at any given time. From a desirability aspect, the more control the state has, other human rights and liberties — like that of the right to privacy — might be negatively impacted. Thus, there is a tradeoff between what the state should access for legitimate enforcement purposes and what should remain out of its reach, ensuring a fair — supposedly optimal — level of protection for individuals' rights and liberties. This trade-off will often be protected by legal mechanisms that would guide law enforcement agencies and judicial authorities on how to conduct their investigations and when to approve legitimate practices, respectively.

But achieving such equilibrium might not be an easy task. It requires close scrutiny on how enforcement measures could negatively impact the right to privacy — especially when new technological measures come into play. To gain a better understanding of the complexity of new technologies' impacts on such a tradeoff, and the potential broader consequences of legal intervention in this respect, this Part will introduce the movement from analog to digital enforcement, while addressing the general collision between law enforcement needs and the right to privacy. It then turns to introduce new technologies — namely IoT and always-on devices — and their potential data mining capabilities, to set grounds for normatively evaluating such practices in the following Parts.

A. From Analog to Digital Enforcement

Eavesdropping is an ancient practice. Much prior to the development of electronic communication, people listened with their naked ear to communications that they were not part of. With the advent of technological developments like that of mail and the telegraph, law enforcement agencies were suddenly placed in a position of using these developments for their own purposes. It increased their power over the individual to snoop or eavesdrop, and it was formally used at least since the 1860s.[6] What first began as eavesdropping on telegraph

[6] *See* Tom Harris, *How Wiretapping Works*, HOWSTUFFWORKS, https://people.howstuffworks.com/wiretapping3.htm (last visited Feb. 1, 2019). Prior to communication technologies, common law treated eavesdropping as a nuisance. *See* Berger v. New York, 388 U.S. 41, 45 (1967).

communication,[7] has expanded to what is known as *wiretapping* of telephones — known to occur at least since the 1890s.[8]

Coincidently, Samuel Warren & Louis Brandeis articulated a need for a "right to be let alone" at roughly the same time,[9] which gave rise to formal acknowledgment of a right to privacy in years to follow.[10] But such acknowledgment took time, as the right to privacy was not yet officially formalized under the legal regime.[11] At that time, with the exception of state laws, many of which outlawed eavesdropping and wiretapping,[12] federal regulation did not directly address both practices — leaving it to courts' discretion over subpoenas.[13] As held by the

[7] Congress sought access to telegraph messages maintained by Western Union as early as after the Civil War. *See* Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY, PLI 1-8 (2006) [hereinafter *A Brief History*]. Notably, in some states it was a crime for a telegraph company or its employees to disclose the contents to anyone but the authorized recipient. Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 14 (2005).

[8] *See* William Lee Adams, *Brief History: Wiretapping*, TIME (Oct. 11, 2010), http://content.time.com/time/magazine/article/0,9171,2022653,00.html.

[9] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

[10] The American right to privacy is protected under various types of legal mechanisms on both federal and state levels. On the federal level, privacy is protected to some extent under the Court's interpretation of the Bill of Rights, mostly within the First, Third, Fourth, and Fifth Amendments. *See* U.S. CONST. amends. I, III-V. Information privacy, i.e., protecting a right to control one's personal data, is further protected under what is termed as a sectoral approach, whereby some types of information are afforded protection within a context of data use or collection, usually directed only to a particular industry or in a specific context. On the state level, the protection of privacy could be part of various forms of legislation and regulation. One example is that of security or data breach notification law — generally requiring entities that had been subject to a data breach to notify data subjects and potentially other parties about the breach, among various requirements. Another example is that of common law tort actions such as intrusion, public disclosure of private facts, false light, and appropriation. One final example is that of protecting consumers from "unfair and deceptive acts" under commercial collection, use, and release of data under some circumstances. *See* Solove, *A Brief History*, *supra* note 7, at 5. For a taxonomy of privacy, see Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 481 (2006); s*ee also* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1090 (2002).

[11] Notably, Warren and Brandeis argued that the right to privacy already existed under various laws, yet questioned whether such protection was sufficient. *See generally* Warren & Brandeis, *supra* note 9, at 197, 206.

[12] The state of Illinois outlawed eavesdropping and wiretapping in 1895, and many states followed suit. ILL. REV. STAT. ch. 38, para. 14-2(a)(1) (1895); s*ee, e.g.*, FLA. STAT. § 934.03 (2019); TENN. CODE ANN. §§ 39-13-601 to -603 (2019); *see also* Berger v. New York, 388 U.S. 41, 46 (1967); Solove, *A Brief History*, *supra* note 7, at 18.

[13] Even without specific regulation, many courts at that time refused to issue subpoenas for telegram communication. *See* Solove, *A Brief History*, *supra* note 7, at 8.

Supreme Court in 1928, even the Fourth Amendment, which could have prevented enforcement agencies from conducting warrantless "unreasonable searches and seizures," did not apply to wiretapping, making it generally permissible for law enforcement agencies to engage in such practices under the Constitution.[14]

Federal protection against some forms of unlawful wiretapping was first created by Congress's passage of the Communications Act of 1934.[15] Generally governing the interception of telegraphic and telephonic communications,[16] the Communications Act was rather limited in various aspects. First, it only restricted disclosing intercepted communications in court proceedings — but not engaging in the practice of intercepting communications.[17] Second, it applied to federal agencies and failed to apply to state officials.[18] Third, it did not cover various electronic devices that could, *e.g.*, pick up conversations and broadcast them to a receiver when they were relatively close by.[19] Eventually, the Communications Act did little to advance the goals of protecting individuals' privacy, and subsequently, the practice of wiretapping was growing apace.[20]

It was not until 1967 that the Supreme Court, in *Katz v. United States*, narrowed down the permissible scope of wiretapping under the

[14] The first Supreme Court wiretap case was *Olmstead v. United States* back in 1928. Olmstead v. United States, 277 U.S. 438 (1928). Here, there was no entry upon premises and thus no physical invasion of privacy, and thus wiretapping was held as constitutionally permitted. *See* U.S. CONST. amend. IV; *Olmstead*, 277 U.S. at 466 (ruling that no warrant is necessary for federal agents to tap a telephone wire).

[15] *See* Communications Act of 1934, Pub. L. No. 73-416, § 605, 48 Stat. 1064, 1103-04 (1934).

[16] Section 605 provided that "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communications to any person." *Id.* at 1104.

[17] *See* Weiss v. United States, 308 U.S. 321, 329 (1939) (holding that section 605 banned the wiretapping of intrastate telephone calls); Nardone v. United States, 302 U.S. 379, 381 (1937) (explaining these restrictions as provided in section 605 of the Communications Act of 1934); Solove, *A Brief History*, *supra* note 7, at 19. However, if a participant in a call consented to a wiretap, the evidence was admissible against the other party to the conversation. *See* Rathbun v. United States, 355 U.S. 107, 110-11 (1957); Robert A. Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of Email*, 10 MICH. TELECOMM. TECH. L. REV. 1, 28 (2003).

[18] *See* Solove, *A Brief History*, *supra* note 7, at 19.

[19] *See* Berger v. New York, 388 U.S. 41, 46-47 (1967).

[20] *See generally* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1128-33 (2002) [hereinafter *Digital Dossiers*] (outlining the history of Fourth Amendment privacy rights).

Constitution.[21] *Katz* was soon followed by a companion — *Berger v. New York* — in which the Court stroke down portions of a New York state wiretapping statute as it lacked sufficient judicial review.[22] These rulings marked a substantial change in the ways that courts interpreted the protection afforded by the Fourth Amendment and, perhaps more importantly, addressed the right to privacy more directly with regard to criminal enforcement.

Soon thereafter, Congress joined this new constitutional interpretation of privacy in light of technology. Responding to *Katz* and *Berger*, Congress regulated the use of wiretaps by passing the Wiretap Statute under Title III of the 1968 Omnibus Crime Control and Safe Streets Act.[23] By doing so, Congress expanded the limited protection of the Communications Act and effectively created a statutory right of privacy in "aural" communications — now applied also to state officials and private parties.[24] This new wiretap statute was drafted to apply to telephones, making it illegal for law enforcement agencies to wiretap them lacking a warrant.[25] Notably, in the years to follow, Congress further regulated wiretapping in foreign intelligence investigations under the rubric of national security.[26]

---

[21] *See* Katz v. United States, 389 U.S. 347, 351 (1967) (ruling that warrantless electronic bugging, even when conducted in a public telephone booth, is illegal, while establishing the doctrine of "legitimate expectation of privacy" as later interpreted in Smith v. Maryland, 442 U.S. 735, 740 (1979)). It should be also noted that in 1961, the Supreme Court held that evidence obtained in violation of the Fourth Amendment in criminal proceedings was excluded from evidence. *See* Mapp v. Ohio, 367 U.S. 643, 655 (1961); Solove, *A Brief History*, *supra* note 7, at 22.

[22] *See Berger*, 388 U.S. at 43-48.

[23] *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82. Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2510-22 (2012)); Susan Landau, *National Security on the Line*, 4 J. TELECOMM. & HIGH TECH. L. 409, 409-10, 414 (2006); Daniel J. Solove*, Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 754 (2005).

[24] *See* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1561 (2004); Solove, *A Brief History*, *supra* note 7, at 23.

[25] *See* 18 U.S.C. §§ 2510-2522 (2019); Mulligan, *supra* note 24, at 1561. For the list of offenses which wiretapping could be approved for, see 18 U.S.C. § 2516 (2019).

[26] *See* Landau, *supra* note 23, at 409-10, 414. Realizing that criminal investigations are only part of the wiretapping equation, Congress further regulated the use of wiretaps in foreign intelligence investigations within the rubric of national security in 1978 under the Foreign Intelligence Surveillance Act ("FISA"). Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978). Generally, FISA sets rules for electronic surveillance of agents of foreign powers. *See id.* It was further amended several times, and perhaps most notably in the 9/11 aftermath when Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools

Technological changes began to play a substantial role within the need to allow enforcement agencies to properly perform their mandate while also accounting for the potential impact of operating in legal grey zones on human rights and liberties, such as the right to privacy. Subsequently, the growth of computer technology led to further reconstruction of Title III in 1986.[27] The Electronic Communications Privacy Act ("ECPA")[28] revised the Wiretap Act,[29] while adding two further acts to deal with new technological developments: The Stored Communications Act ("SCA"), regulating access to both the content and metadata stored by electronic communications services,[30] and the Pen Register Act, regulating devices that obtain information about calls.[31] Among other things, the ECPA prohibited the "interception and disclosure of wire, oral, or electronic communications."[32] With exceptions, enforcement agencies were generally prohibited from intercepting, endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.[33]

Required to Intercept and Obstruct Terrorism Act ("PATRIOT Act"). *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended at scattered sections of the U.S.C. (2012)); Niva Elkin-Koren & Eldar Haber, *Governance by Proxy: Cyber Challenges to Civil Liberties*, 82 BROOK. L. REV. 105, 143-45 (2016). For more on wiretapping in the context of national security, see generally Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 607 (2003) [hereinafter *Internet Surveillance Law*].

[27] David W. Opderbeck, *Encryption Policy and Law Enforcement in the Cloud*, 49 CONN. L. REV. 1657, 1659 (2017); *see* Timothy Casey, *Electronic Surveillance and the Right to Be Secure*, 41 UC DAVIS L. REV. 977, 1001 (2008).

[28] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986); *see* Landau, *supra* note 23, at 410.

[29] This revision has, *inter alia*, extended privacy protections to "electronic" communications and broadened the scope of "wire" and "oral" communications under the Act. *See* Pikowsky, *supra* note 17, at 39-41.

[30] Among other requirements, the Stored Communications Act makes it illegal for someone to, without permission, obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage. *See* 18 U.S.C. §§ 2701-2712 (2019).

[31] *See id.* §§ 3121-3126. Since its enactment, the pen register and trap and trace statute has been expanded beyond telephones, and now includes dialing, routing, addressing, and signaling information of communications, including dialed calls, IP addresses, and email headers. *See* U.S. DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 51 (2018), https://www.justice.gov/ag/page/file/1076696/download [hereinafter AG'S CYBER DIGITAL TASK FORCE].

[32] *See* 18 U.S.C. § 2511.

[33] *See id.* § 2511(1)(a).

When the internet became public, further challenges to law enforcement agencies arose. Prior to the internet, wiretapping statutes were directed towards the government's ability to intercept telephone calls in real time; but with the rise of the internet, the traditional meaning of telephones was changing, and enforcement agencies were unable to implement electronic surveillance court orders, as some service providers did not have the tools to comply with them.[34] Responding to such problems, the Clinton Administration promoted the implementation of what was known as a Clipper Chip — a device that secures voice and data messages and allows law enforcement agencies to decode these messages when necessary.[35]

Congress eventually chose a different path. It reacted to these challenges by requiring telecommunications companies to modify their digital infrastructure so that enforcement agencies could wiretap their networks upon a legal order. Under the Communications Assistance for Law Enforcement Act ("CALEA"),[36] telecommunications carriers were required to "ensure that their equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of facilitating lawful orders for wiretaps and call identifying information."[37] Upon following certain standards — expected to reduce the amount of non-executing wiretaps warrants — service providers will be protected by a "safe-harbor."[38]

Along with technological innovations, such as voice communications over the internet, the Federal Communications Commission ("FCC") further expanded CALEA in 2005 to include Voice over IP ("VoIP") communication. The impact of such expansion was that wiretapping capabilities were required to be implemented into communications networks and not merely telephones.[39] Still, this amendment was rather

[34] *See Network Wiretapping Capabilities: Hearing on H.R. 4922 Before the Subcomm. on Telecomms. & Fin. of the H. Comm. on Energy & Commerce*, 103d Cong. 74 (1994) (statement of Louis J. Freeh, FBI Director); Landau, *supra* note 23, at 418.

[35] For more on the Clipper Chip, see generally A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution,* 143 U. PA. L. REV. 709 (1995) (discussing the Clipper Chip in the context of the Constitution and national security).

[36] *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended at 47 U.S.C §§ 1001-10 (2019)); *see also* Landau, *supra* note 23, at 410.

[37] 47 U.S.C. § 1002(a) (2019).

[38] *See id.* § 1006(a)(2).

[39] *See* Am. Council on Educ. v. FCC, 451 F.3d 226, 227 (D.C. Cir. 2006) (upholding an FCC regulation extending CALEA to VoIP); A. Michael Froomkin,

a narrow one. It only applied on some entities and failed to include several other types of internet communication.[40] One of the reasons for such limitations was that internet infrastructure raised difficulties in implementing any real-time interception, and furthermore, it was almost entirely comprised of written communication, rather than oral or visual.[41] Thus, while CALEA was designed, *inter alia*, to preserve the government's ability to conduct wiretaps,[42] currently most internet communications providers are generally excluded from CALEA requirements.

All in all, the history of access to communications shows that human rights and liberties slowly became part of the law enforcement equation.[43] First crafted by state legislators, followed years later by courts and Congress, policymakers acknowledged that it would be unlawful for enforcement agencies to conduct some types of surveillance without judicial scrutiny. At the same time, CALEA's expansion in 2005 could indicate a moment when policymakers ceased to further regulate access to communication for regular law

Lessons Learned Too Well: Anonymity in a Time of Surveillance, 59 ARIZ. L. REV. 95, 110-11 (2017) [hereinafter *Lessons Learned*]; Landau, *supra* note 23, at 410.

[40] *See* Christa M. Hibbard, *Wiretapping the Internet: The Expansion of the Communications Assistance to Law Enforcement Act to Extend Government Surveillance,* 64 FED. COMM. L.J. 371, 375 (2012).

[41] Notably, internet users could also use other forms of communication like microphones and cameras, but these forms would most likely be the exception rather than the rule.

[42] *See* H.R. REP. NO. 103-827, at 17-18 (1994); *see also* Michael A. Rosow, Note, *Is "Big Brother" Listening? A Critical Analysis of New Rules Permitting Law Enforcement Agencies to Use Dialed Digital Extraction*, 84 MINN. L. REV. 1051, 1058-60 (2000).

[43] By nature, access to data is closely tied with many human rights and liberties, including the right to privacy. Generally, both federal and state laws could impose obligations on governmental entities for obtaining data and the use of their own data; and also on the private sector regarding when to facilitate governmental investigations and data retention in some contexts. In the context of privacy, see, e.g., The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a (2019)) which regulates certain kinds of collection and use of records by certain federal agencies (but excludes the private sector, state and local agencies); The Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a (2019); The Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, tit. XXX, 108 Stat. 2099 (codified at 18 U.S.C. §§ 2721-2725 (2019)) which regulates the states authority to disclose personal driver records by prohibiting, with exceptions, the disclosure or sale of driver's records without obtaining prior consent from the individual. *See* Solove, *A Brief History*, *supra* note 7, at 29, 37. Such form of regulation could address specific industries or relate broadly to any entity. *See, e.g.*, Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114-15 (1970) (mandating federally insured banks and other financial institute to aggregate financial data and reports in order to assist law enforcement agencies to conduct financial investigations).

enforcement purposes (not accounting for national security). While enforcement agencies and other interested parties sought to introduce legislation that allows them to intercept online communications in real time, currently the regulatory framework might not support such desires.[44]

Technology, however, did not stop evolving and might alter the ways enforcement will be commenced, affecting, *inter alia*, the enforcement-privacy conundrum. As the regulatory framework was constructed to properly balance between the necessity of enforcement and individuals' civil rights and liberties, and as technology was responsible for the need for such protection, newest technology forms must be further analyzed to examine whether this regulatory framework still properly balances such equation.

B. The Evolution of the Internet of Things and Always-on Devices

Digital technology changed the way society connects. The public inception of the internet offered individuals a platform to communicate with each other and share their thoughts, music, videos, or almost any other content they desire. Soon thereafter, non-traditional computers, like mobile phones, also became connected to the internet. What first started as simply browsing the internet through mobile phones eventually led to a so-called "smartification" movement, enabling cellphones to rely on the internet more — now relabeled "smartphones."[45]

These developments, however, now extend far beyond smartphones. They include a variety of devices that are connected to the internet and are capable of receiving and transmitting data. These "smart" objects could include houses, vehicles, TVs, refrigerators, wearables, toys, and computerized personal assistants, to name but a few examples.[46] In what is commonly referred to as the *Internet of Things* or IoT, almost any regular object — or more simply stated, "things" — now became

[44] *See* Ellen Nakashima, *Proposal Seeks to Fine Tech Companies for Noncompliance with Wiretap Orders*, WASH. POST (Apr. 28, 2013), https://www.washingtonpost.com/world/national-security/proposal-seeks-to-fine-tech-companies-for-noncompliance-with-wiretap-orders/2013/04/28/29e7d9d8-a83c-11e2-b029-8fb7e977ef71_story.html?utm_term=.0afc13511eff.

[45] For a brief history of smartphones, see Adam Pothitos, *The History of the Smartphone*, MOBILE INDUS. REV. (Oct. 31, 2016), http://www.mobileindustryreview.com/2016/10/the-history-of-the-smartphone.html.

[46] For a full taxonomy of IoT devices, see Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 98-117 (2014).

internetworking, while enabling individuals to be constantly connected and control these things digitally from afar.

IoT consists of a world of devices, not necessarily akin to each other. Some are rather simple, while others are sophisticated. Some are portable, while others are stationary. Some are equipped with few sensors, while others with many. In addition to these potential differences, not all devices necessarily operate in a similar manner, and thus their analysis requires a brief taxonomy: Some IoT devices require physical activation, while others operate in an "always-ready" mode, constantly awaiting a trigger phrase, or an "always-on" mode, constantly receiving and transmitting data. For the purposes of this Article, since always-ready devices must also constantly be on while awaiting the trigger phrase, both types will be jointly referred to as always-on devices.[47]

There are various examples of always-on devices, such as TVs,[48] video game consoles,[49] and children's toys.[50] Another example is that of wearable IoT devices or smart activity trackers that include many types of devices that monitor body activity of some sort and will usually be always-on by their nature. Some of them, like Fitbit, focus on health and fitness.[51] These wearables could be equipped with various sensors

[47] While accounting for their differences, both always-ready and always-on devices could essentially be considered as always-on. Even if they simply await a trigger phrase, the fact that always-ready devices must await the phrase necessitates constantly being on. Notably, always-on devices existed prior to the IoT. Stacey Gray suggested to term these devices microphone-enabled devices. The traditional type of always-on devices are security cameras that transmit data. *See* STACEY GRAY, FUTURE OF PRIVACY FORUM, ALWAYS ON: PRIVACY IMPLICATIONS OF MICROPHONE-ENABLED DEVICES 3-6 (2016); Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1939 (2017).

[48] A known example is that of Samsung's Smart TV. *See* Darren Orf, *Samsung's SmartTV Privacy Policy Raises Accusations of Digital Spying*, GIZMODO (Feb. 8, 2015, 2:30 PM), http://gizmodo.com/samsungs-smart-tv-privacy-policy-raises-accusations-of-1684534051.

[49] *See* John Keilman, *Is My Xbox Spying on Me?*, CHI. TRIB. (Jan. 1, 2016, 2:00 AM), http://www.chicagotribune.com/news/ct-toys-online-spying-keilman-hf-0106-20160101-column.html.

[50] While some, like Hello Barbie, require physical activation, other toys, like My Friend Cayla, operate in an always-on mode. *See* Katie Lobosco, *Talking Barbie is Too 'Creepy' for Some Parents*, CNN MONEY (Mar. 12, 2015, 4:11 PM), http://money.cnn.com/2015/03/11/news/companies/creepy-hello-barbie; Iain Thomson, *Hello Barbie: Hang on, This Wi-Fi Doll Records Your Child's Voice?*, REGISTER: PERSONAL TECH (Feb. 19, 2015, 7:39 AM), http://www.theregister.co.uk/2015/02/19/hello_barbie; *This is Cayla*, MY FRIEND CAYLA, https://www.myfriendcayla.com/meet-cayla-c8hw (last visited Feb. 1, 2019).

[51] Scott Peppet lists five basic types of personal health monitors: (1) countertop devices (such as a blood-pressure monitor or weight scale); (2) wearable sensors (such

that would ultimately monitor heart rate, steps, sleeping patterns, and other vital signs.[52] Other wearables are marketed as a safety device, such as children's GPS watches or wearables, designed to grant parents some form of control on their children's activity and location.[53]

One final example of always-on devices is computerized personal assistants, like Amazon Echo.[54] Much like other so-called "Alexa devices," this voice-activated speaker awaits a voice command such as "Alexa" or "Amazon" depending on the user's preferences,[55] constantly listening for commands. By now, there are various types of digital assistants, ranging from Amazon (Alexa devices), Google (Google

as an arm or wrist band); (3) intimate contact sensors (such as a patch or electronic tattoo); (4) ingestible sensors (such as an electronic pill); and (5) implantable sensors (such as a heart or blood health monitor). *See* Peppet, *supra* note 46, at 98. Notably, IoT and Health literally became closely connected much beyond wearables. Pacemakers and insulin pumps became connected to the internet, along with other medical devices. These devices could include, *inter alia*, cardiac event monitors, electronic diaries for clinical trials, and smart-inhalers for people with asthma. IoT has even expanded further to medical assistance with the invention of "smart pills" which could, by the use of a wireless chip on a prescription bottle, send reminders of pill consumption and even coordinate refills with the doctor. *See* Hillary Brill & Scott Jones, *Little Things and Big Challenges: Information Privacy and the Internet of Things*, 66 AM. U. L. REV. 1183, 1191 (2017); Katherine E. Tapp, *Smart Devices Won't Be Smart until Society Demands an Expectation of Privacy*, 56 U. LOUISVILLE L. REV. 83, 84 (2017); Nissa Simon, *Technology Puts You in Charge of Your Health*, AARP (Sept. 23, 2013), http://www.aarp.org/health/healthy-living/info-09-2013/health-gadgets.html.

[52] Fitbit, for instance, monitors steps and could provide insights, *inter alia*, on individual's heart rate or the quality of sleep. *See* ANDREW HILTS, CHRISTOPHER PARSONS & JEFFREY KNOCKEL, EVERY STEP YOU FAKE: A COMPARATIVE ANALYSIS OF FITNESS TRACKER PRIVACY AND SECURITY, OPEN EFFECT REP. 3-7 (2016), https://openeffect.ca/reports/Every_Step_You_Fake.pdf.

[53] *See* Rebecca Edwards, *The Best Kids GPS Trackers and Wearables*, SAFEWISE, https://www.safewise.com/resources/wearable-gps-tracking-devices-for-kids-guide (last updated Aug. 26, 2019).

[54] Amazon Echo is "a hands-free speaker you control with your voice." It "connects to the Alexa Voice Service to play music, make calls, send and receive messages, provide information, news, sports scores, weather, and more — instantly. All you have to do is ask. Echo has seven microphones and beam forming technology, so it can hear you from across the room — even while music is playing. Echo is also an expertly tuned speaker that can fill any room with 360° immersive sound. When you want to use Echo, just say the wake word "Alexa" and Echo responds instantly. If you have more than one Echo or Echo Dot, Alexa responds intelligently from the Echo you're closest to with ESP (Echo Spatial Perception)." *Amazon Echo*, AMAZON, https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E (last visited Feb. 1, 2019).

[55] *See Change the Wake Word*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201971890 (last visited Feb. 1, 2019).

Home) and Apple (HomePod), to name but a few key market players.[56] This technology is now also becoming more embedded into various devices. Alexa is now integrated into the infotainment systems of many cars, like BMW and Mini models.[57] Many TVs will soon also have personal assistants like Alexa and its like.[58] Digital assistants have also entered the children's market via the Echo Dot "Kids Edition,"[59] and potentially, they might also be available for children soon via the Hello Barbie Hologram — a box with an animated projection of Barbie that responds to voice commands.[60]

Essentially, IoT enables users to be constantly connected to the internet through various means. But while these technological developments have various benefits and could potentially improve their

[56] There are many types of computerized personal assistants, including Apple's Siri and Microsoft's Cortana. *See Top 22 Intelligent Personal Assistants or Automated Personal Assistants*, PREDICTIVE ANALYTICS TODAY, http://www.predictiveanalyticstoday.com/top-intelligent-personal-assistants-automated-personal-assistants/#content-anchor (last visited Feb. 1, 2019).

Google introduced such a technology in 2014, under a pre-installed ability in Google's Chrome browser which passively listened for the words "OK, Google" to launch a voice-activated search function. They later introduced a device akin to Amazon Echo, named Google Home: "Meet the Google Home family of devices. On call, 24/7. Ask your Google Assistant questions. Tell it to do things. It's your own Google, always ready to help." *Google Nest Speakers & Displays*, GOOGLE SUPPORT, https://support.google.com/googlenest/answer/7029281?hl=en (last visited Oct. 8, 2019).

Following this path, Apple introduced the HomePod. *Get to Know Google Home*, GOOGLE HOME, https://madeby.google.com/home (last visited Feb. 1, 2019). *Accord* Tony Bradley, *'OK Google' Feature Removed From Chrome Browser*, FORBES (Oct. 17, 2015, 10:48 AM), http://www.forbes.com/sites/tonybradley/2015/10/17/ok-googlefeature-removed-from-chrome-browser/#16d299a44e27; *The New Sound of Home*, APPLE, https://www.apple.com/homepod (last visited Feb. 1, 2019) [https://perma.cc/ZCR8-WM9T].

[57] *See* Alistair Charlton, *Which Cars Have Amazon Alexa Integration? Updated for 2019*, GEARBRAIN (Apr. 29, 2019), https://www.gearbrain.com/which-cars-have-amazon-alexa-2525958778.html.

[58] *See* Jefferson Graham, *Yes Alexa, We'll be Seeing a Lot More Talking TVs This Year*, USA TODAY (Apr. 21, 2018, 11:17 AM), https://www.usatoday.com/story/tech/talkingtech/2018/04/21/yes-alexa-well-seeing-lot-more-talking-tvs-year/538986002.

[59] *See* Dan Seifert, *Amazon's New Echo Dot Kids Edition Comes With a Colorful Case and Parental Controls*, VERGE (Apr. 25, 2018, 7:25 AM), https://www.theverge.com/2018/4/25/17276164/amazon-echo-dot-kids-edition-freetime-price-announcement-features-specs.

[60] *See* Tim Moynihan, *So, Barbie's a Hologram Now. Oh, and She Responds to Your Voice*, WIRED (Feb. 17, 2017), https://www.wired.com/2017/02/hello-barbie-hologram-matell. Notably, however, Hello Barbie's future (along with the hologram) lies in uncertainty as Apple recently acquired Pullstring — the company that was in charge of Hello Barbie voice analysis. *See* Brain Raftery, *Apple Acquires Voice-Tech Company Behind 'Hello Barbie,'* FORTUNE (Feb. 15, 2019), https://fortune.com/2019/02/15/apple-acquires-pullstring-voice-technology.

users' lives,[61] they could also bear a high cost in terms of individuals' privacy, among other human rights and liberties. They can collect and store mass amounts of data on their users and potentially could also be accessed in real time. While a goldmine for enforcement agencies, a move towards wiretapping IoT or using its acquired data requires further scrutiny in light of the civil rights and liberties that might be jeopardized.[62]

II. LAW ENFORCEMENT AND THINGS

The impact of technology on law enforcement and privacy was evident throughout history. New communication technologies meant improving existing investigatory capabilities for law enforcement agencies. While the internet marked a huge step in data mining capabilities, IoT might take them a step further. It opens a world of possibilities to engage in investigatory and surveillance practices that could potentially capture almost any conversation by any individual at any given time. It could also capture much more than mere conversations, like location, imagery, and live videos. Such a world awash with sensors enables law enforcement agencies to engage in rather new wiretapping practices by accessing the data acquired by the devices or remotely connecting to these devices and activating them without the user's awareness.

To understand these new technologies under the current regulatory framework that enables access to stored communications and wiretapping while providing safeguards for privacy, this Part will be divided into three Sections. Section A discusses the potential use of IoT

[61] IoT devices could be beneficial for both society and individuals. IoT thermostats, for instance, can improve energy efficiency and thus promote social goals. Many IoT devices could, *inter alia*, make everyday tasks more convenient and also potentially improve the lives of many individuals, like those with physical disabilities. Smart toys ("IoToys") can be enjoyable and even potentially assist in the overall education and cognitive development of children. In the near future, devices would be able to even analyze voices and detect whether individuals are stressed (and analyze the source of such stress) or even detect whether we are in danger and contact emergency services. *See, e.g.*, COMM. ON COMMERCE, SCI. & TRANSP., 114th CONG., CHILDREN'S CONNECTED TOYS: DATA SECURITY AND PRIVACY CONCERNS 1-3 (Comm. Print 2016) (Sen. Bill Nelson); GRAY, *supra* note 47, at 3, 10; David Talbot, *The Era of Ubiquitous Listening Dawns*, MIT TECH. REV. (Aug. 8, 2013), http://www.technologyreview.com/news/517801/the-era-of-ubiquitous-listening-dawns.

[62] While this Article focuses on the right to privacy, the consequences of poorly regulated legal framework for data access in IoT might affect civil rights and liberties like freedom of speech, freedom of association and other democratic values. *See, e.g.*, Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 436-37 (2008).

devices by enforcement agencies. Section B discusses access to communications and wiretapping and whether the digital age and the current regulatory framework support such practices. Section C questions whether practical and normative limitations would serve as a barrier to enable wiretapping and access to stored communications in IoT, setting the grounds for a following normative evaluation in Part III.

A. Wiretapping and the Datafication of Things

IoT, and perhaps most importantly, always-on devices, could mark a paradigm shift in the collection and retention of data. Potentially, always-on devices could harvest data at any given time, independently of the active use of their users. To put it differently, these devices are capable of recording and transmitting data without physical activation and without the knowledge of their users. They can use their embedded microphones, sensors, and cameras to constantly collect the data of their users, and the companies that operate them could make use of such data as long as it is permissible under their terms of service or end-user license agreements.[63]

The types and variety of data collected from IoT devices could be enormous. Some smart TVs, for instance, would track their viewers' habits, transmit the names of files on USB drives connected to the TV, and capture data from networks to which they are connected.[64] Wearable IoT devices or smart activity trackers could monitor various types of data, such as heart rate, sexual activity, sleep patterns, steps taken, calorie consumption, and geolocation.[65] Many household meters

[63] For more on licensing of IoT objects, see generally Christina M. Mulligan, *Personal Property Servitudes on the Internet of Things*, 50 GA. L. REV. 1121 (2016).

[64] Vizio smart TVs were found to be tracking viewing habits and sharing it with third parties. *See* Ms. Smith, *Vizio Tracks What 10 Million Smart TV Owners' Watch, Sells Data to Advertisers*, CSO (Nov. 11, 2015, 11:12 AM), https://www.csoonline.com/article/3004552/security/vizio-tracks-what-10-million-smart-tv-owners-watch-sell-data-to-advertisers.html. Eventually, "Vizio ha[d] agreed to pay $2.2 million to settle the charges by the FTC." Ms. Smith, *Vizio to Pay $2.2 Million for Spying on What Customers Watch Without Consent*, CSO (Feb. 7, 2017, 8:18 AM), https://www.csoonline.com/article/3166373/security/vizio-to-pay-2-2-million-for-spying-on-what-customers-watch-without-consent.html. WikiLeaks has reported that the CIA used Samsung's Smart TV to spy on their users. *See* Craig Timberg, Elizabeth Dwoskin & Ellen Nakashima, *WikiLeaks: The CIA is Using Popular TVs, Smartphones and Cars to Spy on Their Owners*, WASH. POST (Mar. 7, 2017, 6:15 PM), https://www.washingtonpost.com/news/the-switch/wp/2017/03/07/why-the-cia-is-using-your-tvs-smartphones-and-cars-for-spying/?utm_term=.095c9b24a645.

[65] For further reading on smart activity trackers, see generally Katharine Saphner, Note, *You Should Be Free to Talk the Talk and Walk the Walk: Applying* Riley v. California *To Smart Activity Trackers*, 100 MINN. L. REV. 1689, 1689-93, 1715 (2016).

could enable the collection of distinct time-stamped data that could reveal a great deal on individuals' lives, such as their daily schedules, whether they use certain types of medical equipment, and even whether they have been growing marijuana.[66]

Other devices could capture even more data. Always-on TVs, for instance, could listen to, record, and send what is caught in the microphone to a third party,[67] and even turn on cameras, when those are built within the TV.[68] Smartphones could enable information gathering by cellular providers (tracking information about their users, like whom they communicate with and their locations); software providers like Google (Android), Apple (iOS), and Microsoft (Windows) could be aware of many actions their users perform on their phones;[69] and smart phone application ("app") developers could obtain valuable data of a user, from her contact list, to tracking her location, and viewing any content present on the device.[70]

Always-on devices that are equipped with sensors could theoretically capture all data in the vicinity of these sensors, depending on the type of data that the sensor could capture. Some devices, like the Nest Cam and other wearables, will constantly record and transmit data until manually turned off.[71] Other devices, like Amazon Echo and Google Home, will record any conversation that was made following the use of

[66] Law enforcement agencies have used user utility data obtained through smart energy meters to detect whether suspects have been growing marijuana in their homes. Jack I. Lerner & Deirdre K. Mulligan, *Taking the "Long View" of the Fourth Amendment: Stored Records and the Sanctity of the Home,* 2008 STAN. TECH. L. REV. 3, 3 (2008) (discussing how power consumption information could reveal personal information about individuals); Perry Chiaramonte, *Is Your Home's Energy Meter Spying on You?*, FOX NEWS (Apr. 17, 2014), https://www.foxnews.com/us/is-your-homes-energy-meter-spying-on-you. For further reading on smart meters, see generally Cheryl Dancey D. Balough, *Privacy Implications of Smart Meters*, 86 CHI.-KENT L. REV. 161 (2011); Megan McLean, *How Smart is Too Smart?: How Privacy Concerns Threaten Modern Energy Infrastructure*, 18 VAND. J. ENT. & TECH. L. 879 (2016); Sonia K. McNeil, Note, *Privacy and the Modern Grid,* 25 HARV. J.L. & TECH. 199 (2011).

[67] *See* April Glaser, *Philip K. Dick Warned Us About the Internet of Things in 1969*, SLATE (Feb. 10, 2015, 5:27 PM), http://www.slate.com/blogs/future_tense/2015/02/10/philip_k_dick_s_1969_novel_ubik_on_the_internet_of_things.html.

[68] *See* Joseph Steinberg, *These Devices May Be Spying on You (Even in Your Own Home)*, FORBES (Jan. 27, 2014), http://www.forbes.com/sites/josephsteinberg/2014/01/27/these-devices-may-be-spying-on-you-even-in-your-own-home/#15407ce56376.

[69] *Id.*

[70] *See, e.g.*, Neil McAllister, *How Many Mobile Apps Collect Data on Users? Oh . . . Nearly All of Them*, REGISTER (Feb. 21, 2014, 9:15 AM), http://www.theregister.co.uk/2014/02/21/appthority_app_privacy_study.

[71] *See Nest Cam Indoor,* NEST, https://nest.com/cameras/nest-cam-indoor/overview (last visited Feb. 1, 2019).

the trigger phrase. But there is no certainty if these devices constantly record content beyond what is recorded after an activation of the device.[72] What is evident, however, is that always-on devices like Amazon Echo and Google Home certainly record conversations following their activation and that the data is stored, perhaps indefinitely, on the companies' servers.[73]

There should be little doubt that the data acquired from IoT devices, whether real-time or stored, could be valuable for criminal enforcement purposes.[74] These devices potentially obtain mass amounts of data on users and could subsequently aid law enforcement agencies in detecting unlawful activity, provide important evidence for investigations, and

[72] Currently, both Amazon and Google declare that they store voice recordings from users only after they are intentionally triggered. Otherwise, these devices are in passive listening mode, recording a fraction of ambient sound, hunting for the acoustic signature of their wake words and then constantly overwriting and discarding that fraction of sound. Furthermore, Google specifically mentions: "Google Home listens in short (a few seconds) snippets for the hotword. Those snippets are deleted if the hotword is not detected, and none of that information leaves your device until the hotword is heard." *More About Data Security and Privacy on Devices that Work with Assistant*, GOOGLE SUPPORT, https://support.google.com/googlehome/answer/7072285?hl=en (last visited Feb. 1, 2019) [https://perma.cc/TU4J-3GAU]; *accord* Sharon Gaudin, *How Google Home's 'Always On' Will Affect Privacy?*, COMPUTERWORLD (Oct. 6, 2016, 12:15 PM), http://www.computerworld.com/article/3128791/data-privacy/how-google-homes-always-on-will-affect-privacy.html; Sapna Maheshwari, *Hey, Alexa, What Can You Hear? And What Will You Do With It?*, N.Y. TIMES (Mar. 31, 2018), https://www.nytimes.com/2018/03/31/business/media/amazon-google-privacy-digital-assistants.html?action=click&module=Intentional&pgtype=Article; Hamza Shaban, *Two Senators Want Amazon's Jeff Bezos to Answer for Alexa's Eavesdropping*, WASH. POST (June 15, 2018, 9:13 AM), https://www.washingtonpost.com/news/the-switch/wp/2018/06/15/two-senators-want-amazons-jeff-bezos-to-answer-for-alexas-eavesdropping/?noredirect=on&utm_term=.300f0820ef42; Brad Stone, *Is Alexa Really Eavesdropping on You?*, BLOOMBERG (Dec. 11, 2017, 4:00 AM), https://www.bloomberg.com/news/articles/2017-12-11/is-alexa-really-eavesdropping-on-you-jb25c6vc. In one instance, it was reported that an Echo device silently sent recordings to the caller without the family's permission or knowledge of the recording itself. For further reading on this topic, see generally Geoffrey A. Fowler, *Hey Alexa, Come Clean About How Much You're Really Recording Users*, CHI. TRIB. (May 25, 2018, 9:15 AM), https://www.chicagotribune.com/business/ct-biz-alexa-recording-20180525-story.html.

[73] *See* Bree Fowler & Mae Anderson, *Shhh, Your Washing Machine Might Overhear You*, AP NEWS (Jan. 5, 2017), https://www.apnews.com/0e6b40f214b74023be798a4351d9fd85; *Set Up Your Amazon Echo (1st Generation)*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201601770 (last visited Feb. 1, 2019).

[74] *See* JONATHAN L. ZITTRAIN ET AL., DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE (2016) ("The audio and video sensors on IoT devices will open up numerous avenues for government actors to demand access to real-time and recorded communications.").

eventually be used in criminal proceedings. Moreover, as these devices could potentially enable real-time interception, enforcement agencies might seek to legally obtain a warrant to wiretap them in some instances — and turn them "on." But such access to data raises important normative questions that must be further scrutinized: First, does the current legal framework for obtaining both stored communications and wiretapping could be used for IoT devices? And second, does IoT technology — and more specifically always-on devices — make a difference regarding its potential use under the current regulatory framework?

B. Access to Communication and Wiretapping in the Age of IoT

1. Constitutional Protection

From a legal standpoint, one of the key questions regarding the legality of enforcement practices within the notion of privacy is whether the conduct falls within the protection afforded by the Fourth Amendment.[75] If so, it would generally be a constitutional violation if governmental agents obtained data, whether in real time or while the device is at rest, without a warrant and probable cause.[76]

The Fourth Amendment protects "persons, houses, papers, and effects" from unreasonable *searches and seizures*.[77] To know whether the data that could be obtained from IoT devices falls under this protection, one needs first to examine whether it is considered either a person, house, paper, or effect and whether search or seizure is conducted. IoT devices should generally meet the first requirement. The device itself should be labeled as an effect, as it considered an individual's personal property.[78] Many of these devices might also be protected under the rubric of a house, as they will be present within individuals' houses.

The more complex examination in this context would be to decide whether search or seizure is conducted when accessing data gathered by IoT devices. Under the famous *Katz* decision, the Fourth Amendment is applicable where people have a legitimate expectation of privacy.[79] *Katz* created a test to know whether or not an investigative

[75] *See* U.S. CONST. amend. IV.

[76] *See id.*

[77] *Id.*; Katz v. United States, 389 U.S. 347, 359 (1967).

[78] For more on IoT devices as effects, see Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 826-30 (2016).

[79] In *Katz*, Justice Harlan offered a twofold requirement to determine whether governmental conduct constitutes a search: that a person has exhibited a subjective

technique is legal: one must first decide whether the conduct constitutes a search, as otherwise it would lack constitutional protection.[80] A search is conducted if the conduct violates a reasonable expectation of privacy, that is, both subjectively (whether an actual expectation of privacy exists) and objectively (whether that expectation is one that society is prepared to recognize as "reasonable").[81] If a search is conducted, then law enforcement agencies are required to obtain a warrant in most instances,[82] unless a specific exception for the need of such warrant exists.[83]

expectation of privacy and that the expectation be one that society is prepared to recognize as "reasonable." *Katz*, 389 U.S. at 361 (1967) (Harlan, J., concurring).

[80] *See id.* at 353; Riley v. California, 573 U.S. 373, 381-82 (2014); William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1829 (2016); Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 581-82 (2017).

[81] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring); Smith v. Maryland, 442 U.S. 735, 740 (1979). Still, one of the challenges that is greatly debated in court proceedings and academic literature is what constitutes as "reasonable." *See, e.g.*, Flippo v. West Virginia, 528 U.S. 11, 12, 15 (1999) (per curiam) (discussing reasonable expectation of privacy in a cabin at a state park); Minnesota v. Olson, 495 U.S. 91, 96-97 (1990) (holding that an overnight guest had a reasonable expectation of privacy in a host's home); Stoner v. California, 376 U.S. 483, 484 (1964) (warrantless search of a hotel room violates reasonable expectation of privacy); Henry F. Fradella et al., *Quantifying* Katz*: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 338-42 (2011).

[82] Notably, there is also a type of search which is undertaken for a non-law enforcement purpose. This "special needs" search could include the purpose of "ensuring the safety of railway passengers, maintaining a positive learning environment in schools, securing the country's borders," and anti-terrorism (when the search per se is not considered as a law enforcement purpose, e.g., when searching all airplane passengers). Ric Simmons, *The Mirage of Use Restrictions*, 96 N.C. L. REV. 133, 155-62 (2017); *see* Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 633-34 (1989); New Jersey v. T.L.O., 469 U.S. 325, 347-48 (1985); United States v. Martinez-Fuerte, 428 U.S. 543, 566-67 (1976).

[83] These exceptions could include, *inter alia*, exigent circumstances, consensual searches, the Terry stop and frisk search (which requires reasonable suspicion rather than probable cause), items that are in plain view during their searches, provided that officers encounter this evidence during their authorized search and that the incriminating nature of the evidence is "immediately apparent" and airport and courthouse searches. *See* Maryland v. Macon, 472 U.S. 463 (1985); Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971); Terry v. Ohio, 392 U.S. 1 (1968) (holding that the Fourth Amendment is not violated for the purposes of a frisk search, when the officer has a reasonable suspicion that the person has committed, is committing, or is about to commit a crime and has a reasonable belief that the person may be armed and presently dangerous). *See generally* Benjamin T. Clark, *Why the Airport and Courthouse Exceptions to the Search Warrant Requirement Should Be Extended to Sporting Events*, 40 VAL. U. L. REV. 707, 715-23 (2006) ("In carving out exceptions to the warrant requirement, courts generally engage in a tripartite weighing of public necessity, efficacy of the search, and degree of the intrusion."). Moreover, when deciding whether

Assuming that these search warrant exceptions would not generally apply to IoT devices, one must begin with the subjective component of the test: do individuals that communicate with IoT devices expect that their data would be shielded from outside scrutiny? While this subjective test is difficult to evaluate, generally the answer to this question should be in the affirmative. When one communicates with Alexa to make orders, play songs, or ask questions, it is fairly reasonable to assume that one does not expect that such data will be made public. The question might become more challenging when the IoT device is not located within the house but rather worn on an individual's body. Some data obtained from an IoT wearable, for instance, worn when an individual decides to go for a run, might subjectively not be perceived as shielded from outside scrutiny, like the distance of the run. Other types of data, like vital signs, might however receive such protection, as they would not be in public's plain view. Thus, the subjective test could rely on various elements, like that of the location of the device and the type of data gathered.

Under the objective part of this test, one must examine whether society is prepared to recognize that expectation as reasonable.[84] The objective test should generally lead to similar outcomes as the subjective one. The more IoT devices will become integral in our lives, more members of society will be willing to objectively consider their protection under the Fourth Amendment, as obtaining access to their data will reveal more of their personal and sensitive data. Courts have held that such expectation exists with letters, telephone calls, historical cellphone location records, and even emails.[85] IoT, as a form of

an individual is protected by the Fourth Amendment, Courts have focused, *inter alia*, on the location of the search or seizure. *See* Minnesota v. Carter, 525 U.S. 83, 90-91 (1998). For more on the plain view doctrine in the digital age, see generally Andrew Vahid Moshirnia, Note, *Separating Hard Fact from Hard Drive: A Solution for Plain View Doctrine in the Digital Domain*, 23 HARV. J.L. & TECH. 609 (2010).

[84] *See Smith*, 442 U.S. at 740.

[85] *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (holding that accessing historical records containing the physical locations of cellphones necessitates a search warrant); United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy . . . ."); *Smith*, 442 U.S. at 746 (Stewart, J., dissenting) ("[S]ince Katz[,] it has been abundantly clear that telephone conversations carried on by people in their homes or offices are fully protected by the Fourth and Fourteenth Amendments."); United States v. Warshak, 631 F.3d 266, 283-88 (6th Cir. 2010) (holding that an individual has a reasonable expectation of privacy in the contents of emails held by ISPs). While the Supreme Court had not tackled protection of emails under the Fourth Amendment directly, the decision in *Warshak* seems to be the prevailing view currently. *See, e.g.*, United States v. Ackerman, 831 F.3d 1292, 1307-08

commination and expression, should not generally receive different protection.

But there are exceptions to this test. The Fourth Amendment protection does not apply when individuals knowingly expose information to the public.[86] In this case, IoT devices might receive different protection depending on their location and use. As mentioned, communicating with Alexa within or outside one's house might alter the outcome of this analysis. Obtaining data from one's Fitbit worn outside one's house will depend on whether the data was exposed to the public (e.g., distance) or not (e.g., vital signs).

Another potential exception would be invoking the so-called *third-party doctrine*, which was established by the Supreme Court in the late 1970s and followed by the Court's interpretation of it in light of digital changes.[87] Under the third-party doctrine, there is no reasonable expectation of privacy when individuals share some types of information with a third party who is the intended recipient of the information.[88] Namely, these types of information include, *inter alia*, subscriber information, communications metadata (like IP address and telephone numbers),[89] bank records, motel registration, employment

(10th Cir. 2016); Vista Mktg., LLC v. Burkett, 812 F.3d 954, 969 (11th Cir. 2016). *But see, e.g.*, United States v. Graham, 824 F.3d 421, 437-38 (4th Cir. 2016); United States v. Carpenter, 819 F.3d 880, 887-89 (6th Cir. 2016).

[86] *See* California v. Greenwood, 486 U.S. 35, 39-42 (1988) (holding that a search of trash did not violate the Fourth Amendment). Another example is that of surveillance from an Aircraft. *See* California v. Ciraolo, 476 U.S. 207, 215 (1986).

[87] *See Carpenter*, 138 S. Ct. at 2217; Riley v. California, 573 U.S. 373, 386 (2014) (holding that warrantless search of an arrestee's cellphone was not a reasonable search); United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."); *Smith*, 442 U.S. at 745-46 (a telephone number dialed from the defendant's home was not within the Fourth Amendment's scope); United States v. Miller, 425 U.S. 435, 437-43 (1976) (holding that the Fourth Amendment's protections do not extend to copies of checks and deposit slips held by the defendant's banks). For more on the third-party doctrine, see generally Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 976 (2007); Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 374, 378 (2006); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563–64 (2009) [hereinafter *Third Party Doctrine*].

[88] *See supra* note 87 and accompanying text (discussing and applying the third-party doctrine).

[89] *See, e.g.*, United States v. Ulbricht, 858 F.3d 71, 94-98 (2d Cir. 2017); Mayer, supra note 80, at 596 n.90 (listing courts decisions on these issues).

information, and geolocation records;[90] Congress has placed limited restrictions on acquiring such data — all without a warrant.[91]

As for other types of content, even lacking a Supreme Court decision, it seems that at least some types of communication will receive Fourth Amendment protection not subjected to the third-party doctrine.[92] This would include contents of emails, text messages, and private content on a social network, to name but a few examples.[93] The *third-party doctrine* will also not apply if physical trespass is involved, i.e., the data is contained in personal digital devices, because in those cases a search is conducted.[94] Furthermore, even without physical trespass, if enforcement agencies use a device to intercept the IoT signals, which is analogous to practices held by the Court in the past to violate a reasonable expectation of privacy, it will not likely be constitutionally permissible.[95]

Generally, whether access to stored communications or wiretapping of IoT devices fall under the constitutional protection or its exceptions could be questionable. It would highly depend on the IoT in question and the data that is gathered, the interpretation of the reasonable expectation of privacy test, and whether the third-party doctrine applies. At best, the Fourth Amendment will likely apply to many instances in which law enforcement agencies will be required to comply with the Fourth Amendment search requirements when seeking communications content.[96]

---

[90] *See* Note, *supra* note 47, at 1931; Mayer, *supra* note 80, at 593.

[91] *See* 18 U.S.C. §§ 2703(c)(2), 2709 (2019); Mayer, *supra* note 80, at 593.

[92] *See, e.g.*, United States v. Warshak, 631 F.3d 266, 283-88 (6th Cir. 2010) (holding that an individual has a reasonable expectation of privacy in the contents of emails held by ISPs); *see also* Mayer, *supra* note 80, at 592.

[93] *See, e.g.*, *In re* Search of Info. Associated with the Facebook Acct. Identified by the Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 6-7 (D.D.C. 2013); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 906-09 (9th Cir. 2008); Mayer, supra note 80, at 595 n.87 (listing court's decisions on these issues).

[94] *See* Riley v. California, 573 U.S. 373, 386 (2014) (holding that tapping a suspect's phone is considered a search); Florida v. Jardines, 569 U.S. 1, 10-12 (2013) (holding that police use of drug-sniffing dogs is a search); United States v. Jones, 565 U.S. 400, 404-05 (2012) (holding that a physical trespass against a car constitutes a search). *See also* Mayer, *supra* note 80, at 594-95.

[95] *See* Kyllo v. United States, 533 U.S. 27, 34-35 (2001); Ferguson, *supra* note 78, at 838.

[96] *See* Payton v. New York, 445 U.S. 573, 586-90 (1980) (documenting the basic principle of Fourth Amendment law that protects the privacy of the home against intrusion); Ferguson, *supra* note 78, at 837.

But uncertainty lies here. The current interpretation of the Fourth Amendment requires adjustments to the digital age. As use of IoT devices will become more integral to our daily routine, regardless of the location of the device, a legitimate expectation of privacy should not be easily waived simply due to exceptions like that of the third-party doctrine, which becomes obsolete due to technological and social changes.

Even prior to such potential adaptions, protection of individuals' privacy does not stop with the Fourth Amendment. As mentioned, Congress regulated access to data in some instances; thus, access to stored IoT communications, or their real-time interception, might be protected by statutory requirements. As the next Subsection discusses, the lawfulness of the enforcement activity will be examined through the main regulatory framework related to obtaining data, i.e., the SCA and the Wiretap Act.[97]

2. Statutory Access to Stored Communications in IoT

While access to stored communications was regulated prior to the internet in 1986, these regulations have long been applied to the storage of online communications.[98] Thus, to obtain any IoT data that is stored on remote servers, the governmental agent must follow the procedural framework set by the SCA, i.e., he will be required to obtain a warrant, an administrative subpoena, or a court order pursuant to 18 U.S.C. § 2703(d).[99] If the data is considered as non-content communication — those that do not concern the substance, purport, or meaning of the communication — then such access might also be permissible with little judicial overview.[100]

---

[97] Notably, this Article focuses only on the federal level, while state laws could also impose various obligations on data access. *See, e.g.*, Electronic Communications Privacy Act, CAL. PENAL CODE §§ 1546.1-1546.4 (2019). *See generally* Sarit K. Mizrahi, *The Dangers of Sharing Cloud Storage: The Privacy Violations Suffered by Innocent Cloud Users during the Course of Criminal Investigations in Canada and the United States*, 25 TUL. J. INT'L & COMP. L. 303, 334-36 (2017).

[98] *See generally* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2109 (2009) (discussing the framework governing the surveillance of electronic communications while suggesting a framework that distinguishes content from envelope information).

[99] *See* 18 U.S.C. § 2703(b) (2019); United States v. Warshak, 631 F.3d 266, 283 (6th Cir. 2010).

[100] 18 U.S.C. § 2510(8) (2019); *see, e.g.*, Ilana R. Kattan, *Cloudy Privacy Protections: Why the Stored Communications Act Fails To Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. TECH. L. 617, 641 (2011); Mizrahi, *supra* note 97, at 332-

The applicability of the SCA to IoT service providers might not be as evident as one might think. To fall under the SCA, service providers must be classified as either an Electronic Communication Service ("ECS") or a Remote Computing Service ("RCS").[101] Simply to exemplify, ECS providers would generally include telephone companies and email service providers,[102] while RCS providers offer an off-site computer that stores or processes data for a customer, like Dropbox.[103]

Categorization as either an ECS or RCS could greatly affect the procedure — and thereby the level of privacy protection.[104] Beyond modest differences within the prohibitions on voluntary disclosure of the contents of electronic communication,[105] such classification would change the process. While for ECS, content information held in storage for 180 days or less is pursuant to a warrant,[106] RCS merely requires a notice to the user and a subpoena or a § 2703(d) specific and articulable

33. *See generally* William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1207-09 (2010).

101 *See* 18 U.S.C. § 2703(b)(2) (2019). An Electronic Communication Service is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *See id.* § 2510(15). Remote Computing Service is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." *See id.* § 2711(2).

102 *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 900-03 (9th Cir. 2008) (categorizing text messaging service provider is an ECS); S. REP. NO. 99-541 at 14 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3568; DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 117 (3d ed. 2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf [hereinafter SEARCHING AND SEIZING ELECTRONICS].

103 *See* DEP'T OF JUSTICE, SEARCHING AND SEIZING ELECTRONICS, *supra* note 102, at 119; *cf.* Eric R. Hinz, Note, *A Distinctionless Distinction: Why the RCS/ECS Distinction in the Stored Communications Act Does Not Work*, 88 NOTRE DAME L. REV. 489, 515 (2012) (noting that Dropbox could actually be considered as an ECS).

104 For more on distinctions between ECS and RCS, see generally Hinz, *supra* note 103.

105 For example, while an ECS cannot disclose communication in "electronic storage," RCS cannot disclose communication held by the service solely as storage or for computer processing. One notable difference is that providers of ECS must obtain the consent of the sender or the receiver of the communication, while a provider of RCS need only get consent of the subscriber to the service. *See* 18 U.S.C. §§ 2702(a)(1), 2702(b)(3), 2510(17)(B) (2019); Hinz, *supra* note 103, at 497-501.

106 *See* 18 U.S.C. § 2703(a). Beyond 180 days, the government can use an administrative subpoena, a grand jury subpoena, a trial subpoena, or a court order. *See id.* §§ 2703(a), 2703(b). Non-content information could be obtained without notice, pursuant to a warrant with § 2703(d) specific and articulable facts order or through the consent of the user. Some non-content communication, like the name of the user, telephone numbers or network addresses, and means of payment, such as credit card numbers, could be obtained pursuant to a subpoena to the network service provider. *See id.* §§ 2703(d), 2703(c)(1)(A)-(C); Hinz, *supra* note 103, at 499-500.

facts order showing reasonable grounds that the data is relevant and material to an ongoing criminal investigation.[107]

Aside from various variations, these rather outdated categories might not fit as clearly to IoT as one might think. Take digital personal assistants like Amazon Echo as an example. When examining the classifications of the SCA, one must first ask whether the Echo device allows its customers to send or receive wire or electronic communications while held in electronic storage — and thus should be treated as ECS. For most IoT, much like the Echo, the answer to this question will most likely be in the negative. While the communication will be deemed as electronic to satisfy the Act's requirements,[108] the stored data is neither "temporary and intermediate" nor "incidental to the electronic transmission" and is not meant to provide backup protection.[109] Storing data temporarily will most likely defeat the purposes of using these services, as they often rely on machine learning algorithms that require data, and due to the fact that data has become a business model for many service providers.[110]

If the IoT device is not labeled as an ECS, then one must examine whether it provides "computer storage or processing services by means of an electronic communication system" and thus should be labeled as RCS instead.[111] For that purpose, one might need to examine whether the data is stored "solely for the purpose of providing storage or computer processing services"[112] and whether the IoT service provider is not "authorized to access the contents of any such communications for purposes of providing any services other than storage or computer

[107] And with a RCS, even the notice may be delayed for up to ninety days if it would adversely affect a trial, and the government may seek to extend that period in 90-day increments. *See* 18 U.S.C. § 2705 (2019); United States v. Warshak, 631 F.3d 266, 291 (6th Cir. 2010); Hinz, *supra* note 103, at 501.

[108] Electronic communications are defined to mean nearly any form or style of communication, including "signs, signals, writings, images, sounds, data or intelligence of any nature." *See* 18 U.S.C. § 2510(12) (2019). That would include, for instance, email and instant messages. *See In re* United States for an Order Authorizing the Installation and Use of a Pen Register, 416 F. Supp. 2d 13, 18 (D.D.C. 2006); Quon v. Arch Wireless Operating Co., 309 F. Supp. 2d 1204, 1207-10 (C.D. Cal. 2004).

[109] *See* 18 U.S.C. § 2510(17) (2019).

[110] One example would be the use of contextual advertising which necessitates data storage. *See* Robison, *supra* note 100, at 1213-14.

[111] *See* 18 U.S.C. §§ 2510(14), 2711(2) (2019). Notably, the data must also be received electronically from the customer. *See id.* §§ 2702(a)(2)(A), 2703(b)(2)(A).

[112] *See id.* § 2702(a)(2)(B).

processing."[113] Going back to the example of the Echo device, such a classification will not likely apply as well. While the data could arguably be stored for the purpose of providing storage or computer processing services, it is highly questionable if Amazon is not authorized to access the contents for other reasons than storage or computer processing — especially when data is highly valuable for many companies as a business model.[114]

In other words, IoT is much more complex than these rather old categories. Several of these devices, like the Echo, are multifunctional.[115] They can operate similar to a search engine when a user asks Alexa questions, they can operate similar to an email provider when a user asks Alexa to send or read an email,[116] and they can even be used as a telephone or intercom-like service when communicating with other Echo users. Hence, it might not be the device itself — but rather the nature or specific use of it — that will eventually dictate whether and how the SCA applies.[117]

Aside from some exceptions set under the SCA for law enforcement purposes in some instances,[118] if the stored data from the IoT device is

[113] *See id.* In addition, the data must contain "content"; must be "carried or maintained . . . on behalf of . . . a subscriber or customer," and have been electronically transmitted to the provider. *See id.* § 2702(a)(2)(A).

[114] In this respect, Amazon claims that it "use[s] the information that you provide for such purposes as responding to your requests, customizing future shopping for you, improving our stores, and communicating with you." *See Amazon Privacy Notice*, AMAZON (Aug. 29, 2017), https://www.amazon.com/gp/help/customer/display.html?nodeId=201909010. Notably, a *Sun* investigation recently discovered that Amazon staff were actively listening to recordings of Echo users — allegedly to improve their services. *See* Nick Parker, *ALEXA, STOP BEING A PERV: Outrage as Amazon's Alexa Listens to Brits Having Sex, Rowing, Swearing and Sharing Medical News,* SUN (July 29, 2019), https://www.thesun.co.uk/tech/9611689/outrage-as-amazons-alexa-listens-to-brits-having-sex-rowing-swearing-and-sharing-medical-news.

[115] *See* Allegra Bianchini, Note, *Always On, Always Listening: Navigating Fourth Amendment Rights in a Smart Home*, 86 GEO. WASH. L. REV. ARGUENDO 1, 22-26 (2018) (describing multifunctional devices).

[116] *Id.* at 22-23.

[117] *See* Brittany Brattain, *The Electronic Communications Privacy Act: Does the Act Let the Government Snoop Through Your Emails and Will It Continue?*, 17 N.C. J.L. & TECH. ONLINE ED. 185, 196 (2016); Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 397 (2014) [hereinafter *Next Generation*].

[118] *See* 18 U.S.C. §§ 2702(b), 2703(a)-(c) (2019) (listing, *inter alia*, exceptions for the disclosure of communications such as to a law enforcement agency, if the contents were inadvertently obtained by the service provider and appear to pertain to the commission of a crime. Another exception in this context is to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency). For more on the exceptions of the SCA,

classified as neither ECS nor RCS, it will be exempt from the SCA.[119] In both instances, i.e., falling out of the SCA protection, any stored data from IoT devices will greatly depend on the general protection afforded by the Fourth Amendment, and subsequently, in light of the third-party doctrine, on the IoT service provider's willingness to share the data with law enforcement agencies which will depend, *inter alia*, on the terms of agreement or privacy policy.[120]

While the legal framework that would govern such access to data might be currently outdated and highly questionable,[121] IoT devices have in fact already begun to assume a role in criminal enforcement, especially when dealing with stored communications. One example is the use of the data obtained through fitness trackers[122] — serving as a source for evidence in criminal investigations and trials, from rape to murder allegations.[123] Another example is household meters and

see Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1223 (2004).

[119] For such an argument, see Seth Weintraub, *Hey Alexa: Was It the Butler, in the Foyer, with the Candlestick? Understanding Amazon's Echo and Whether the Government Can Retrieve Its Data*, 7 AM. U. BUS. L. REV. 155, 173-75 (2018); Christopher J. Borchert et al., *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act,* 13 DUKE L. & TECH. REV. 36, 42 (2015); Bianchini, *supra* note 115, at 18. It appears that even if the IoT service provider uses a cloud computing service, it will generally not fall within the statutory language of the SCA. *See* Robison, *supra* note 100, at 1212-18.

[120] Any IoT device will most likely come with a policy of some sort. The policy might be simply obliged by the law or by the corporate's terms of use. This policy will most likely include what the company does with the captured data, how is it stored and where, for what length of time, how is it secured, and who might the information will be shared with. For such an argument within the realm of cloud computing, see Robison, *supra* note 100, at 1223.

[121] Many scholars have argued that the ECPA is outdated and should be revised. *See, e.g.*, Kerr, *Next Generation*, *supra* note 117, at 419 (arguing that the ECPA should be updated to reflect modern privacy threats); Jay P. Kesan, Carol M. Hayes & Masooda N. Bashir, *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 401 (2013) ("The status of the SCA is problematic because much of the language is very unclear or outdated . . . ."); Opderbeck, *supra* note 27, at 1660 ("Meanwhile, the ECPA and SCA, which were adopted prior to the explosion of the commercial Internet, have become badly outdated.").

[122] *See* Kate Crawford, *When Fitbit Is the Expert Witness,* ATLANTIC (Nov. 19, 2014), https://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936.

[123] *See* Erin Moriarty, *The Fitbit Alibi: 21st Century Technology Used to Help Solve Wisconsin Mom's Murder*, CBS NEWS (Oct. 20, 2018), https://www.cbsnews.com/news/the-fitbit-alibi-21st-century-technology-used-to-help-solve-wisconsin-moms-murder (using data from a Fitbit proved that the suspect was not the murderer of a young woman); Kate Pickles, *Police Claim Woman Lied About Being Raped After Her*

personal assistants,[124] used for evidence in alleged murder cases.[125] Finally, even pacemakers have begun to play a part in criminal investigations. Equipped with a search warrant, investigators were able to access a man's pacemaker and used the details to corroborate details of his story, leading to charges of aggravated arson and insurance fraud against him.[126]

'Fitbit' Fitness Watch Showed She Had Not Been Dragged From Her Bed, DAILY MAIL (June 22, 2015, 10:41 AM), http://www.dailymail.co.uk/news/article-3134701/Police-claim-woman-lied-raped-Fitbit-fitness-watch-showed-not-dragged-bed.html (according to the police, the Fitbit activity tracker, combined with other circumstances, disproved rape allegations).

[124] Notably, enforcement agencies used energy consumption data much prior to the emergence of smart meters. *See* Balough, *supra* note 66, at 171.

[125] In late 2016, an Arkansas prosecutor demanded for information from a murder suspect's smart water meter and Echo smart speaker. The prosecutor's hope was that potential recordings from the device would shed further light on the death of a 31-year-old man that was found dead in the hot tub of the suspect, James Bates. The murder suspect's alleged use of an exorbitant amount of water led investigators to believe that he used it as part of an attempt to clear blood off a patio. As for the Echo device, when Amazon were first approached with a request to disclose what this specific device captured throughout the night of the alleged murder, while agreeing to provide account information and purchase history, they refused to disclose other data on grounds of the first amendment, consumer's privacy and the over-broadness of the request. More specifically, Amazon stated that they "will not release customer information without a valid and binding legal demand properly served on us," and that they "object to overbroad or otherwise inappropriate demands as a matter of course." While Amazon filed a motion to dismiss, eventually, the suspect voluntarily handed over the recordings, making this potential legal battle unnecessary for this specific case. *See* Ashley Carman, *Amazon Says Alexa's Speech is Protected by the First Amendment*, VERGE (Feb. 23, 2017, 2:39 PM), https://www.theverge.com/2017/2/23/14714656/amazon-alexa-data-protection-court-free-speech; Alex Hern, *Murder Defendant Volunteers Echo Recordings Amazon Fought to Protect*, GUARDIAN (Mar. 7, 2017, 6:11 PM), https://www.theguardian.com/technology/2017/mar/07/murder-james-bates-defendant-echo-recordings-amazon; Eliott C. McLaughlin & Keith Allen, *Alexa, Can You Help with this Murder Case?*, CNN (Dec. 29, 2016, 1:48 AM), http://edition.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd/index.html. Another murder case in New Hampshire involving an Amazon Echo device as potential evidence is currently still in court proceedings. *See* Meagan Flynn, *Police Think Alexa May Have Witnessed a New Hampshire Double Homicide. Now They Want Amazon to Turn Her Over*, WASH. POST (Nov. 14, 2018, 7:28 AM), https://www.washingtonpost.com/nation/2018/11/14/police-think-alexa-may-have-witnessed-new-hampshire-double-slaying-now-they-want-amazon-turn-her-over/?noredirect=on&utm_term=.250732055355.

[126] Investigators, for instance, have used a pacemaker that was tracking every beat of a suspect's heart to corroborate details of his story. *See* Cleve R. Wootson Jr., *A Man Detailed his Escape from a Burning House. His Pacemaker Told Police a Different Story*, WASH. POST (Feb. 8, 2017, 3:15 AM), https://www.washingtonpost.com/news/to-your-health/wp/2017/02/08/a-man-detailed-his-escape-from-a-burning-house-his-pacemaker-told-police-a-different-story/?tid=a_inl&utm_term=.f260ee0da168.

All in all, while access to stored communications in IoT seems to be increasing, the regulatory framework that governs such access is highly questionable. Beyond the rather obsolete categorizations, the SCA fails to acknowledge the potential differences between various technological devices that might be multifunctional and capture various types of data in various forms, while not accounting for the potential sensitivity of such data. Prior on embarking on a normative evaluation in Part III, and as wiretapping presents rather similar challenges with respect to data sensitivity, the following Subsection will scrutinize the applicability of the current legal framework to wiretapping.

3. Statutory Wiretapping of IoT

Assuming that the Fourth Amendment protects the *Wiretapping of Things*, connecting to any device in real time without judicial approval will generally be unconstitutional without a warrant. But even lacking constitutional protection, which could be questionable in some instances, enforcement agencies will be required to meet statutory requirements. Real-time interception of non-content communications will require a pen register order.[127] Interception of content, however, will be subject to heightened Fourth Amendment protections, i.e., fulfilling the requirements of a Title III wiretap order — also known as a super-warrant — stricter than a standard Fourth Amendment search warrant.[128]

Obtaining a super-warrant is purposely not easy. To receive a super-warrant, enforcement agencies must adhere to a higher threshold than the regular probable cause requirement,[129] i.e., they must demonstrate that regular investigative procedures are inadequate or have failed,[130] and that they will ensure that the wiretapping will be conducted in a way that minimizes the interception of non-pertinent communications.[131]

[127] *See* 18 U.S.C. § 3123 (2019); Kerr, *Internet Surveillance Law*, *supra* note 26, at 645. Notably, this will require the use of a "trap and trace device." *See* 18 U.S.C. §§ 3127(3)-(4) (2019).

[128] A "super-warrant" is a warrant issued under the Wiretap Act, whose requirements are stricter than a standard Fourth Amendment search warrant. *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1282 (2004).

[129] The probable cause to search a computer or electronic media, relies on a belief that the media will contain evidence of a crime; contraband, fruits of crime, or other items illegally possessed; property designed for use, intended for use, or used in committing a crime; or an instrumentality of a crime. *See* FED. R. CRIM. P. 41(c).

[130] *See* 18 U.S.C. §§ 2518(1)(c), (3)(c) (2019); United States v. Giordano, 416 U.S. 505, 515 (1974).

[131] *See* 18 U.S.C. § 2518(5) (2019).

Furthermore, it requires approval from high-ranking officials,[132] is restricted to pre-listed predicate felony offenses,[133] requires a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted,[134] sets time limits for the interception,[135] and requires prompt notice to the target.[136] It further requires that the judge must determine that there is probable cause for belief that the facilities from which or the place where the interception of communication is made are leased to, listed in the name of, or commonly used by that person.[137]

Deciding whether a super-warrant can be issued for an IoT device first requires acknowledging the potential differences between regular and IoT wiretapping. Some of the requirements for a super-warrant will not make a difference in this respect. For instance, the fact that the government must show probable cause does not change in light of technology. Similarly, the requirement that the government must show that reasonable efforts to get the information in traditional ways have failed does not change. Finally, showing that the wiretapped device is, at the very least, commonly used by that person (if not also listed in his name), might even become easier and more accurate with IoT devices, or at the very least, it should not substantially change in light of IoT technology.

What potentially changes is mainly the location of the wiretap. Discussing the location in wiretapping IoT is linked to the type of IoT device in question and its potential portability. Some IoT devices will not make much of a difference in this respect. Much like telephones, they might be relatively non-portable and remain generally in the same location most, if not all, of the time. This will be evident for those IoT devices that are either physically difficult to move around, like an IoT refrigerator, or are simply rather fixed in their place due to their

---

132 *See id.* § 2516(1); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL § 9-7.100 (1998).

133 As listed in § 2516. *See* 18 U.S.C. §§ 2518(3)(a)-(b).

134 *See id.* § 2518(1)(b). The particularity requirement for warrants ensures that "warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." Marron v. United States, 275 U.S. 192, 196 (1927); *see also* Stanford v. Texas, 379 U.S. 476, 485 (1965).

135 *See* 18 U.S.C. § 2518(1)(d).

136 *See id.* § 2518(8)(d).

137 *See id.* § 2518(3)(d). Accordingly, the court must specify "the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted." *Id.* § 2518(4)(b).

functionality, like an IoT toaster or a smart TV that will most likely be present in one's kitchen or living room, respectively. Other IoT devices are designed to be portable. A good example is that of health and fitness wearables or smart watches that a person is likely to wear as she goes. For other IoT devices, however, the location might be more in the grey zones. Personal assistants, like Amazon Echo or Google Home, could be placed in various locations within or outside of the house, and their portability will depend mainly on the user's preferences and needs. Practically, fulfilling the location requirements seems rather problematic for IoT. Without using intrusive means of surveillance that will reveal the device's location, enforcement agencies will have difficulty complying with this requirement.

The Act, however, specifies that a warrant could still be issued even without these requirements, depending on whether the subject is oral, wire, or electronic communications.[138] For oral communication, the state could use covert listening devices, like a "roving bug," upon fulfilling various requirements.[139] This is probably less relevant for IoT devices in general, as oral communication relates to face-to-face conversations and does not include electronic communication.[140] Depending on the device in question, IoT will more likely fall under the second category of wire or electronic communications.[141]

To obtain electronic communications under the second exception — a "roving wiretap" to intercept wire communications — the state must, *inter alia*, both identify "the person believed to be committing the offense and whose communications are to be intercepted" and make "a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility."[142] In fact, roving wiretaps are effectively used by enforcement agencies to turn on microphones. Back in 2003, the Ninth Circuit denied the Federal Bureau of Investigation's ("FBI") request to turn on

138 *See id.* § 2518(11).

139 *See* United States v. Oliva, 686 F.3d 1106, 1100 (9th Cir. 2012); United States v. Tomero, 462 F. Supp. 2d 565, 567 (S.D.N.Y. 2006). Covert listening devices might go by various names, such as bugs, wires, or a "spike mike." *See* Pikowsky, *supra* note 17, at 30.

140 "Oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation. However, such term does not include any electronic communication. *See* 18 U.S.C. § 2510(2); CHARLES DOYLE, CONG. RESEARCH SERV., R41733, PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 12 (2012).

141 *See* 18 U.S.C. § 2518(11)(b).

142 *See id.* § 2518(11)(b)(ii); Oliva, 686 F.3d at 1110.

a microphone in a car ("cartapping") that was part of the system's safety features,[143] but only on ground that this warrant would completely disable the system's safety features — without ruling out the possibility of wiretapping in-car communication devices.[144]

By 2006, reports indicated that activating cellphones' microphones was considered a legitimate practice by the Department of Justice.[145] In 2012, the Ninth Circuit held that this practice could be permissible as long as the government specifically requests that authority and that, upon scrutiny, the authorization orders must be clear and unambiguous and comply with the statutory requirements.[146] Currently, such practice will also apply to non-audio communications, as the general approach held by federal appellate courts is that super-warrants are required for them as well.[147]

Overall, the current regulatory framework could practically enable law enforcement agencies both access to at least some stored IoT communications (whether under the SCA or under the third-party doctrine) and even the wiretapping of these devices. Normatively, however, the implications of the wiretap location, and the sensors that are embedded within IoT, might greatly affect the privacy interest of individuals differently from what policymakers sought to protect in the past. But prior on embarking in such normative evaluation in Part II, the pragmatic aspects of wiretapping are also non-negligible. Even with a super-warrant, enforcement agencies might encounter various

[143] *See* Company v. United States, 349 F.3d 1132, 1146 (9th Cir. 2003); ZITTRAIN ET AL., *supra* note 74, at 13-14.

[144] The wiretapping was only permitted if it is executed with a 'minimum of interference,' but in this case, the service would have been completely shut down as a result of the surveillance and thus was not permitted. *Company*, 349 F.3d at 1145 ("We need not decide precisely how much interference is permitted. A minimum of interference at least precludes total incapacitation of a service while interception is in progress."); ZITTRAIN ET AL., *supra* note 74, at 13-14.

[145] *See* Declan McCullagh, *FBI Taps Cell Phone Mic as Eavesdropping Tool*, CNET (Dec. 4, 2006, 6:56 AM), http://www.cnet.com/news/fbi-taps-cell-phone-mic-as-eavesdropping-tool. The *Wall Street Journal* also reported that the FBI used this technique in 2013. *See* Jennifer Valentino-DeVries & Danny Yadron, *FBI Taps Hacker Tactics to Spy on Suspects*, WALL ST. J. (Aug. 3, 2013, 3:17 PM), http://www.wsj.com/articles/SB10001424127887323997004578641993388259674.

[146] *See* Jose Pagliery, *How the NSA Can 'Turn on' Your Phone Remotely*, CNN (June 6, 2014, 8:03 AM), https://money.cnn.com/2014/06/06/technology/security/nsa-turn-on-phone/.

[147] *See* United States v. Torres, 751 F.2d 875, 882-85 (7th Cir. 1984); *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 759-61 (S.D. Tex. 2013); Mayer, *supra* note 80, at 639-40.

difficulties when attempting to execute them, as the following Section shows.

C. Practical Enforcement in the Age of IoT

Executing a super-warrant for IoT might prove to be highly impractical. Currently, the regulatory framework under CALEA does not generally include IoT operators, as they would not likely be deemed as telecommunications carriers.[148] Thus, even upon service of a super-warrant, many IoT operators lack a legal obligation to have their network facilitate lawful orders for wiretaps, and lacking other incentives, they might not comply.

Prima facie, this difficulty might strike one as rather easy to resolve. Congress could simply require all IoT companies that operate within the U.S. to enable real-time access to their devices when required.[149] Pragmatically, however, it would be rather difficult to obligate IoT providers to comply with wiretapping requirements due to various reasons, including costs and technology barriers. For example, compliance costs might be unduly burdensome for many IoT providers. As a reference, even after CALEA was enacted, many companies were unable to comply with requests due to technological and financial difficulties.[150] While courts could impose compensation for reasonable expenses on the government, reimbursement for carriers must be set high to ensure that the potential fines that are associated with non-compliance will not create a chilling effect and a market barrier to new

---

[148] *See* 47 U.S.C. § 1001(8) (2019) (stating that "telecommunications carrier" means "a person or an entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire; and includes a person or an entity engaged in providing commercial mobile service or a person or an entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public's interest to deem such a person or an entity to be a telecommunications carrier").

[149] For propositions of mandating companies to enable real-time access through what is commonly known as "back-doors," see, e.g., Spencer Ackerman, *FBI Chief Wants "Backdoor Access" to Encrypted Communications to Fight ISIS*, GUARDIAN (July 8, 2015, 4:38 PM), https://www.theguardian.com/technology/2015/jul/08/fbi-chief-backdoor-access-encryption-isis; Brian Fung & Andrea Peterson, *FCC Chairman Suggests Expanded Wiretap Laws in Response to the Paris Attacks*, WASH. POST (Nov. 17, 2015, 5:24 PM), https://www.washingtonpost.com/news/the-switch/wp/2015/11/17/the-fcc-suggests-expanded-wiretap-laws-in-response-to-the-paris-attacks/.

[150] *See* Constance L. Martin, Note, *Exalted Technology: Should CALEA Be Expanded to Authorize Internet Wiretapping?*, 32 RUTGERS COMPUTER & TECH. L.J. 140, 146 n.35 (2005) ("[S]pokespersons for the FBI and DOJ stated that many companies still do not comply with CALEA, primarily because of inadequate technology.").

IoT companies.[151] But the major challenge is that forcing IoT companies for compliance would apply to a nearly infinite number of devices, all operating in potentially different forms of communication that are potentially incapable of enabling real-time transmission, and thus, unlike circuit-switched telephones, it might be technologically implausible to conduct. In turn, if compliance is forced, it could have dire consequences in terms of innovation.[152]

Even if the compliance challenges could be met, it is plausible that other forces might push against such a legal obligation. One potential force is that of social norms. If tendency towards privacy protection will be high within the public, then individuals might push back against any form of legislation they find too intrusive against their rights and liberties.[153] While some argue that the digital era led to the demise of privacy,[154] we have witnessed at least some shifts in privacy perception, mainly in the post-Snowden revelations.[155] To that extent, social norms might affect the market by driving consumers to refrain from using devices that could be more easily wiretapped than others, lacking any legal obligation to do so.[156]

---

[151] *See* Hibbard, *supra* note 40, at 382.

[152] *See* Steven M. Bellovin et al., *Going Bright: Wiretapping Without Weakening Communications Infrastructure*, 11 IEEE SECURITY & PRIVACY 62, 66 (2013) [hereinafter *Going Bright*].

[153] *See* Simmons, *supra* note 82, at 186 ("[A] more uniform distribution of privacy infringement will naturally lead to political pushback against this increased surveillance.").

[154] Scott McNealy, chief executive officer of Sun Microsystems, is famously quoted suggesting "You have zero privacy anyway . . . . Get over it." *See* Polly Sprenger, *Sun on Privacy: 'Get Over it*,' WIRED (Jan. 26, 1999, 12:00 PM), https://www.wired.com/1999/01/sun-on-privacy-get-over-it; *see also* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1466 (2000).

[155] *See* John Everington, *Push for a More Secure Digital Privacy Irreversible After Edward Snowden Leaks*, NATIONAL (Feb. 11, 2015), https://www.thenational.ae/business/push-for-a-more-secure-digital-privacy-irreversible-after-edward-snowden-leaks-1.32374; *The State of Privacy in Post-Snowden America,* PEW RES. CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america ("Some 86% of internet users have taken steps to remove or mask their digital footprints, but many say they would like to do more or are unaware of tools they could use."). *But see* Sören Preibusch, *Privacy Behaviors After Snowden*, 58 COMM. ACM 48, 48 (2015) (arguing that surveillance disclosures led to a decrease in privacy-centered behavior). For more examples of how public criticism could shape market-choices, see Note, *Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance*, 131 HARV. L. REV. 1722, 1730-32 (2018).

[156] Notably, there could also be some self-aid solutions, as users might assure that their IoT device is not wiretapped by physically disconnecting them when not in use or by pressing a hardware switch if one exists. However, these self-aid solutions are neither convenient nor plausible. This is because one of the main benefits of IoT is their remote

On the other hand, one barrier to the effect of social norms on the market is that of knowledge and expertise. Users will not often be exposed to the practices of wiretapping; they might not be aware of the possibility that their IoT device could be wiretapped; and they might not consider the consequences of such wiretaps on their right to privacy. Among many things, this potential knowledge and expertise gap is closely linked with the software of the IoT device — generally controlling what is gathered, how and where it is stored, for how long it is stored, and who has access to it.[157] Due to secrecy, most companies will not release their code — often protected as a trade secret — or their practices, making it difficult for users to examine security *ex ante*.[158] Still, users are not generally aware of how companies enable wiretapping, especially when these companies might be forbidden to share governmental requests.[159]

But even without legal obligations to comply, some companies might still be incentivized to voluntarily aid enforcement agencies for reasons such as obtaining immunity or other benefits.[160] Under these so-called public-private partnerships, which existed for a while,[161] private companies could implement measures that would aid law enforcement agencies when in need, as long as they do not break the law.[162] Furthermore, policymakers could aid in persuading the market to implement such measures voluntarily, much like they have done with the Clipper Chip.[163]

activation and voice control. If users will need to physically unplug all their digital devices, that would make their smart home rather dumb.

157 *See* Jay Stanley, *The Privacy Threat from Always-On Microphones Like the Amazon Echo*, ACLU (Jan. 13, 2017, 10:15 AM), https://www.aclu.org/blog/privacy-technology/privacy-threat-always-microphones-amazon-echo?redirect=blog/free-future/privacy-threat-always-microphones-amazon-echo.

158 And even if companies expose their security measures or practices, we often learned *ex post* that they were dishonest. *See id.* (mentioning the Volkswagen scandal as an example of a company's dishonesty).

159 Generally, super-warrants are subjected to *ex post* notice, meaning that the notice is issued with delay. *See* 18 U.S.C. § 2518(8)(d) (2019). In some instances, however, courts have relaxed that requirement, merely notifying the third-party business. *See* Mayer, *supra* note 80, at 634-35. Furthermore, the statutory framework might also enable courts to issue sealing and non-disclosure on service provider to the user or subscriber, meaning that these orders will lack transparency. *See, e.g.*, 18 U.S.C. §§ 2703(b), 2705(b).

160 *See* Elkin-Koren & Haber, *supra* note 26, at 143-44.

161 For more on public-private partnerships in the context of national security, see generally *id.*

162 *See* Froomkin, *Lessons Learned*, *supra* note 39, at 109-10.

163 *See id.*

Much like the potential pushback from social norms, voluntarily cooperation might also face resistance similar to that of legislative attempts to expand CALEA. Companies, for instance, might fear that enabling wiretapping of their devices could alienate their consumers if they become aware of such practices, which might either limit their usage or push them towards their competitors. Moreover, some companies might desire to restrict wiretapping access due to the potential threat to their network security inherent in enabling such access. In turn, the government might find some IoT operators that will partner with them, but one "weak" link in the chain might not advance the goal of wiretapping, unless this specific IoT device is used by the suspect.[164]

Furthermore, the potential security risks are non-negligible in the context of IoT. Enabling wiretapping could have dire consequences on many users in terms of infrastructure and network security. To comply with IoT wiretapping, many companies will generally need to do one of two things: decrease or increase system complexity. Some companies might simply choose to lower their security by default for all users to reduce costs. This choice, however, might be less plausible for some companies, as substantially reducing the overall security of all devices could have a negative market effect. Thus, it is plausible that at least some companies will not reduce cybersecurity but rather make it more complex, attempting to ensure that devices could only be accessed lawfully.

Increasing system complexity might also be problematic, as it is often considered one of the enemies of good security.[165] New features built in the system could create new vulnerabilities that, in turn, could be exploited by malicious actors.[166] Moreover, complex systems might make wiretapping highly difficult. Wiretapping telephones was possible partly due to the network's centralized nature, while the decentralization of IoT would make it much more difficult.[167] This potential barrier of enabling real-time access to IoT relates, *inter alia*, to

[164] It will become more fruitful if these devices allow third-party apps, like the Echo's Skills. Then, law enforcement agencies might seek the third-party app that would allow such an interception, or even go a step further, and develop such a skill on their own. For a general discussion on expanding the scope of CALEA to apply on internet OSPs, see generally Hibbard, *supra* note 40.

[165] HAROLD ABELSON ET AL., KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS 2 (2015), https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

[166] *See id.*

[167] For more on decentralization in the context of wiretapping, see Bellovin et al., *Going Bright*, *supra* note 152, at 64-66.

forms of communications like peer-to-peer methods and to what is commonly referred to as the "crypto wars" or the "going dark" problem — government access to encrypted communications — which can be traced back to the 1970s.[168] Suppose that some IoT devices use security measures while data is in transit. Using encrypted end-to-end communication, for instance, would require the IoT provider to equip the government with a key to such communication, which would otherwise be in escrow.[169] Those IoT companies must ensure that the governmental agent can access communication limited to a specific warrant — and that it could not be used for decrypting communications for other users, or even the same user outside the scope of the warrant.

We can term this as the "lawful access only" problem,[170] which is based on creating an exceptional access system — also known as a backdoor.[171] The problem, however, is that once one inserts backdoors, vulnerability is introduced to the system, and therefore, it is not an ideal security practice.[172] Aside from the potential misuse by the government, it will expose the network to increased risks from hackers and other nation states, who may exploit this new vulnerability.[173]

---

168 *See id.* at 62; ZITTRAIN ET AL., DON'T PANIC, *supra* note 74, at 5. For further reading on the history of wiretapping, see generally WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 1-10 (2007). For further reading on the crypto wars, see generally Eric Rice, *The Second Amendment and the Struggle over Cryptography*, 9 HASTINGS SCI. & TECH. L.J. 29, 32-44 (2017).

169 *See* EUROPOL, FIRST REPORT OF THE OBSERVATORY FUNCTION ON ENCRYPTION 32 (2019) (explaining the key escrow system).

170 The lawful access only problem was articulated, *inter alia*, by Matt Blaze. *See Encryption Technology and Potential U.S. Policy Responses: Hearing Before the Subcomm. on Infor. Tech. of the H. Comm. on Oversight & Gov't Reform*, 114th Cong. 57-58 (2015) (written testimony of Prof. Matt Blaze); *see also* Bruce Schneier, *Security or Surveillance?*, LAWFARE (Feb. 1, 2016, 1:01 PM), https://www.lawfareblog.com/security-or-surveillance.

171 There are various types of backdoors that could allow exceptional access to communication. One example is that of the use of encryption algorithms with vulnerabilities that are known only to the enforcement agency. Another example is a key escrow (also known as "fair public-key cryptosystem") which requires each user of a public key to deposit an extra associated private key with an escrow agent. *See* Opderbeck, *supra* note 27, at 1663-64.

172 These practices could include, *inter alia*, "forward secrecy" ("where decryption keys are deleted immediately after use") or "authenticated encryption" (using a "temporary key to guarantee confidentiality and to verify that the message has not been forged or tampered with"). *See* ABELSON ET AL., *supra* note 165, at 2.

173 *See* Bellovin et al., *Going Bright*, *supra* note 152, at 63; Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1, 4 (2014) [hereinafter *Lawful Hacking*].

But the lawful access problem is not the only concern with respect to security. Another concern is that some companies will seek to make their communications highly secured. It could, for instance, occur as a market-response to consumer fears that devices could be accessed by other parties, without authorization, or even with. While many IoT devices are currently vulnerable to hacking because the data it transmits is not encrypted,[174] this practice might change. Suppose a market player decided to offer an IoT device that uses strong security measures — so strong that even the IoT provider does not have access, rather only the user has the ability to access the data. Should policymakers oblige this company to enable access to that communication when required by enforcement agencies or courts?

Generally, requiring IoT providers to design security breaches in the communications network could be terrifying, as these vulnerabilities could be exploited.[175] Internet platforms should not be subjected to the same requirements as phone networks. They operate differently, and the tradeoff is not similar. Even if Congress attempts to regulate the security of things in this aspect, market forces might push back. We have witnessed such a pushback in what had become to be known as the "Apple-FBI Standoff," in which the FBI sought Apple's cooperation in gaining access to an encrypted iPhone that was used by the deceased San Bernardino mass-shooter named Syed Rizwan Farook.[176] The government relied on the All Writs Act — a statute which dates back to

[174] *See, e.g.*, Mahendra Ramsinghani, *How the 'Insecurity of Things' Creates the Next Wave of Security Opportunities,* TECHCRUNCH (June 26, 2016, 8:00 AM), https://techcrunch.com/2016/06/26/how-the-insecurity-of-things-creates-the-next-wave-of-security-opportunities. Notably, however, computerized personal assistants like Amazon Echo, Google Home, and Apple's HomePod currently encrypt the voice recordings sent to their respective servers. *See* Alfred Ng, *HomePod, Echo, Google Home: How Secure are your Speakers?*, CNET (June 8, 2017, 5:00 AM), https://www.cnet.com/news/homepod-echo-google-home-how-secure-are-your-speakers/.

[175] *See* Landau, *supra* note 23, at 426 ("Building surveillance technology into Internet communications protocols will create vulnerabilities.").

[176] *See In re* An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15-0451M, 2016 U.S. Dist. LEXIS 20543, at *1-2 (C.D. Cal. Feb. 16, 2016); *In re* Apple, Inc., 149 F. Supp. 3d 341, 349 (E.D.N.Y. 2016). For more on the Apple-FBI standoff, see generally Steven R. Morrison, *Breaking iPhones Under CALEA and the All Writs Act: Why the Government Was (Mostly) Right*, 38 CARDOZO L. REV. 2039, 2040-44 (2017). Notably, these battles extend far beyond this single incident. For instance, Apple has recently added protections in its new iOS (operating system) against the USB devices being used by law enforcement and private companies that could bypass an iPhone's passcode and evade Apple's encryption safeguards. *See* Chris Welch, *Apple Releases iOS 11.4.1 and Blocks Passcode Cracking Tools Used by Police*, VERGE (July 9, 2018, 2:17 PM), https://www.theverge.com/2018/7/9/17549538/apple-ios-11-4-1-blocks-police-passcode-cracking-tools.

1789 and empowers courts to issue "all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[177] A day before the hearing was scheduled, the FBI announced that it was able to get assistance from a third party and thus was in no need of Apple's compliance eventually.[178] Cases like this seem to reappear in the context of wiretapping as well, as the government is currently attempting to force Facebook to break the encryption of its Messenger app so law enforcement may wiretap a suspect's voice conversations in a criminal probe.[179]

These cases, however, illustrate not only that security could be meaningful for some companies, but also that this pragmatic aspect, while challenging, might not be as challenging as one might suspect. Enforcement agencies might invest heavily on technical innovations — or outsource such abilities — that would enable them to intercept communications in real time, with or without the use of CALEA.[180] Either within their labs or by outsourcing,[181] they could exploit existing weaknesses in IoT devices, or over the network, to install interception

[177] 28 U.S.C. § 1651(a) (2019). For more on the All Writs Act in this context, see generally Morrison, *supra* note 176; John L. Potapchuk, *A Second Bite at the Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data Under the All Writs Act*, 57 B.C. L. REV. 1403 (2016).

[178] *See* Arjun Kharpal, *Apple vs FBI: All you Need to Know*, CNBC (Mar. 29, 2016, 6:34 AM), https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html.

[179] *See* Dan Levine & Joseph Menn, *Exclusive: U.S. Government Seeks Facebook Help to Wiretap Messenger – Sources*, REUTERS (Aug. 17, 2018, 1:34 PM), https://www.reuters.com/article/us-facebook-encryption-exclusive/exclusive-u-s-government-seeks-facebook-help-to-wiretap-messenger-sources-idUSKBN1L226D.

[180] See, for example, the FBI's "Going Dark" project, which "seeks legal and technical innovations to enhance lawful communications intercept capabilities." *See* Froomkin, *Lessons Learned*, *supra* note 39, at 135; *Going Dark*, FBI, https://www.fbi.gov/services/operational-technology/going-dark (last visited Feb. 1, 2019). It should be noted that enforcement agencies are making use of technological measures, like that of malware, to aid in espionage to the least. *See* Scott Shane, Matthew Rosenberg, & Andrew W. Lehren, *WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents*, N.Y. TIMES (Mar. 7, 2017), https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html?_r=0 (describing the CIA's alleged methods of hacking). For more on this topic, see generally Paul Ohm, *The Investigative Dynamics of the Use of Malware by Law Enforcement*, 26 WM. & MARY BILL RTS. J. 303 (2017).

[181] The FBI has established the National Domestic Comm Assistance Center (NDCAC) to aid against the so-called "Going Dark" problem. *See* Bellovin et al., *Going Bright*, *supra* note 152, at 63; *About the NDCAC*, NAT'L DOMESTIC COMMC'NS ASSISTANCE CTR., FED. BUREAU OF INVESTIGATIONS, https://ndcac.fbi.gov/about/about-the-ndcac (last visited Feb. 1, 2019).

software and use it upon issuance of a warrant.[182] This scheme might be more preferable from a security aspect, as it only exploits existing vulnerabilities, while not creating new ones. Still, it could be questionable as to the potential misuse of such a technology beyond a warrant's requirement and the lack of judicial oversight over its implementation.

There is little chance that Congress would generally eliminate the use of encryption for a variety of reasons, and perhaps partially due to the First Amendment, as source code could be considered speech.[183] The government might also generally desire that companies will have strong encryption, to ensure that unauthorized actors — like foreign states — will not be able to access the data.[184]

But the pragmatic challenges to the *Wiretapping of Things* do not stop here. Wiretapping of IoT will most likely raise jurisdictional difficulties.[185] Solving crimes within one jurisdiction might require the real-time interception of data that does not physically pass through the jurisdiction's physical borders. Furthermore, an intended crime within the physical borders might be organized outside of them, necessitating law enforcement agencies to act beyond their mandates. To address this issue, states might seek the aid of service providers that operate within

[182] *See* Bellovin et al., *Going Bright*, *supra* note 152, at 62-63. One example is that of installing keylogging malware that records inputs from its user prior to data encryption. *See* Opderbeck, *supra* note 27, at 1662. But such keylogging malware will not work on all IoT devices, mainly as they often operate in a different manner. They will have to find an equivalent of such malware to capture oral communication. As another example, Amazon's Alexa had an exploit that allowed activating the device at any time. *See* Rob LeFebvre, *Amazon Fixed an Exploit that Allowed Alexa to Listen All the Time*, ENGADGET (Apr. 25, 2018), https://www.engadget.com/2018/04/25/amazon-fixed-exploit-alexa-listen. For more on governmental use of malware, see Mayer, supra note 80, at 583-89.

[183] *See* Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1143-45 (9th Cir. 1999) (Fletcher, J.), *rehr'g en banc granted*, 192 F.3d 1308 (9th Cir.1999); Froomkin, *Lessons Learned*, *supra* note 39, at 109 (arguing that banning strong crypto is probably not a viable option, partially due to the first amendment).

[184] *See, e.g.*, *Going Dark*, *supra* note 180 ("Make no mistake, the FBI supports strong encryption, and we know firsthand the damage that can be caused by vulnerable and insecure systems . . . . The government uses strong encryption to secure its own electronic information, and it encourages the private sector and members of the public to do the same.").

[185] As for stored communication, the SCA was recently amended to confront this issue. The so-called CLOUD Act grants federal law enforcement the ability to compel U.S.-based technology companies (via warrant or subpoena) to provide requested data stored on servers regardless of their location. *See* Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115–141, 132 Stat. 1217 (2018) (codified at 18 U.S.C. § 2523 (2019)). For more on data, law enforcement and jurisdictions, see generally Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179 (2018).

their jurisdictions. Otherwise, enforcement agencies would have to rely on assistance from other countries. Such assistance could be interpreted within what is known as the Convention on Cybercrime, which requires signatory parties to establish the powers and procedures for the purpose of specific criminal investigations or proceedings.[186] That could include the disclosure of decryption keys.[187] In addition, they could do so by informal requests or by signing mutual legal assistance treaties.[188] The problem, however, is that law enforcement agencies might need real-time interception of data expeditiously, and these legal mechanisms might be lengthy.[189]

Without belittling the pragmatic and normative challenges that arise from access to IoT communications, let us assume at this point that they could be overcome, either by service providers actually enabling real-time interception or by policymakers deciding to require all IoT operators to comply with CALEA. Let us further (and carefully) assume that compliance does not risk network security to a great extent and that this potential capability will not be misused by governmental agencies. As the next Part shows, even with these rather optimistic assumptions, applying the current regulatory framework will create challenges to human rights and liberties, like that of the right to privacy, and thus must be reconfigured in the always-on era to properly balance such a tradeoff.

III. RECONFIGURING LAWFUL ACCESS TO COMMUNICATION IN THE ALWAYS-ON ERA

Something is changing within the paradigm of law enforcement and technology. As noted by the Supreme Court in recent years, searching digital data is not equivalent to a physical search.[190] "Digital is different," as some scholars argue, and the enforcement paradigm is beginning to slowly adapt to technological changes.[191] IoT might even take these notions further. Not only are IoT devices often equipped with various sensors — like microphones and cameras — they often rely on

186 *See* Convention on Cybercrime art. 14, Nov. 23, 2001, E.T.S. 185.

187 *See* Froomkin, *Lessons Learned*, *supra* note 39, at 127.

188 *See* Mizrahi, *supra* note 97, at 345.

189 *Id.*

190 *See* Riley v. California, 573 U.S. 373, 446-49 (2014) (holding that electronic device searches implicate greater privacy interests than physical searches). Notably, however, courts have not explicitly held that Riley applies to all IoT devices yet.

191 Mayer, supra note 80, at 610; *see* Orin Kerr, *The Significance of* Riley, WASH. POST (June 25, 2014, 8:56 AM), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/25/the-significance-of-riley.

oral or visual communications as their main features, thus potentially making any device subject to real-time interception of communication and making it more plausible that law enforcement agencies will seek to employ such interception tactics. Stored communications are also greatly affected by these new technologies. Aside from the fact that IoT devices might collect vast amounts and varied types of data about their users, this data could now be stored, usually using cloud computing services,[192] for longer time periods than before, while storage costs keep falling.[193] With technological developments in storage capacity and reduced costs associated with such storage, stored communications could become much more valuable for criminal enforcement purposes.

Aside from the pragmatic challenges of applying the regulatory framework to IoT communications, and their potential implications on security, allowing access to communications of IoT raises many normative difficulties for human rights and liberties, mainly to individuals' privacy. Furthermore, with more rapid advancements in identification technologies, law enforcement in the always-on era might become more intrusive than ever in the history of humankind. To address these challenges, Section A will discuss the privacy implications of the always-on era, while arguing that the current regulatory framework is ill-suited to properly protect privacy. This analysis compares existing technology to IoT, and explains significant differences for the purposes of regulation and privacy protection. Section B will offer guidelines for policymakers to ensure a proper balance between privacy rights and enforcement needs, while discussing further challenges to law enforcement in the always-on era.

A. Privacy Implications of Access to IoT Data and Communications

Access to IoT communications, whether to data at rest or in real time, affects the privacy interests of individuals. As noted by the Supreme Court, searching a mobile phone could reveal the "sum of an

[192] Cloud computing could be defined as "data, processing power, or software stored on remote servers made accessible by the Internet as opposed to one's own computers." *Cloud Computing*, EPIC, https://www.epic.org/privacy/cloudcomputing (last visited Feb. 1, 2019).

[193] *See* Robison, *supra* note 100, at 1197-99 (describing the cost reductions in data storage). To add to this argument, cloud-based services reduced costs for law enforcement agencies as they often directly approach service providers with subpoenas. *See* Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECH. L. 359, 386-87 (2010).

individual's private life,"[194] and at least some IoT devices could well fall within this reasoning.[195] As previously noted, enabling such access might lower network security and negatively impact IoT infrastructure, potentially exposing consumers to unauthorized access by malicious parties. Furthermore, without proper safeguards, enabling such access might also be abused by governmental agencies that either operate outside the scope of their legal mandates or interpret the current framework to apply on IoT. In these instances, the right to privacy will be greatly impacted.

Aside from these concerns, the broader normative question is how the right to privacy, among other civil rights and liberties, will be affected by lawful access to IoT data and communications. To begin such an assessment, one might question whether, and to what extent, lawful access to IoT data and communications could affect the privacy interests of individuals differently than that of other communication technologies like telephones, bugs and the internet, as currently governed by the regulatory framework. In other words, how does IoT differ from previous technologies with regard to privacy in the context of the regulatory framework that was designed with these technologies in mind?

At its core, the regulatory framework governs access to communication by differentiating between actions that could affect the privacy interests of individuals differently. It sets a higher regulatory threshold for those actions that are more likely to infringe upon individuals' privacy, while adding more checks and balances for when the access occurs. Thus, while an impact on individuals' privacy is generally debatable and difficult to assess, what greatly affects the impact would be the nature of the potential data acquired by the access to IoT communications and its potential sensitivity.

Generally, data sensitivity could depend on various factors affected, *inter alia*, by the aforementioned device's location and portability, and by the device's embedded sensors that detect and capture human activity. Thus, when generally comparing IoT devices to other technologies, one might argue that the potential data that could be acquired from these devices could increase the *quality* and *quantity* of data, depending on the nature of the devices, their embedded sensors,

---

194 *Riley,* 573 U.S. at 394. *See* Bianchini, *supra* note 115, at 14-15. For more on the search incident to arrest doctrine, see generally Kelly Ozurovich, Riley v. California – *Cell Phones and Technology in the Twenty-First Century*, 48 LOY. L.A. L. REV. 507, 509-13 (2014).

195 For an argument as to why *Riley v. California*'s cellphone exception should apply on fitness trackers, see Saphner, *supra* note 65, at 1720.

their location, and generally the use of these devices. In other words, in many instances, IoT devices might gather more data, from more individuals, which might contain a richer variety than if gathered using the regulatory framework for telephones, bugs, and even the internet. The analysis, however, should focus more closely on the different technologies in both the context of access to stored communications and real-time access.

This analysis begins with telephones. IoT differs from telephones in many aspects. Unlike IoT, telephones are generally limited in disclosing an individual's location, they are limited to capturing oral communication, and they must be actively used in order to be tapped. Aside from these differences, wiretapping IoT would, in many instances, differ greatly in terms of data sensitivity. This is especially evident for those IoT devices that are multifunctional, that is, that individuals might use as a substitute form of communication — instead of telephones — while also using them for other purposes. In terms of access to stored communications, while IoT could, and many times does, store data indefinitely, a practice of storing telephone calls, lacking a legal obligation by telephone companies, is not feasible or currently known to occur as a practice or as a business model for telephone companies.

The more accurate comparison would be between IoT and covert listening devices — more simply stated, bugs. Bugs are more akin to IoT than telephones, as their locations will be known to the agency; they do not require users' activation — hence are "always-on"; and while perhaps only true in recent years, the data gathered could be stored for a long, perhaps indefinite, period. The difference in privacy interests relies upon two main factors: the sensors embedded in IoT and its infrastructure.

Sensors could greatly affect privacy interests. While bugs are designed for capturing oral communication, i.e., they are microphones, IoT could capture much more, like visual communications. But even if we assume that bugs are not limited to microphones, thus eliminating this difference, IoT infrastructure does make a substantial difference. Before IoT, placing bugs involved physical work, expense, and time. Bugging was rather difficult to implement, even with a warrant.[196] While unintentional, this practical element set a barrier on bugging that increased the protection of privacy. The *Wiretapping of Things* is

[196] To exemplify how placing bugs are rarely used by enforcement agencies, in 2017, out of the 2,421 orders for which intercepts were installed, only seven were labeled as "oral." *See Table Wire 6 - Wiretap*, U.S. COURTS (Dec. 31, 2017), http://www.uscourts.gov/statistics/table/wire-6/wiretap/2017/12/31 [hereinafter *Table Wire 6*].

different in this aspect, as long as intermediaries could provide such services on behalf of government agents.

Moreover, bugs are not generally portable, as they are placed in specific locations, while many IoT devices are. Such portability greatly affects privacy. Especially when IoT devices surround individuals — and in some instances are constantly worn by them. Arguably, the fact that bugs must be concealed to avoid detection might also lead to a more limited use of them, or to some extent, using microphones that are of a lesser-quality than many IoT sensors. Finally, in the context of both access to stored communications, the use of intermediaries increases the data that is gathered prior to any legal obligation, and intermediaries' capacity to store such data indefinitely increases the potential negative implications on the right to privacy. Essentially, applying the regulatory framework set for bugs to IoT might increase the probability of infringing one's privacy and eliminate the barriers that placing bugs has set.

The analysis now turns to the internet. Arguably, IoT might not dramatically alter the already mass amounts of stored communications which are currently held by service providers online.[197] In many instances, online intermediaries will collect and retain data on individuals that is much more pervasive than that gathered by at least some IoT devices — if not most. There are some differences that should be accounted for when discussing the potential privacy threats.

One of the main differences between the internet and IoT relies both on the portability and the form of communication. While using the internet could reveal an individual's location, it would not be generally different from knowing that a telephone is within someone's home. The second difference is that the internet captures mostly written communications, although it can also capture both oral and visual communications. While depending on the IoT device and its sensors, it could often capture both oral and visual communications, as these sensors are often embedded as a main feature of communication with the device.

Another feature that might dramatically change the outcomes of such an analysis depends on whether the IoT is always on or not. If always-on devices constantly collect and retain data without the user's awareness, then such data might be more massive, pervasive, and

[197] Google, for example, already collects massive amounts of data from individuals like what they are searching, the phrases they use in their Gmail accounts, and their locations, among other things. *See* Gaudin, *supra* note 72.

invasive than the data that is routinely acquired online.[198] If this is the case, then one of the differences in terms of privacy expectation is that, unlike always-on devices, when someone uses the internet he "turns it on" *per se*, i.e., knowing that third parties might use this data for various purposes. The always-on feature is non-negligible in this context. The fact that devices constantly monitor their users is not akin to the use of the internet, at least in the traditional sense of using computers.

Overall, while accounting for differences in the device and its use, whether it would be a telephone, a bug or the internet, data quality and quantity might increase in IoT due to a higher probability that sensitive data will be gathered from various sensors. This is due, *inter alia*, to the potential ability of sensors to communicate and store data containing location and expanding the types of data that is gathered, i.e., not just oral and written communications. Moreover, IoT devices could be portable and located in rather intimate areas, which might contribute to the gathering of sensitive data. Fitness wearables, for instance, could be worn almost constantly on an individual, thus leading to the gathering of data anywhere the individual goes. In this instance, the gathered data could be deemed as, e.g., sensitive health data acquired by these devices. Some non-portable devices raise a different concern that is linked specifically with their locations. Access to data from someone's household object, without knowing the exact location of the device within the household, could have dire implications on a user's privacy. It could reveal highly intimate details about the individual and other members of the household — well beyond the requirements of a wiretapping warrant.[199]

Nevertheless, when we compare the potential sensitivity of gathered data from telephones, bugs, and the internet against IoT, it is not clear-cut whether IoT data is always more sensitive by default than older technologies. There is a real chance that in many instances these technologies, and mainly the internet, subject individuals to revealing data that is more sensitive than the data revealed in IoT, especially when the IoT devices gather data that is less likely to be deemed as sensitive. Stored communications of some IoT devices, like washing machines and smart water meters, would likely be less sensitive than almost any regular use of the internet, like that of browsing. Living in a smart home, for instance, could be the equivalent to using the internet almost

198 *See* Laura DeNardis & Mark Raymond, *The Internet of Things as a Global Policy Frontier*, 51 UC DAVIS L. REV. 475, 482 (2017).

199 Bianchini, *supra* note 115, at 3; *see* Arielle M. Rediger, *Always-Listening Technologies: Who Is Listening and What Can Be Done About It*, 29 LOY. CONSUMER L. REV. 229, 240 (2017).

constantly, even if the devices are not "always-on," as the household members will constantly generate data while they use their washing machine, refrigerator, toaster, TV, and computerized personal assistants, to name but a few examples.[200]

The implications of the quantity of data on privacy will become more evident if such data could be aggregated from various sources. A single search warrant for a smart thermostat might not seem a risk to privacy *per se*, as the stored data might only reveal a fraction of human conduct. But when combined with other datasets, connecting the dots becomes much easier, thus increasing privacy risks. Under what is often termed as the *mosaic theory*, the aggregation of many bits of non-intimate data about a person can reveal intimate information about a person's life, potentially becoming a "search" that would implicate the Fourth Amendment.[201] More simply stated, access to IoT stored communications, when aggregated, could reveal a great deal on individuals' lives. Due to storage capabilities and relatively low costs, IoT companies might have little prioritization of what data should be kept.[202]

---

[200] A Federal Trade Commission report from 2015 found that "fewer than 10,000 households using the company's IoT home-automation product can 'generate 150 million discrete data points a day.'" *See* PRIVACY & SECURITY IN A CONNECTED WORLD, *supra* note 5, at 14.

[201] *See* United States v. Maynard, 615 F.3d 544, 561-62 (D.C. Cir. 2010) (introducing the mosaic theory). *See generally* David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J. L. & TECH. 381, 390 (2013) (arguing that "for the mosaic theory to be a serious response to the disconcerting encroachment of modern surveillance technologies on our reasonable expectations of privacy, its proponents must develop a practical means of implementation"); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 314 (2012) (considering the consequences of possible judicial adoption of a mosaic theory, and mapping the possible futures of mosaic theory); Gabriel R. Schlabach, Note, *Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act*, 67 STAN. L. REV. 677, 679–80 (2015) (arguing the Stored Communications Act's "protections are inadequate in light of the conceptual insights of the mosaic theory and the massive technological changes that have occurred since the statute's passage in 1986"); Simmons, *supra* note 82, at 146-52 (defining and describing the growth of the mosaic theory and its potential implications on Fourth Amendment doctrine); Christopher Slobogin, *Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 4 (2012) (proffering a statute that attempts to operationalize mosaic theory based on the proportionality principal and John Hart Ely's political process theory).

[202] *See* Patricia L. Bellia, Symposium, *Surveillance: The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 148 (2008); Kerr, *Next Generation*, *supra* note 117, at 391-92 ("Users no longer need to be careful about what they keep on the server. The server

The fact that IoT devices are less likely to be used only by a single individual could also increase the quantity of data, at least to some extent. The captured data from IoT devices could, in these instances, increase the amount of data that is not relevant to an investigation.[203] On the other hand, as annual reports on all Title III wiretaps indicate, law enforcement agencies have increasingly requested wiretaps for smartphones rather than traditional phones,[204] which in turn could increase the possibility of capturing the target's conversations, and not those of individuals who are not suspects.[205] But while this might be true for those IoT devices that are only used by a single individuals, it might not be the case for other IoT devices. Thus, IoT data could be collected inadvertently and could greatly affect the privacy interests of third parties. It could collect potentially irrelevant — and many times intimate — information about individuals using the IoT devices or those that are simply within the reach of its sensors. While telephones and bugs also present such challenges, the privacy risks for IoT devices are enhanced due to the aforementioned sensitivity of data that is revealed inadvertently.

Overall, IoT makes access to stored communications or real-time access more complex from a legal perspective. Applying the current regulatory framework to access to IoT communications, without further assessing the privacy implications of such moves, fails to acknowledge the implications of such access due to the technological innovations involved. More closely, the current regulatory framework was set to ensure the tradeoff between enforcement needs and privacy — while privacy implications dramatically change and thus the tradeoff is off balance. As indicated in Part II.C, the current framework might exclude IoT operators from legally obliging to have their network facilitate lawful orders for wiretaps, and even when their network could facilitate these orders, it might be technologically implausible to conduct. But even when these challenges are met, the privacy implications of IoT, as indicated in this Part, are non-negligible. With these differences in mind, applying a regulatory framework that reflects lower plausibility

can keep everything . . . Today's Internet providers can — and often do — store everything.").

203 For more on the privacy of innocent users regarding cloud storage, see generally Mizrahi, *supra* note 97.

204 The 2017 Wiretap Report indicates that of the 2,218 intercepts installed in 2017, telephone wiretaps accounted for 92 percent — while the majority of them involved cellular telephones. *See Table Wire 6*, *supra* note 196; Bellovin et al., *Lawful Hacking*, *supra* note 173, at 13.

205 Bellovin et al., *Lawful Hacking*, *supra* note 173, at 13.

of privacy violations, fails to configure a proper tradeoff between enforcement needs and privacy, when potential privacy violations rose. Thus, both access to stored communications and, perhaps most importantly wiretapping, must be reconsidered, and potentially reconfigured, in light of these changes.

B. Rethinking Lawful Access in the Always-on Era

Considering the differences between IoT and existing technologies that render the current regulatory framework inadequate, the legislature and judiciary must respond with improvements. Technological changes relating to stored communications might generally not be as dramatic as one might think. As mentioned, the internet has already made such a shift in the potential privacy implications regarding the sensitivity of data that could be accessed. In terms of privacy, one might even argue that the vast amount of metadata gathered from the internet and IoT devices could actually increase individuals' rights and liberties, as law enforcement agencies might make more use of non-content communication records that could include a variety of data on individuals, like their locations, contacts, and movements.[206] Taking this argument further, with the increased availability of both metadata and data from various resources, law enforcement agencies might actually be able to engage in less real-time access and, thus, at least presumably, be less intrusive.[207]

Naturally, if law enforcement agencies will rely more on stored communications than on wiretapping, then allegedly it would increase the privacy protection of individuals, as arguably real-time access is more intrusive at its core. Nevertheless, such a move could prove to be a double-edged sword in terms of privacy. Other than the fact that real-time access is not more sensitive than stored communications *per se*, if always-on devices actually record and store data all the time, or even most of the time, then it becomes somewhat meaningless to differentiate

---

206 *See* Bellovin et al., *Going Bright*, *supra* note 152, at 62.

207 Technological advancement has greatly improved the practical ability to monitor criminals, even without warrants, due to the existence and availability of other information, such as location data, commercial data dossiers, and readily available contact information. *See* SUSAN LANDAU, SURVEILLANCE OR SECURITY?: THE RISKS POSED BY NEW WIRETAPPING TECHNOLOGIES, 99-101 (2011); Bellovin et al., *Lawful Hacking*, *supra* note 173, at 13; Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 463-64 (2012).

between real-time capture of information from online storage.[208] Stored data will effectively become real-time data that is stored with delay, enabling enforcement agencies to obtain communications almost in real time. If enforcement agencies could easily acquire stored data within IoT servers, then they could do so without real-time interception, but rather by accessing databases after the transmission ends. Thus, an always-on era might mean that any storage becomes rather similar to real-time interception,[209] and normatively, any access to such stored communication should be treated under the regulatory safeguards of wiretapping, rather than that of stored communications.

In practice, however, it seems that currently many IoT devices are not generally "always-on" in this context. While this might be untrue for IoT wearables, IoT devices like computerized personal assistants do not harvest data without activation, even if they are labeled as always-on. In that instance, stored communications would not be as beneficial as real-time access, and governmental agencies might still seek to activate these devices in real time. Moreover, when IoT devices are not always-on, enforcement agencies must wait to know whether the user activated the device or not. Practically, as long as the IoT device does not constantly record everything in its vicinity, such data might not be sufficient for enforcement agencies seeking to gain real-time access to such communications.

The impact on the right to privacy in this context will greatly depend on shifts in how companies store information, and the length of such storage could greatly affect the relevancy of accessing stored communications. Privacy protection could increase if companies adopt a data minimization agenda,[210] i.e., storing only relevant data for a limited period. Without legal intervention, however, it seems unlikely that the market will voluntarily make such a move without proper incentives.[211] After all, consumer data is at the core of many IoT business models, and the goal of for-profit companies is to generate

---

[208] Declan McCullagh, *Why DOJ Didn't Need a 'Super Search Warrant' to Snoop on Fox News' E-mail*, CNET (May 25, 2013, 12:50 PM), https://www.cnet.com/news/why-doj-didnt-need-a-super-search-warrant-to-snoop-on-fox-news-e-mail.

[209] Kerr, *Next Generation*, *supra* note 117, at 393 ("When everything is stored, stored access begins to reveal the same level of detail as real-time access.").

[210] Much like the FTC's recommendation that IoT providers minimize their collected data and retention period. PRIVACY & SECURITY IN A CONNECTED WORLD, *supra* note 5, at iv.

[211] A notable exception would be Apple's Siri, as Apple only stores voice recordings with identifiers for six months, and after that they are deleted automatically. *See* Zack Whittaker, *Amazon Won't Say if it Hands Your Echo Data to the Government*, ZDNET (Jan. 18, 2018, 9:36 PM), https://www.zdnet.com/article/amazon-the-least-transparent-tech-company.

profits for their shareholders.[212] The impact could also change in light of self-management tools that users could deploy to protect themselves, like physically turning off sensors or deleting all their data, but it might still be insufficient for many users, as this solution relies on various assumptions, like that of awareness, expertise, and feasibility.[213] Thus, at this point, one might simply argue that IoT might necessitate rethinking of access to stored communications.

As for the *Wiretapping of Things*, the current super-warrant requirements are outdated, as they fail to recognize the differences between a telephone or a bug and IoT devices. As the regulatory framework failed to govern the internet (aside from VoIP), mainly due to infrastructure barriers, the leap towards enabling the *Wiretapping of Things* is non-negligible. It does not mean that IoT will never be accessed in real time. Aside from technical difficulties, generally speaking, wiretap warrants could most likely be issued for at least some IoT devices. But if such a leap from telephones to IoT occurs, then policymakers must take into account the potential probability of revealing sensitive — and many times irrelevant — data from the suspect and from the device's surroundings. They must consider taking the super-warrant requirements at least a step up — creating requirements for an *ultra-warrant* — granted only in rare cases under a stricter regulatory framework that reconfigures civil rights and liberties within such a practice, while increasing procedural safeguards like oversight and transparency.

When considering the current super-warrant requirements, it strikes one as rather obvious that IoT must adhere to a higher threshold. Obviously, the location and nature of the facilities might have a direct linkage with the potential sensitive data that could be revealed through the wiretapping. But the nature of data changes due to other factors as well, and in IoT, these factors must be taken into account when considering the privacy implications of such wiretaps. Thus, judges must be highly careful when granting ultra-warrants. They must examine, *inter alia*, the types of sensors the IoT device has and accordingly account for the potential sensitivity of data that could be revealed in light of the enforcement purposes. Crafting such ultra-warrants requires policymakers and courts to account for various considerations — added to the current requirement of super-warrants.

---

[212] *See* Note, *Cooperation Or Resistance?*, *supra* note 155, at 1730-35.

[213] *See* Mark Jones, *How to Hear All Your Amazon Echo Recordings (and Delete Them Too!)*, KIM KOMANDO SHOW (Apr. 8, 2017), https://www.komando.com/tips/395933/amazon-echo-essential-security-settings/2.

One consideration is *relevancy*. First, rather similar to law enforcement practices regarding the wiretapping of phones, courts must ensure a *minimization provision* that ensures that law enforcement agencies will cease interception when irrelevant information — that which is not subject to interception under the order — is shared.[214] This is highly important in the *Wiretapping of Things*, mainly due to secondary users that could be exposed to such tapping inadvertently.[215] Next, to safeguard individuals who are not part of the investigation, beyond a requirement to cease storage of incriminating data, policymakers must make sure that such incriminating evidence will also be inadmissible in a criminal proceeding.[216]

Another consideration is *use restriction* of stored data acquired from the wiretap.[217] Considering the "things" in question regarding the potential sensitivity of the gathered data, while also accounting for data aggregation and big data analysis,[218] Courts must not only place limitations on the use of wiretapping technology, but also restrict future use of it. One restriction, for instance, should be on the length of time that enforcement agencies are allowed to store the acquired data. Another would be to limit the scope of the stored data to incriminating evidence on individuals that are part of the investigation.

A third consideration is that of *security*. Policymakers must ensure that only lawful interception is likely to occur. That would include both governmental misuse and hackers. Security in IoT devices is important for various reasons, but within the context of this Article, it is crucial to safeguard the potential abusive power of the vulnerabilities that could be included within the IoT devices in order to comply with legal

214 *See* 18 U.S.C. § 2518(5) (2019).

215 *See* Alex B. Lipton, Note, *Privacy Protections for Secondary Users of Communications-Capturing Technologies*, 91 N.Y.U. L. REV. 396, 398-99 (2016).

216 *See* 18 U.S.C. § 2515. While such evidence might also be found in wiretapping of phones or bugging, when dealing with an always-on device, one might argue that *Wiretapping of Things* might result in capturing more incriminating evidence on these individuals.

217 For further information on use restriction, see Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH. L. REV. 1 (2015); Simmons, *supra* note 82, at 148.

218 For more on the use of big data analysis in criminal investigations, see Stephen E. Henderson, *Our Records Panopticon and the American Bar Association Standards for Criminal Justice*, 66 OKLA. L. REV. 699, 722-23 (2014). For more on the implications of big data analysis on privacy, see, e.g., Jane Bambauer, *Hassle*, 113 MICH. L. REV. 461 (2015); Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327 (2015); Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259 (2012).

obligations.[219] Thus, if the enabling of IoT devices for lawful wiretaps decreases security for other users, then *Wiretapping of Things* should not be allowed unless the agency requesting the warrant is able to prove in that particular case that the wiretapping can be done without such a decrease.

One final example of such considerations is *success*. As wiretapping IoT might be highly intrusive to individuals' lives, policymakers must evaluate and reexamine whether real-time access to IoT actually achieves its purposes for fighting criminal activity. If criminals will become aware of these practices, they might be reluctant to use such devices or simply use commercial off-the-shelf encryption software to ensure that their data will remain secure.[220] Arguably, many of them will not likely use a Fitbit or an Amazon Echo.[221] It will mainly affect the privacy interests of everyone else who will be less aware of these practices. This challenge might go even further due to the use of encrypted networks like that of Tor[222] — or any equivalent that will rise in years to follow — leading many individuals to opt for ways to keep their communications secure.[223] Thus, if *Wiretapping of Things*

[219] The state of California has recently passed a bill which requires IoT manufacturers to include "reasonable security features" within their devices. *See* Luana Pascu, *California Passes Cybersecurity Law for Connected Devices, Receives Mixed Feedback*, BITDEFENDER (Oct. 2, 2018), https://www.bitdefender.com/box/blog/iot-news/california-passes-cybersecurity-law-connected-devices-receives-mixed-feedback/?cid=soc%7Cbox%7cfb%7Cnoncomm (discussing how the state of California has recently passed a bill which requires IoT manufacturers to include "reasonable security features" within their devices).

[220] *See* Opderbeck, *supra* note 27, at 1672 (arguing that users can easily encrypt their personal storage media using inexpensive commercial off-the-shelf full disk encryption software, but that most individuals do not do so).

[221] *But see* Bellovin et al., *Lawful Hacking*, *supra* note 173, at 15 (arguing that "criminals are like other people: few use cutting edge or experimental devices to communicate. Instead, they stick with COTS [Commercial Off-The-Shelf] products"); *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 2, 18 (2011) (statement of Valerie Caproni, General Counsel, FBI), https://www.govinfo.gov/content/pkg/CHRG-112hhrg64581/html/CHRG-112hhrg64581.htm ("Criminals tend to be some-what lazy, and a lot of times, they will resort to what is easy.").

[222] Tor is an acronym of "The Onion Router," a free software for enabling anonymous and encrypted communication. *See Tor: Overview*, TOR PROJECT, https://www.torproject.org/about/overview.html.en (last visited Feb. 1, 2019).

[223] For more on the challenges of encryption to law enforcement, see U.S. DEP'T OF JUSTICE, AG'S CYBER DIGITAL TASK FORCE, *supra* note 31, at 116 ("The advent of such widespread and increasingly sophisticated encryption technologies that prevent lawful access poses a significant impediment to the investigation of most types of criminal activity, including violent crime, drug trafficking, child exploitation, cybercrime,

eventually does not advance enforcement needs, then it should be abandoned as a practice.

These requirements are important not only to protect privacy, but also as such wiretapping practices could affect the use of IoT devices by ordinary users.[224] Knowing that one's IoT device was streaming all one's data all the time could have a negative effect on its use. While this argument might also be true for other devices, like a smartphone, IoT might be different. Arguably, unlike the use of mobile phones, IoT is not generally a necessity. And upon knowledge that these devices could be activated by governmental agencies, it would seem like an unnecessary risk for many individuals, even for those who argue that they have "nothing to hide." They might simply cease using such technologies, unless the trade-off will be worthwhile for them.[225] Thus, they will opt for the personal assistant that could guarantee that no direct interception could ever occur, if such devices even exist.

In other words, enabling the *Wiretapping of Things* through ultra-warrants must take into account the potential impact on human rights and liberties, and perhaps mostly the right to privacy. As people should feel safe in their homes and in person, both physically and mentally, turning IoT into spying devices could very well pose a threat to privacy. At this point, it is important for policymakers to acknowledge that current super-warrant requirements are inadequate, as securing the house as a surveillance-free space is also highly essential for the exercise of other civil rights and liberties, such as free speech and free association, and the *Wiretapping of Things* could create a chilling effect on the use of IoT.[226] It is essential to a democracy for individuals to feel that they can freely share their thoughts while surrounded by technology. If the home is one's castle,[227] and this notion is embedded

money laundering (including through cryptocurrencies), and domestic and international terrorism.").

[224] Generally, super-warrants necessitate that the wiretapped individual will be notified on the wiretap no later than ninety days after the completion of the wiretap. *See* 18 U.S.C. § 2518(8)(d) (2019).

[225] For more on the chilling effect of surveillance on technology use, see Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117, 126 (2016).

[226] *Cf.* Hibbard, *supra* note 40, at 389 ("[T]here is an inherent fear that chilling of speech could occur. . . . In the case of Internet wiretaps, the fear that private information communicated to other parties could be intercepted by the government or hackers could cause pervasive anxiety.").

[227] The notion of the home as one's castle appeared as early as 1499. *See* Solove, *A Brief History*, *supra* note 7, at 4; Note, *The Right to Privacy in Nineteenth Century America*, 94 HARV. L. REV. 1892, 1894 n.18 (1981).

within the Third, Fourth, and Fifth Amendments,[228] then our castles are in great need of legal protection. With exceptions,[229] warrantless searches and seizures inside a home are considered unreasonable by default for a reason.[230]

If we consider the protection afforded by the Fourth Amendment, then the fact that many of these devices reside in our houses might make a difference. In the words of the Supreme Court: "The Fourth Amendment has drawn a firm line at the entrance to the house."[231] It could even become more intrusive than just within the house due to the developments of the Internet of Bodies, which might enable agencies to acquire real-time information of what goes on within the suspect's body, e.g., his voice (from within the body), heart rate, glucose level, and blood pressure, through devices such as smart contact lenses, cochlear implants, and Bluetooth-equipped electronic pills.[232] Congress must acknowledge the potential privacy implications that would arise from such warrants.

These considerations, while normatively important, could become somewhat meaningless practically lacking transparency and oversight mechanisms. In other words, the *Wiretapping of Things* must be embedded with higher procedural safeguards. Policymakers must implement mechanisms that would, at the very least, increase transparency and oversight to ensure that law enforcement agencies comply with the warrant's requirements. While always a crucial element in protecting human rights and liberties, the need or necessity for transparency and oversight increases in IoT wiretapping. Many IoT devices are becoming integral to our daily lives, and many times they are effectively acting as internet-based sensors, like microphones sitting inside our houses. More transparency regarding the types of devices tapped and data that is acquired is needed to assess their potential impact on privacy and other human rights. Individuals must possess a right to review IoT access, *ex post* at the very least, as to fight against overbroad requests.[233] Such transparency must be dual: to the user from the companies prior to consenting to use the IoT device in a clear and understandable manner, and governmental transparency regarding the

---

228 Solove, *A Brief History*, *supra* note 7, at 5.

229 *See supra* note 83 and accompanying text.

230 *See* Payton v. New York, 445 U.S. 573, 586 (1980).

231 *Id.* at 590.

232 *See* Mary Lee, *The 'Internet of Bodies' is Setting Dangerous Precedents*, WASH. POST (Oct. 15, 2018, 10:39 AM), https://www.washingtonpost.com/news/theworldpost/wp/2018/10/15/health-data/?utm_term=.9ea8d9835f86.

233 *See* Whittaker, *supra* note 211.

actual use of these devices in investigations. As Freedom of Information Act ("FOIA") requests will not aid in transparency much, as it will likely exclude law enforcement records for the *Wiretapping of Things*,[234] courts will have to carefully consider whether to issue non-disclosure orders for any type of IoT data that is revealed.[235]

Generally, the future of the right to privacy will greatly depend on how the regulatory framework will be shaped, and whether effective oversight mechanisms will be feasible. In this respect, the Fourth Amendment protection of online activity and the third-party doctrine must also be reexamined,[236] especially if the use of IoT will reach a societal tipping point and transform it from convenience to necessity.[237] Courts must thus modify the scope of the third-party doctrine and adjust it to a new era of privacy expectations. Unlike famous idioms on the demise of privacy[238] — or social changes that made individuals value

[234] *See* 5 U.S.C. §§ 552(b)(7)(E), 552(c) (2019).

[235] Indeed, the FBI has already replied to a request regarding the potential wiretapping of Amazon Echo devices, neither confirming nor denying such practices. *See* Matt Novak, *The FBI Can Neither Confirm Nor Deny Wiretapping Your Amazon Echo*, GIZMODO (May 11, 2016, 5:00 PM), https://paleofuture.gizmodo.com/the-fbi-can-neither-confirm-nor-deny-wiretapping-your-a-1776092971; Jana Winter, *How Law Enforcement Can Use Google Timeline to Track Your Every Move*, INTERCEPT (Nov. 6, 2015, 6:53 AM), https://theintercept.com/2015/11/06/how-law-enforcement-can-use-google-timeline-to-track-your-every-move.

[236] *See, e.g.*, Patricia L. Bellia & Susan Freiwald, *Law in a Networked World: Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 149 (2008); Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199, 1202 (2009); Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 689 (2011); Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 296-99 (2005); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1009 (2010) [hereinafter *A General Approach*]; Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1247 (2009); Ric Simmons, *From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1321-35 (2002); Solove, *Digital Dossiers*, *supra* note 20, at 1138-39 (2002); Jonathan Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. F. 83, 92 (2005); *cf.* Kerr, *Third Party Doctrine*, *supra* note 87, at 563-66; Orin S. Kerr, *Defending the Third-Party Doctrine: A Response to Epstein and Murphy*, 24 BERKELEY TECH. L.J. 1229, 1229 (2009). For more on the need to reconfigure the third-party doctrine due to IoT, see generally Note, *If These Walls Could Talk*, *supra* note 47, at 1942-45.

[237] *Cf.* Katz v. United States, 389 U.S. 347, 352-53 (1967) ("To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."); Robison, *supra* note 100, at 1230 (in the context of cloud computing).

[238] *See supra* note 154 and accompanying text.

privacy in a different manner[239] — users cannot be expected to understand that all of their data that is captured by IoT devices could be divulged to the state without strict statutory limitations. It will put almost any second of life under constant surveillance that might be accessed by governmental entities without proper procedural safeguards. Even if we acknowledge that under the assumption of risk principle, people will expect that IoT devices equipped with sensors could be wiretapped, such a lack of privacy expectation would effectively lead to living in a world that disregards civil rights and liberties.

At the very least, courts must not apply the third-party doctrine for IoT devices that are not "always-on." While consumers might expect that their communications with Alexa could very well fall under the third-party doctrine in some instances, and while the regulatory framework that governs access to stored communications might also not fit within this new technology, allowing enforcement agencies to activate these devices without users' awareness goes well beyond any subjective or objective expectation of privacy under the *Katz* test. That data was not effectively shared with a third party, and thus, the third-party doctrine should not be invoked. But even always-on devices should enjoy some level of constitutional protection. When the always-on technology is integral to the device's operation, like a smart refrigerator, an individual's expectation of privacy might still persist. Thus, in those instances, even if the constitutional protection does not generally apply, the regulatory framework should protect consumers, as they are left solely to rely on companies' policies, while the smartification trend will eventually leave consumers without dumb machines.

This notion extends far beyond the security of one device or another. With the smartification of private household objects, we will likely also experience the smartification of the public sphere. While the smart home is privately owned, and perhaps will not be accessible to governmental agencies, the outdoors will be a different story. We will use smart cars, driven in the streets of a smart city, which is part of a smart state. Here, the control of the state could be vast. It could require, for instance, manufacturers of smart cars to enable wiretapping whenever requested — which could in turn depend on a license to

239 *See, e.g.*, JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 101 (2008) ("Digital Natives, who live so much of their lives in networked publics, are unlikely to come to see privacy in the same terms that previous generations have, by and large.").

operate. Infrastructure will likewise depend on the state, if not already owned and operated by it.

To that extent, one of the major concerns with the enabling of IoT wiretapping goes well beyond the individual's privacy in the context of his or her data. It applies to society as a whole, as these exploits might very well be exploited by governmental agencies or other malicious entities. When the physical infrastructure exists, it leaves the consumer relying on security,[240] data policies of the companies, and the legal regime that governs such use.[241] If the smart world will be subject to trust in the government not to misuse its powers, then individuals might not feel safe anywhere.

As a potential glimpse to the future, the smartification of everything could even increase the potential threat to privacy and other civil rights and liberties due to datamining and data analysis capabilities. For instance, with the potential use of biometric identification methods, like that of facial and voice recognition,[242] enforcement might move towards the detection of suspects by wiretapping everything and everyone. With a computerized scan, law enforcement agencies might search for a suspect's voice over the network as it was captured by an IoT device, identify him or her, and even analyze various attributions of his mental state or location.[243] It will require them to obtain voiceprints of the suspect, which they could gather from the IoT companies that store such data.[244] Reporters claim that such programs have in fact been in use by the National Security Agency ("NSA") since 2004.[245] When searching for a suspect, enforcement agencies might turn to these private companies, whether acting under the regulatory framework

[240] These are already subject to criticism as providing poor security measures. *See* Nick Feamster, *Mitigating the Increasing Risks of an Insecure Internet of Things*, 16 COLO. TECH. L.J. 87, 89 (2017).

[241] *See* Stanley, *supra* note 157.

[242] It should be noted that while speech recognition refers to the ability to speak naturally and contextually with a computer system in order to execute commands or dictate language, voice recognition refers to identifying the speaker, not the speech. *See* GRAY, *supra* note 47, at 4. For more on the potential implications of facial recognition on privacy, see generally Douglas A. Fretty, *Face-Recognition Surveillance: A Moment of Truth for Fourth Amendment Rights in Public Places*, 16 VA. J.L. & TECH. ASS'N 430 (2011).

[243] *See* Judith Shulevitz, *Alexa, Should We Trust You?*, ATLANTIC (Nov. 2018), https://www.theatlantic.com/magazine/archive/2018/11/alexa-how-will-you-change-us/570844.

[244] *See* Russell Brandom, *The NSA's Voice-Recognition System Raises Hard Questions for Echo and Google Home*, VERGE (Jan. 22, 2018, 3:37 PM), https://www.theverge.com/2018/1/22/16920440/amazon-echo-google-home-nsa-voice-surveillance.

[245] *See id.* (describing a "system known as Voice RT, which was able to match speakers to a given voiceprint").

requirements or simply asking them to do so voluntarily, and scan their network against the suspect's voiceprint.[246] Indeed, police officers already began to implement IoT devices like smart bracelets, smart clothing, and smart firearms for the purpose of better identifying suspects and arresting individuals.[247] But even lacking presumptions about the future of law enforcement, the public sphere is already more embedded with sensors that could detect real-time gunshots,[248] and some could even be equipped with voice and facial recognition, thus enabling law enforcement agencies to intercept everything in real time and detect criminal activity and suspects of crimes.[249]

As the smartification of lives could blur traditional distinctions like outdoor/indoor,[250] privacy must be closely monitored — but not in a literal sense.[251] Thus, any new enforcement mechanism necessitates rethinking of the regulatory framework that governs such access. Both Congress and the courts must readapt the checks and balances that were previously set under the regulatory framework that governs access to communication and wiretapping to the always-on era. Without such proper checks and balances, liberal democracies might make a transition into totalitarian regimes.

CONCLUSION

Our notion of privacy — or our expectation of it — is not a constant. It changes over time, and technology can shape much of our perception of it. It does not mean that privacy is dead, not for now at least. It only

246 *Id.*

247 *See* Colin Neagle, *How the Internet of Things is transforming law enforcement*, NETWORKWORLD (Nov. 3, 2014, 6:33 AM), https://www.networkworld.com/article/2842552/internet-of-things/how-the-internet-of-things-is-transforming-law-enforcement.html.

248 *Id.*

249 *See generally* Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV. 1283, 1349-53 (2014) (discussing Fourth Amendment protection from surveillance technologies in public). For a general review on the smartification of both the private and public spheres, see generally BRUCE SCHNEIER, CLICK HERE TO KILL EVERYBODY: SECURITY AND SURVIVAL IN A HYPER-CONNECTED WORLD (2018).

250 Within the context of the penetration of the internet to our homes, Ellen Ullman argued "[t]he boundary between the outside world and the self is penetrated. And the boundary between your home and the outside world is penetrated." Rory Carroll, *Goodbye Privacy, Hello 'Alexa': Amazon Echo, the Home Robot Who Hears it All*, GUARDIAN (Nov. 21, 2015, 7:07 AM), https://www.theguardian.com/technology/2015/nov/21/amazon-echo-alexa-home-robot-privacy-cloud.

251 *See* Kerr, *A General Approach*, *supra* note 236, at 1009-12.

means that with advancements in technologies that aid law enforcement agencies in their investigatory powers, we should be wary that such powers will not be misused or will be overly broad, potentially leading to fishing expeditions. For that, policymakers must acknowledge the privacy and other human rights concerns that arise from the implementation of any new technology, especially within the always-on era. They must reevaluate and reconfigure the checks and balances that were set for prior technologies and adapt them to properly cover innovative technologies like that of IoT.

The use of IoT for law enforcement purposes becomes highly relevant in an era of ubiquitous surveillance. While we came to understand under Edward Snowden's revelations that enforcement agencies like the NSA have the abilities to capture our conversations and online activities, this form of surveillance could even mark a step-up in their capabilities. If IoT truly becomes always-on, then that means that we will all have microphones, sensors, and even cameras wherever we go, and perhaps primarily, inside our own homes, blurring the boundaries between private and public spheres. Lacking proper safeguards, democracy is at great risk. Thus, policymakers must acknowledge, evaluate, and reconfigure the current regulatory framework that governs both access to IoT communications and perhaps most importantly, the *Wiretapping of Things*. Otherwise, civil rights and liberties like that of the right to privacy will effectively be dissolved from this world.