Washington Journal of Law, Technology & Arts

Volume 13 | Issue 1 Article 2

10-1-2017

Neighborhood Watch 2.0: Private Surveillance and the Internet of Things

Daniel Healow

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 13, ISSUE 1 FALL 2017

NEIGHBORHOOD WATCH 2.0: PRIVATE SURVEILLANCE AND THE INTERNET OF THINGS

Daniel Healow[*]

Cite as: 13 Wash. J.L. Tech. & Arts 1 (2017)

http://digital.law.washington.edu/dspace-law/handle/1773.1/1748

ABSTRACT

The use of low-cost cameras and internet-connected sensors is sharply increasing among local law enforcement, businesses, and average Americans. While the motives behind adopting these devices may differ, this trend means more data about the events on Earth is rapidly being collected and aggregated each day. Current and future products, such as drones and self-driving cars, contain cameras and other embedded sensors used by private individuals in public settings. To function, these devices must passively collect information about other individuals who have not given the express consent that is commonly required when one is actively using an online service, such as email or social media. Generally, courts do not recognize a right to privacy once a person enters public spaces. However, the impending convergence of privately-owned sensors gathering information about the surrounding world creates a new frontier in which to consider private liberties, community engagement, and civic duties. This Article will analyze the legal and technological developments surrounding: (1) existing data sources used by local law enforcement; (2) corporate assistance with law enforcement investigations; and (3) volunteering of personal data to make communities safer. After weighing relative privacy interests, this Article will explain, under current laws, the utility of private data to make communities safer, while simultaneously

[*] Daniel Healow, University of Washington School of Law, Class of 2018. Thank you to my colleagues on WJLTA for their feedback and editorial work, my topic advisor, Assistant Professor Ryan Calo, for sharing his expertise on these issues, and my friends and family for their support and encouragement.

advancing the goals of fiscal responsibility, government accountability, and community engagement.

TABLE OF CONTENTS

INTRODUCTION

Surveillance programs are generally pictured as large-scale and well-funded efforts that governments or other state actors undertake directly. But what if the government empowered individual citizens to contribute photos or videos passively collected from products they already own to help solve crimes in their communities?

"Neighborhood watch" programs have roots tracing back to American colonial settlements, and have long been encouraged by local law enforcement to supplement their crime-fighting efforts and foster a shared sense of community.[1] Residents in these programs are encouraged to report suspicious activity in their communities, share information with their neighbors, and promote safety.[2]

While neighborhood watch programs are generally considered effective at crime prevention in their own right,[3] people cannot constantly watch their surroundings. The Internet of Things (IoT) has the potential to fill these gaps and jumpstart a new era of community involvement in crime prevention. While the IoT manifests its presence in the world through physical "sensors" the real game-changing value comes from using internet-connected machines to ingest sensor data and analyze it in real time to provide actionable insights.[4] Put simply, these sensors measure, evaluate, and gather data.[5] Installations and uses of this technology, which already monitors physical things such as homes, bridges, vehicles, and traffic, are expected to rapidly increase in the coming decade.[6]

---

[1] *See Neighborhood Watch*, NAT'L CRIME PREVENTION COUNCIL (Nov. 4, 2016), http://www.ncpc.org/topics/home-and-neighborhood-safety/neighborhood-watch.

[2] *Id*.

[3] *E.g.*, *Does Neighborhood Watch Reduce Crime?*, NAT'L CRIME PREVENTION COUNCIL (JULY 10, 2008), http://www.ncpc.org/resources/files/pdf/neighborhood-safety/does-neighborhood-watch-reduce-crime.pdf.

[4] *E.g.*, Daniel Burrus, *The Internet of Things is Far Bigger Than Anyone Realizes*, WIRED (Nov. 4, 2016), https://www.wired.com/insights/2014/11/the-internet-of-things-bigger/.

[5] *Id*.

[6] *Id.*

People are used to having their data collected when they are direct users of a product or service, but the adoption of IoT devices changes the data sharing dynamic. What makes many IoT devices unique is that they capture information about the environment as a whole rather than just individual user information,[7] thus implicating the privacy rights of non-participants. With a large amount of data being collected at minimal cost to localities, IoT deployment represents a prime, new investigative resource for local law enforcement. Currently voluntary data disclosure regulation is limited, thus communities, corporations, and local governments must initiate discussion about how to encourage or limit the use of private data.[8] Having these discussions now will help minimize negative externalities in the coming public data revolution.

I. PRIVACY LAW GOVERNING PUBLIC SPACES

A. Overview

There is little to no restriction on how most information gathered by privately-owned IoT devices may be used by the device owner.[9] One possible source for restriction is the Fourth Amendment, which protects citizens against unreasonable searches and seizures.[10] However, recent Supreme Court jurisprudence has reinforced the doctrine that collection of "visual information" does not constitute a "search" for purposes of the Fourth Amendment.[11] Additionally, third parties who provide information about others to law enforcement generally may do so without implicating that person's Fourth Amendment rights.[12] This specific allowance of "visual" information is critical in the IoT era, as it represents a large portion of the data that will be incidentally collected and stored.[13]

---

[7] *See, e.g.*, *id.* (providing the example of smart city infrastructure).

[8] *Cf.* Smith v. Maryland, 442 U.S. 735 (1979) (affirming the third-party doctrine, meaning law enforcement may use information freely provided by a third-party).

[9] *Id.*

[10] U.S. CONST. amend. IV.

[11] *See, e.g.*, United States v. Jones, 565 U.S. 400, 410 (2012).

[12] *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976).

[13] *See, e.g.*, Davide Santo, *Autonomous Cars' Pick: Camera, Radar, Lidar?*,

Ultimately, requesting information gathered by the public sidesteps the few existing legal hurdles barring such a program today.

B.The "Reasonable Expectation of Privacy" Standard

Original Fourth Amendment interpretation was based on traditional notions of property rights.[14] However, the Supreme Court updated this standard in 1967 to address more "modern" privacy challenges, finding that the touchstone of Fourth Amendment analysis is whether a person has a "constitutionally protected reasonable expectation of privacy."[15] *Katz* broadened the scope of the inquiry from whether law enforcement committed a "physical trespass" to whether there was an "invasion" of a reasonable expectation of privacy.[16] *Katz* also led to a new two-part test isolating the factors that establish this "reasonable expectation": (1) "whether the individual, by his conduct, has 'exhibited an actual (subjective) expectation of privacy,'" and (2) "whether the individual's subjective expectation of privacy is 'one that society is prepared to recognize as 'reasonable.'"[17] Thus, the breadth of individual privacy rights under the Fourth Amendment are determined by weighing both an individual's actual conduct and societal values.

C.Third-Party Information

While the Fourth Amendment provides individuals with some safeguards against government information collection, information shared with others enjoys much less protection.[18] The Court later

---

EETIMES (JULY 7, 2016), https://www.eetimes.com/author.asp?section_id=36&doc_id=1330069 (explaining the large amount of data collected by autonomous vehicles, with cameras as the "volume leader").

[14] *E.g.*, Florida v. Jardines, 569 U.S. 1, 11 (2013) (noting the "traditional property-based understanding of the Fourth Amendment").

[15] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

[16] California v. Ciraolo, 476 U.S. 207, 219 (1986).

[17] Smith v. Maryland, 442 U.S. 735, 740 (1979).

[18] *See, e.g.*, *Smith*, 442 U.S. 735 at 743-744; United States v. Miller, 425 U.S. 435, 433 (1976).

built upon *Katz* in finding private third parties may share information on a target subject with law enforcement for use in an investigation: "[w]hat a person knowingly exposes to the public…is not a subject of Fourth Amendment protection."[19] The *Miller* court reasoned under the *Katz* test that a bank and its customers had no "reasonable expectation of privacy" by virtue of their relationship, as the information had become a business record of the bank.[20] This decision is especially significant given the relationship between the parties: the individual was a customer of a bank, and the bank later provided law enforcement with records of his transactions.[21] Therefore, if this precedent holds with parties in a business relationship, those not in privity of contract will have an especially difficult burden to establish infringement on their reasonable expectations of privacy when the information is gathered in a public forum.

D.Self-Determination of Privacy Expectations

The rise of industrialization and the growth of metropolitan cities created major population centers that changed the implied social contract for living in such a community.[22] Courts recognize there is no uniform expectation of physical privacy throughout the United States, and instead variations are to be expected based on self-selection of living environment.[23] In *Vargas*, the court found people living in a "rural" environment can reasonably expect greater levels of privacy than urban dwellers due to the low likelihood of passersby.[24] Factors such as "gravel roads," "distant neighbors," and "no public sidewalks" suggest a higher expectation of privacy.[25]

In contrast, urban areas with major public thoroughfares are

[19] *Miller*, 425 U.S. at 442.
[20] *Id.*
[21] *Id.*
[22] Howard Gillman, The Constitution Beseiged: The Rise and Demise of Lochner Era Police Powers Jurisprudence 76-86 (Duke University Press 1993).
[23] *See, e.g.*, United States v. Vargas, No. CR-13-6025-EFS, 2014 U.S. Dist. LEXIS 184672 (E.D. Wash. Dec. 15, 2014).
[24] *Id.* at 20.
[25] *Id.*

more likely to be frequented by IoT devices with sensors,[26] and surrounding residents are also less likely to have a valid privacy expectation in property exposed to roadways. The Supreme Court has gone so far as to say that under certain conditions there is no right to privacy on public land.[27] In *Knotts*, the Court held that a person traveling in an automobile on public roads has no reasonable expectation of privacy in his or her movements from one place to another.[28] Thus, locality attributes are likely to play a significant factor in the development of public opinions and reasonable expectations on the use of IoT data by local law enforcement.

However, physical setting is not the only factor that makes a privacy expectation "reasonable." While geographical attributes are likely to remain fairly consistent over time, the Court has also indicated that the development of new technology represents a more elastic variable that can change reasonable societal expectations of privacy.[29] The *Jones* court found that "[t]he availability and use of . . . new devices will continue to shape the average person's expectations about the privacy of his or her daily movements."[30] The adoption of IoT products and services in the coming years will likely reduce this overall "reasonable expectation" of privacy, especially in cities. With an estimated 50 billion new sensors connecting to the internet by 2020,[31] the adoption of new IoT technologies encourages consideration of whether the same legal framework and surveillance programs make sense in this new era of technology. The use of IoT data by local law enforcement presents a prime issue for public input based on the Court's interpretation of "reasonable expectations" of privacy in relation to local attributes.

---

[26] *See, e.g.*, Burrus, *supra* note 4.
[27] *E.g.*, United States v. Knotts, 460 U.S. 276, 281 (1983).
[28] *Id.*
[29] *E.g.*, United States v. Jones, 565 U.S. 400, 429 (2012).
[30] *Id.*
[31] *See, e.g.*, *CEO to shareholders: 50 billion connections 2020*, ERICSSON, (Apr. 2010), https://www.ericsson.com/en/press-releases/2010/4/ceo-to-shareholders-50-billion-connections-2020.

II. CURRENT INFORMATION GATHERING PROGRAMS

While various forms of neighborhood watch programs have been used for years in communities throughout the country, the format has not significantly changed. Typically, information is generally spread person-to-person or through neighborhood meetings.[32] Citizens report crime tips to law enforcement,[33] but it is not always clear whether the relayed information will be acted upon or whether it is particularly useful. While this communication method may work in some situations, IoT technology has the potential to collect useful information and discharge their public safety responsibilities in a cost-effective manner.

A.Local Governments

Local law enforcement agencies have already begun utilizing cameras to collect information for investigations and to improve public safety.[34] The speed, efficiency, and increased widespread use of such systems is causing public concern over government collection of data.[35] Adding to the confusion, community groups often condition their support for body cameras on implementation of privacy and publication policies, rather than the use of the technology itself.[36] Ultimately, the propensity for legal challenges and costs, demonstrates the benefits of moving towards crowdsourcing of data collection.

1. Direct Data Collection by Law Enforcement

---

[32] *See, e.g.*, *Neighborhood Watch*, *supra* note 1.

[33] *See, e.g.*, *Neighborhood Watch*, *supra* note 1.

[34] *See, e.g.*, Kaveh Waddell, *How License-Plate Readers Have Helped Police and Lenders Target the Poor*, THE ATLANTIC (Apr. 22, 2016), http://theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436.

[35] *Id.*

[36] *See, e.g.*, American Civil Liberties Union, *Police Body Cameras*, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/police-body-cameras (providing one example of implementation-dependent support).

Law enforcement agencies are increasingly looking to technology as a means of accomplishing public safety goals while mitigating the effects of reduced budgets and fewer officers. The most recent technology receiving notoriety is body-worn cameras. With increasing public scrutiny of police use of force, departments across the country are rapidly deploying body cameras as a means of documenting incidents through an impartial lens.[37] While these cameras seemingly represent increased government surveillance of the public, civil liberties groups are generally in support of the technology as long as policies are in place to maximize accountability.[38] The relative value of having video evidence, as long as it is properly implemented, is thought to outweigh the associated privacy interest.[39] Los Angeles is spending nearly $60 million over five years to provide over 7,000 officers with body cameras.[40] However, purchasing the camera equipment itself is only a small fraction of the roll-out challenge. In addition to storing the roughly 10,000 hours per week of video generated by police in large cities,[41] employees must be assigned to review the footage and evaluate usage.[42]

Since state governments have been slower to react to this new technology,[43] "police departments . . . have been left on their own"

---

[37] *E.g.*, Mike Maciag, *Survey: Almost All Police Departments Plan to Use Body Cameras*, GOVERNING (Jan. 26, 2016), http://www.governing.com/topics/public-justice-safety/gov-police-body-camera-survey.html.

[38] *See, e.g.*, American Civil Liberties Union, *supra* note 36.

[39] *Id.*

[40] Kate Mather & David Zahniser, *City Council vote resumes $57.6-million rollout of LAPD body Cameras*, LOS ANGELES TIMES (June 22, 2016), http://www.latimes.com/local/lanow/la-me-ln-lapd-body-cameras-20160622-snap-story.html.

[41] *E.g.*, John Sanburn, *Storing Body Cam Data is the Next Big Challenge for Police*, TIME (Jan. 25, 2016), http://time.com/4180889/police-body-cameras-vievu-taser/.

[42] *See, e.g.*, *For police body cameras, big costs loom in storing footage*, CHICAGO TRIBUNE (Feb. 6, 2015), http://chicagotribune.com/bluesky/technology/chi-body-cameras-hidden-costs-20150206-story.html.

[43] *See, e.g.*, Niraj Chokshi, *These are the states that want to regulate police body camera videos*, WASHINGTON POST (Feb. 25, 2016),

and forced to "improvise" when it comes to applying existing laws to this new data source.[44] One of the largest unintended consequences has been the application of Public Records Acts to body camera footage. There has already been at least one attempt to force a department to release all footage collected, a task that was purported to take four years to complete.[45] While the cameras help solve some immediate challenges facing communities, subjecting a vast new database to established laws creates new problems demanding a rapid policy response to avoid undesirable consequences.

Though costly to implement,[46] investments in body cameras are already proving useful for many municipalities. Studies show that use of body cameras may reduce police use of force by nearly 50%, while citizen complaints have declined by over 90%.[47] Thus, the use of cameras appears to have a highly desirable impact on public safety and accountability from both the standpoint of the public as well as law enforcement.

While deployment of body cameras for police accountability purposes is generally viewed in a positive light, the use of cameras to improve the efficiency of policing efforts has received a sharply contrasting response. One such implementation is license plate-reading technology.[48] License plate camera systems may be

---

https://www.washingtonpost.com/news/post-nation/wp/2016/02/25/these-are-the-states-that-want-to-regulate-police-body-camera-videos/?utm_term=.989d558fbcee7.

[44] Kate Mather & Cindy Chang, *Fresno police break ranks with other departments by releasing shooting video from body camera*, LOS ANGELES TIMES (July 15, 2016), http://www.latimes.com/local/california/la-me-fresno-police-body-cameras-20160714-snap-story.html.

[45] *E.g.*, Andrew Binion, *Body cam legislation in the works as more requests come in*, KITSAP SUN (Nov. 22, 2014), http://www.kitsapsun.com/news/local/body-cam-legislation-in-the-works-as-more-requests-come-in-ep-792583825-355115031.html.

[46] Jason Kotowski, *Money, Storage Primary Obstacles in Police Body Camera Implementation*, EMERGENCY MANAGEMENT (March 8, 2016), http://www.govtech.com/em/safety/Police-Body-Cam-Installation.html.

[47] *E.g.*, Barak Ariel, *Do Police Body Cameras Really Work?*, IEEE SPECTRUM (May 4, 2016), http://spectrum.ieee.org/consumer-electronics/portable-devices/do-police-body-cameras-really-work.

[48] *See, e.g.*, Kim Zetter, *Even the FBI Had Privacy Concerns on License*

mounted to infrastructure or mobile vehicles, where they take photos of license plates which are stored on a database.[49] Photographic records can be linked and the information gleaned from these records can reportedly be used to track the movement of individuals.[50]

While relatively effective in gathering and aggregating data at scale, the technology has not escaped the criticism of civil liberties groups and even some law enforcement agencies. Documents obtained by the ACLU suggest that in 2012 the FBI put its license plate reader program on hold after concerns over its legality.[51] As many publications note, the primary privacy issue with direct data collection by law enforcement is not the camera, but the centralized "storing and studying [of] people's everyday activities."[52] Thus, the inevitable legal challenges to recently adopted technology enabling direct data collection by law enforcement will play a key role in determining the policing strategies of the future.

2. Challenges to Direct Data Collection by Law Enforcement

While the Supreme Court has shown mixed responses to warrantless use of new police technology, it has remained fairly consistent in permitting the gathering of information that can otherwise be observed with the naked eye.[53] This interpretation stays close to the traditional Fourth Amendment position that "mere visual observation does not constitute a search."[54] The Court has categorized modern investigative tools according to their technological function and scope: (1) expanding the abilities of officers to use the naked eye from public thoroughfares, (2) expanding the abilities of officers to see "beyond" the naked eye

Plate Readers, WIRED (May 15, 2015), https://www.wired.com/2015/05/even-fbi-privacy-concerns-license-plate-readers/.

[49] *See, e.g.*, Waddell, *supra* note 34.

[50] *Id.*

[51] Zetter, *supra* note 48.

[52] Conor Friedersdorf, *An Unprecedented Threat to Privacy*, THE ATLANTIC (Jan. 27, 2016), http://www.theatlantic.com/politics/archive/2016/01/vigilant-solutions-surveillance/427047/.

[53] *E.g.*, United States v. Jones, 565 U.S. 400, 412 (2012).

[54] *Id.*

from public thoroughfares, and (3) expanding the abilities of officers with no line of sight.

In addition to finding no reasonable expectation of privacy when individuals are on a public street, the Court has found a similar lack of a cognizable privacy right from human aerial observation. For example, pre-warrant surveillance of a suspect's backyard by an officer looking out of an airplane at 1,000 feet was found lawful.[55] The *Ciraolo* court held that even though the suspect may have established a subjective expectation of privacy, that expectation was neither reasonable nor one "that society is prepared to honor."[56] Later decisions indicate altitude is not a determining factor in the "reasonableness" evaluation.[57] The *Riley* court noted "in an age where private and commercial flight in the public airways is routine," it was unreasonable for the defendant to expect privacy in his backyard activities.[58] Additionally, the court reemphasized that the Fourth Amendment does not protect activity "visible to the naked eye" from "public airways."[59] Thus, public airways appear to extend the same minimal "eyesight" privacy protections existing on ground-based public thoroughfares.

Once police agencies use technology that goes beyond what can be observed with the naked eye, the Court has been less willing to allow warrantless operation. One example of such technology is thermal cameras, which can be operated from a public road yet see through walls and other obstructions to give a rough image of activities inside a home or other building.[60] In *Kyllo*, law enforcement used a thermal camera from a public street to look into a suspected grow house to determine whether lamps for growing marijuana were inside.[61] The Court held that the occupants had been subjected to a "search" in violation of the Fourth Amendment, as

[55] California v. Ciraolo, 476 U.S. 207, 213–214 (1986).
[56] *Id.* at 214.
[57] Florida. v. Riley, 488 U.S. 445 (1989).
[58] *Id.* at 450.
[59] *Id.*
[60] Kyllo v. United States, 533 U.S. 27, 29 (2001).
[61] *Id.*

they satisfied both the subjective understanding and reasonable expectation prongs of the *Katz* test.[62]

The *Kyllo* Court made a particularly valuable observation that will likely prove useful in evaluating future technologies. The opinion notes the expansion of technology has "uncovered portions of the house and its curtilage that once were private."[63] The novel use of thermal cameras led the Court to hold that law enforcement usage "constitute[d] a search – at least where (as here) the technology in question is not in general public use."[64] Therefore, similar to airplanes in *Ciraolo* and helicopters in *Riley*, *Kyllo* suggests "mainstream adoption of technology" and a "reasonable expectation of privacy" exist on a sliding scale. While technological extensions of the "naked eye" are infringing at this point in time, they may be considered reasonable in the future depending on increased use, especially among consumers.

Finally, technologies enabling law enforcement to "track" individuals have received a more adamant rejection from the Supreme Court in the absence of a search warrant. Placing a tracking device on an individual's private property is a clear violation of the right to privacy as established under original Fourth Amendment prohibitions on physical intrusion.[65] In *Jones*, the Court held that law enforcement violated the Fourth Amendment when officers "installed a GPS tracking device on the undercarriage of the Jeep while it was parked in a public parking lot."[66] Despite the Jeep being a vehicle, the Court extended physical property protections equivalent to those of a private home, rendering a *Katz* analysis unnecessary. Though the *Katz* test may have expanded the Court's interpretation of a "reasonable expectation of privacy," physical intrusions remain unconstitutional.[67] Thus, infringing on private property through the use of physical equipment establishes a strong upper bound on the capacity of law enforcement to gather information without obtaining a search warrant.

---

[62] *Id.* at 34.
[63] *Id.*
[64] *Id.*
[65] *E.g.*, United States v. Jones, 565 U.S. 400, 404–05 (2012).
[66] *Id.* at 403.
[67] *Id.* at 407.

3. Why Neighborhood Watch Programs in the IoT Era?

Beyond the economic and social considerations encouraging the development of neighborhood watch programs, the Fourth Amendment framework articulated by the Supreme Court to establish the "reasonable expectation of privacy" provides legal and operational incentives for law enforcement to enlist the help of private citizens. First, citizens provide additional sets of eyes on public thoroughfares, which have been repeatedly reaffirmed as public information under the Fourth Amendment.[68] Second, information gathered by third parties under such circumstances may be used in an investigation without implicating the Fourth Amendment rights of the subject individual.[69] Finally, information collected by the public serves as a useful barometer under the Court's reservation in *Kyllo* to demonstrate that a technology has reached the status of "general public use," and thus a corresponding expectation of privacy by an individual is no longer "reasonable."[70] Therefore, financial, social and legal factors may not only drive existing neighborhood watch programs forward, but could make them stronger than ever with the proper mix of policy changes.

B.Modern Neighborhood Watch Programs

1. Security Camera Registries

In addition to the traditional housing community-based neighborhood watch programs, local security camera registries are another fast-growing tool of civic activists who are concerned with crime in their community.[71] These types of neighborhood watch programs can take two primary forms: (1) businesses provide police with their addresses so they can be contacted for a copy of security video if there is an incident within the vicinity of their locations, and

[68] *E.g.*, *Id*. at 412.

[69] *E.g.*, United States v. Miller, 425 U.S. 435, 441 (1976).

[70] *Kyllo*, 533 U.S. at 34 (2001).

[71] *See, e.g.*, *PPB joins surveillance camera registry program*, KOIN (Apr. 27, 2017), http://koin.com/2017/04/27/ppb-joins-surveillance-camera-registry-program/.

(2) direct connection of security cameras into a centralized city database.[72] While one might expect the public to be hesitant to accept a system of constant monitoring from a centralized location, public surveys appear to indicate the opposite: "86% of adults expect private business surveillance video to help law enforcement identify suspects and solve crimes."[73] Perhaps more surprisingly, over 50% of those surveyed indicated businesses have an affirmative duty to ensure their systems are capable of contributing to police efforts.[74] By doing so, the overall utility of the system increases as more public spaces are recorded. Thus, the effectiveness and low overall social cost of instituting a security camera registry suggests this could be an increasingly useful investigative resource as we enter the IoT era.

2. Wireless Emergency Alerts (WEA)

While fliers and community meetings have traditionally informed the public of threats facing their safety, the exponential rise of cellphones offer a unique tool for authorities who are responsible for keeping those communities safe. The Warning, Alert, and Response Network (WARN) Act of 2006 created a new, voluntary nationwide alert system for communicating with the public during emergency situations.[75] Key provisions of the law set requirements for who may send a message; a qualifying event requires an "imminent threat to the public health or safety."[76] Additionally, the statute recognizes the need to remain current with advancements in technology, charging the National Alert Office with publishing a plan every five years outlining "future capabilities and communications platforms for the [system]."[77] A National Alert System working group comprised of subject area experts also

[72] *See, e.g.*, Kevin Dolak, *Private Surveillance Cameras Catching More Criminals*, ABC NEWS (Jan. 26, 2013), http://abcnews.go.com/US/private-surveillance-cameras-catching-criminals/story?id=18315023.
[73] *Id.*
[74] *Id.*
[75] Warning, Alert, and Response Network Act, Pub. L. No. 109–347 (2006).
[76] *Id.*
[77] *Id.*

regularly meets to make new recommendations based on advancements in technology.[78]

While the WARN Act represents a step in the right direction toward improving public safety, a decade later, the system is under widespread criticism for the slow pace of modernization.[79] After the September 2016 New York and New Jersey bombings, Senator Charles Schumer cited the Wireless Emergency Alert system's lack of ability to send a photo of the suspect as a crucial shortcoming.[80] In the same week, emergency management officials from four major cities, the National Oceanic and Atmospheric Administration, and the National Weather Service each urged the Federal Communications Commission to speed approval of a more advanced system.[81] While the FCC did approve the implementation of phone number and URL linking in WEA messages by 2019, there is still a long way to go before realizing the full potential of IoT to aid public safety.[82] Abilities such as text, photo, or video replies are notable omissions that will be key to IoT's societal contribution. Thus, while means already exist to communicate with the public on safety issues, additional work is necessary before law enforcement can leverage the information sharing capabilities of modern IoT devices.

3. AMBER Alerts

While the WEA system was primarily created to inform the public of threats, the America's Missing: Broadcast Emergency Response (AMBER) Alert system directly enlists the public's help

[78] *Id.*

[79] *See, e.g.*, Diana Goovaerts, *N.Y. Senator Shumer, Emergency Officials Push FCC to Fix "Gaping Loophole" in Wireless Alert System*, WIRELESS WEEK (Sep. 2016), https://www.wirelessweek.com/news/2016/09/ny-senator-schumer-emergency-officials-push-fcc-fix-gaping-loophole-wireless-alert-system.

[80] *Id.*

[81] *Id.*

[82] *See, e.g.*, *FCC Strengthens Wireless Emergency Alerts as a Public Safety Tool*, FCC NEWS (Sept. 29, 2016), https://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0929/DOC-341504A1.pdf.

in locating abducted children. Since the system's creation in 1996, over 800 children have been rescued specifically because of AMBER Alerts.[83] In addition to a message being sent out using the WEA system, warnings "are broadcast on radio and television and [Department of Transportation] highway signs."[84] Broadcast warnings and highways signs are utilized based on the suspected locality of the child, and phones of local citizens are targeted through the WEA system based on their GPS location."[85] Though public safety officials seek to create awareness and participation through AMBER Alert communication, users are still limited in the ways they can respond as a message recipient.[86] While links to phone numbers and picture URLs will improve the system, there is still no planned means of reply other than via phone call.[87] The lack of a digital two-way communications system in response to public alerts raises an important question: how much safer and more effective could public safety efforts become if individuals could respond to a crisis with not only what they see, but also the data captured by their IoT devices?

III. FUTURE SOURCES OF LAW ENFORCEMENT INFORMATION

> [T]he Katz test rests on the assumption that the hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes . . . . In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative . . . A legislative body is

[83] *See AMBER Alert*, U.S. DEPT. OF JUSTICE (Nov. 4, 2016), http://www.amberalert.gov/faqs.htm.

[84] *Id.*

[85] Brad Knickerbocker, *Amber Alerts* THE CHRISTIAN SCIENCE MONITOR (Aug. 11, 2013), http://www.csmonitor.com/USA/2013/0811/Amber-Alerts-How-successful-have-they-been-in-saving-abducted-kids.

[86] *See, e.g.*, *AMBER Alert*, U.S. DEPT. OF JUSTICE (Oct. 12, 2017), http://www.amberalert.gov (explaining the Sept. 29, 2016 FCC policy updates and contact information for NCMEC).

[87] *Id.*

> well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.[88]

While the WEA system and AMBER Alerts have already improved public safety for many years, recent events like the 2016 New York and New Jersey bombings underscore the need for further collaboration between law enforcement/watch programs and modern technologies. While a photo or longer message would serve as a step in the right direction, technology can be more extensively utilized under current Supreme Court privacy interpretations to bolster public safety through improved data sharing. In a short number of years, drones and self-driving cars are expected to revolutionize a number of fields, including transportation, delivery, and mapping. Some of these new IoT technologies are expected to capture information at one gigabyte per second, potentially adding up to two petabytes per year with a single device.[89] For context, that is twice the amount of all of the data stored in all of the academic research libraries in the United States.[90]

With each citizen and business soon collecting seemingly unimaginable amounts of data about the world, there is great potential for communities and government to work together to determine ways for this information to be used for the public good. Despite the passage of hundreds of years of technical advancement since the creation of neighborhood watch programs, relatively little has changed in how information is shared between neighbors and public officers. While in-person interaction between neighbors characterized the first iterations of neighborhood watch programs, soon the technological pieces will be in place for neighborhood watch 2.0.

---

[88] United States v. Jones, 565 U.S. 400, 427–30 (2012) (Alito, J., concurring).

[89] *See, e.g.*, Lucas Mearian, *Self-driving cars could create 1GB of data a second*, COMPUTERWORLD (July 23, 2013), http://www.computerworld.com/article/2484219/emerging-technology/self-driving-cars-could-create-1gb-of-data-a-second.html.

[90] *See, e.g.*, David Schilling, *Knowledge Doubling Every 12 Months, Soon to be Every 12 Hours*, INDUSTRY TAP (Apr. 19, 2013), http://www.industrytap.com/knowledge-doubling-every-12-months-soon-to-be-every-12-hours/3950.

A.Data Sources of Tomorrow

> "[Driverless] cars are going to be out there looking . . . [w]e'll have to put limitations on it. We'll have to encrypt that data and make sure I can't tell that it's John's [car] necessarily . . . but the amount of social good that can come from that far outweighs those concerns." – Brian Krzanich, Chief Executive Officer, Intel, Inc.[91]

1. Corporations/Businesses

As existing security camera registries demonstrate, there is tremendous potential for solving crimes and public safety challenges by creating a mesh network of privately-owned resources. Additionally, technology systems owned by businesses generally have more advanced features and utilize industry standards for interoperability, which are lacking in many consumer products. The growth of IoT gives law enforcement the opportunity to redouble their efforts to collaborate with local businesses and benefit from more investigative data from fewer sources.

a. Principle Benefit – Data Aggregation

Businesses regularly organize the information they collect to improve manageability, creating an opportunity for law enforcement to leverage this accessibility when conducting an investigation. As previously mentioned with the deployment of body cameras, extracting relevant and actionable information has added substantial complexity and cost to the rollout of this new technology. Municipalities are already experiencing benefits as a result of working with private entities to leverage their collected data. The Alphabet-owned mapping and traffic app Waze is quickly becoming an invaluable tool in transportation planning, with over 72 United

[91] Chantel McGee, *Self-driving cars will double as security cameras, says Intel CEO Brian Krzanich,* CNBC (June 1, 2017), https://cnbc.com/2017/06/01/intel-ceo-krzanich-self-driving-cars-will-double-as-security-cameras.html.

States municipalities already benefitting from their "Connected Citizens Program" data base.[92] Waze crowdsources user data through its smartphone app about real-time road conditions, such as potholes, slow traffic, and flooding.[93] Crowdsourcing is defined as "the practice of obtaining needed services, ideas, or content by soliciting contributions from a large group of people and especially from the online community."[94] Not only is this information collected without cost to the city, but Waze has even worked to integrate its data with at least one company that develops mapping software commonly used by transportation departments.[95] Thus, not only are public agencies benefitting from cost savings by having to maintain less infrastructure to accomplish the same tasks, but the data is even already organized and ready for use.

Business suppliers are already envisioning the deployment of data aggregation software with camera systems. In June 2015, Ford applied for a patent on a system that crowdsources license plate images from back-up cameras.[96] Ford claims it will initially only be used in commercial fleets.[97] However, with back-up cameras already a common feature in personal vehicles, this program may be subject to expansion with minimal technical difficulty in the future.[98] By adopting improved communications technologies, law enforcement agencies could request information and benefit from advancements already present in private industry.

---

[92] *Connected Citizens Program*, WAZE (Nov. 4, 2016), https://wiki.waze.com/wiki/Connected_Citizens_Program.

[93] *Id*.

[94] "Crowdsourcing," *Merriam-Webster Dictionary*, https://www.merriam-webster.com/dictionary/crowdsourcing (2017).

[95] *See, e.g.*, Charlie Sorrel, *Waze Now Shares Its Data With Cities to Improve Roads and Speed Up Journeys*, FAST COMPANY (Oct. 21, 2016), https:www.fastcoexist.com/3064840/waze-now-shares-its-data-with-cities-to-improve-roads-and-speed-up-journeys.

[96] Andrew Krok, *Ford's recently published patent should freak you out a bit*, ROAD SHOW BY CNET (Dec. 12, 2016), https://www.cnet.com/roadshow/news/fords-recently-published-patent-should-freak-you-out-a-bit/.

[97] *Id.*

[98] *Id.*

b. Legal Limits of Data Aggregation

While receiving the data collected by corporations appears to be an attractive proposition from a cost perspective, there are several legal issues that should be taken into account before starting to make bulk requests for company information. While information may be collected from public thoroughfares, that does not always mean such data is lawful. For example, the interception of Wi-Fi communications collected by a vehicle driving through a neighborhood was found to be unlawful.[99] Additionally, companies' ability to access system-wide data and pinpoint individuals, viewing their location and personally identifying information, has come under scrutiny.[100] Ride-hailing app Uber was fined $20,000 by the New York Attorney General's office after an investigation found excessive internal access to sensitive customer information.[101] Both law enforcement agencies and companies must carefully craft agreements that respect the privacy of customers, while distinguishing types of data in which a company has more extensive rights of use for public benefit.

2. Private Citizens as Data Sources

Communities have been slower to adopt technologies that allow them to share data for mutual benefit. However, there is tremendous potential for a new era of safe neighborhoods with crowdsourced data and well-discussed policies at its core. With its reliance on open standards and integrations, IoT technologies will drive a new level of interoperability, similar to that which is already seen in collaboration between police and the business community.

Despite these new potential sources of data, a key challenge will be the communication and notification infrastructure that enables sharing both within neighborhoods and between neighborhoods and law enforcement. While the WEA system is one promising

[99] *E.g.*, Joffe v. Google, Inc., 729 F.3d 1262, 1279 (9th Cir. 2013).

[100] *See, e.g.*, Kaja Whitehouse, *Uber settles 'God View' allegations*, USA TODAY (Jan. 6, 2016), http://www.usatoday.com/story/tech/2016/01/06/uber-settles-god-view-allegations/78383276/.

[101] *Id.*

candidate, the FCC's slow development of even one-way photo messaging indicates that a federal system remains a distant possibility. Fortunately, the public has already demonstrated a willingness to adopt smartphone apps to engage with those around them. Nextdoor is one such neighborhood network app, which as of 2015, had over 77,000 communities signed up for the service.[102] Unlike Facebook or other traditional social media tools, Nextdoor connects users solely with people in their geographic area.[103] The app has already found a number of uses including wild animal alerts, crime reporting, searching for missing animals, and notification preferences that can send special alerts in case of emergency.[104]

While Nextdoor is not the only application with these features, it serves as a useful starting point to consider the future role IoT could play in making communities safer. Ultimately the success of any neighborhood data sharing program will depend on the views and attributes of that particular community. By starting a discussion now, cities can begin to determine: (1) whether the public is interested in such a program, and (2) a desirable operations model for the development of such a program. Like the Waze Connected Citizens Program, public-private partnerships could be developed to help municipalities start similar programs at little to no cost, once appropriate ordinances are in place. Alternatively, a city desiring tighter control over the sharing of citizen data could work with the National Alert Office to create enhanced capabilities in their region, or invest in necessary communications infrastructure themselves. From a budgetary perspective, citizens will purchase their own IoT hardware for personal use, meaning the costly task of deploying this equipment will already be complete. With proper leadership, communities will have the opportunity to experience substantial gains in public safety at low cost, with only minimal impact on overall privacy.

---

[102] Jennifer Jolly, *Meet the Neighbors? There's an App for That*, NEW YORK TIMES (Oct. 13, 2015), http://well.blogs.nytimes.com/2015/10/13/meet-the-neighbors-theres-an-app-for-that/?r=1.

[103] *Id.*

[104] *Id.*

a. Principle Benefits – Community Engagement and Establishing "Reasonability"

With a voluntary data crowdsourcing strategy, many of the problems that have plagued direct collection of data can be avoided while citizens serve as a check on the invasiveness of law enforcement in their community. As previously discussed with the rollout of body cameras, one of the major costs and logistical challenges has been sorting through footage and determining what is important. Additionally, the lack of previously considered policies creates substantial concerns over the actual processing of the data, how long it is stored, and whether it was correctly obtained. By relying on community members to voluntarily contribute information from narrow temporal or geographic windows, the public will have greater confidence that information being collected by law enforcement has a strong connection to public safety concerns in their area. From a community engagement perspective, the opportunity to contribute IoT data for the good of the public represents a low-cost, low-effort way to improve the safety of the local neighborhood.

Beyond policy and social benefits, there are compelling legal reasons to employ a voluntary data crowdsourcing system. Since relevant IoT devices would be collecting information from public areas, this data source represents a category of information repeatedly recognized by the Supreme Court as explicitly not protected under the Fourth Amendment.[105] Even more useful from the perspective of law enforcement is the fact that such data collection will signify mainstream consumer adoption; the *Kyllo* court hinted this may be enough to overcome a "reasonable expectation of privacy" that does not take into account the advancements of modern technology.[106] For example, driving video has traditionally required individuals to purchase a separate dash camera that must be individually operated. But now, automakers are moving towards direct access of video captured by built-in cameras used for safety and semi-autonomous systems.[107] The capture of

---

[105] *See, e.g.*, United States v. Jones, 565 U.S. 400, 412 (2012).
[106] *See, e.g.*, *Kyllo*, 533 U.S. at 34.
[107] *See, e.g.*, Kirsten Korosec, *Elon Musk Says Tesla Is Working On a*

driving video by increasingly mainstream, integrated vehicle systems provides one example of a societal shift that is likely to alter the reasonable expectation of privacy. Thus, encouraging a crowdsourced data model while limiting law enforcement adoption of more advanced tools will keep the public informed on the state of their privacy rights and minimize the likelihood of intrusive, bulk collection of data directly by law enforcement.

b. Limits of a Citizen Data Crowdsourcing Strategy

As with most types of municipal technology adoption, implementation will be key to maximizing the positive effects of a crowdsourcing strategy. First, frequently contacting citizens about crimes could risk an increase in apathy if cooperation is overly burdensome or taken advantage of by law enforcement in a way that hurts individuals. As the WARN Act and the AMBER Alert program each demonstrate, there is already an effort to minimize notification to only the most serious situations to prevent disinterest or annoyance. Any system that a local government considers should be operated to minimize the likelihood of such a community response.

Second, the slower pace of policymaking relative to the consumer product market means careful consideration should be given not only to current IoT products, but also to those that are yet to be developed. Only the public should have the option to contribute information gathered from a new device if it is not used where someone would have both a subjective and reasonable expectation of privacy. Changes to the scope or operations of the program should come only after a dialogue with the public to ensure continued community support for such efforts.

Finally, while current Supreme Court interpretations of individual privacy rights allow for the creation of this system, large-scale efforts to collect and aggregate private data could be implemented in a way deemed too invasive. Similar to the concern of FBI legal counsel over the aggregation of license plates,[108] the

Dash Cam Feature, FORTUNE (Aug. 30, 2017), http://fortune.com/2017/08/30/elon-musk-dashcam-tesla/.

[108] *See* Zetter, *supra* note 48.

collection of citizen-sourced data, even if lawful, could be mistaken for government intrusion, unless the system is tactfully implemented. Though it does not directly contradict the Court's opinion on tracking in *Jones*,[109] this new investigative tool may be viewed as an alternate means of accomplishing the same invasive end.

CONCLUSION

The growth of the Internet of Things offers new opportunities for the average citizen to contribute data collected by their devices to enhance public safety in their communities. While the Court has not directly ruled on the legality of such a system, the framework articulated by the Court for interpreting modern privacy rights under the Fourth Amendment suggests the law will not interfere with such a system if properly implemented. An early public dialogue and policy drafting process will be crucial no matter how extensively local governments wish to use data from IoT devices for public purposes. In the meantime, the public should encourage both the National Alert System working group and National Alert Office to further develop the WEA system as soon as possible, not only to allow communication of more expansive content to the public, but also to create the capacity to receive information and route it to the appropriate bodies. While it will ultimately be up to each community to determine how they wish to use their personal data, the Internet of Things represents an opportunity to make neighborhood watch more vigilant than ever before.

[109] *Jones*, 565 U.S. at 412.

PRACTICE POINTERS

- Public willingness to contribute information depends on establishing thorough and thoughtful policies surrounding aggregation, use, storage, and deletion of data. Existing body camera policies in many cities will provide a good starting point for determining how citizen IoT data should be handled in the future.
- The sourcing of citizen-collected data will likely be useful in establishing the "objective reasonableness" prong of the *Katz* "reasonable expectation of privacy" test. The Court previously recognized "reasonableness" changes over time with developments in society and technology. If private citizens purchase IoT devices capable of interfacing with law enforcement systems on a large scale, this offers a built-in measure of community expectations and shift in what is "reasonable."