# Citizen Searches and the Duty to Report

WAYNE A. LOGAN*

TABLE OF CONTENTS



## I. INTRODUCTION

Today, law enforcement benefits from an ever-increasing abundance of information sources. Technologies such as automated license plate readers and facial recognition, for instance, allow for the identification and tracking of individuals over long periods of time,[1] information that is often combined with other data to provide a comprehensive understanding of surveilled individuals (indeed, entire communities).[2] Meanwhile, private companies and "data brokers" augment the data flow, usually free of Fourth Amendment constraints.[3]

This paper considers another information source: private citizens.[4] Traditionally, the Fourth Amendment has imposed no limits on information provided to police by

* Steven M. Goldstein Professor, Florida State University College of Law. Thanks to the *Journal* for the invitation to the symposium and the help of staff members in preparing this contribution for publication. Thanks also to David Logan and Zachary Kaufman for their input on prior drafts of the paper.

[1] *See generally* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1142–47 (2021).

[2] *See Fusion Centers*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/state-and-major-urban-area-fusion-centers [https://perma.cc/RF6P-6F5Y] (Oct. 17, 2022); *see also* JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 3 (2014) ("We are living in a Dragnet Nation—a world of indiscriminate tracking where institutions are stockpiling data about individuals at an unprecedented pace."). Regarding the surveillance of communities, an example is found in the recent lawsuit addressing a Fourth Amendment challenge to extensive police surveillance of Baltimore by airplane overflights. Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 334 (4th Cir. 2021).

[3] *See, e.g.*, Lauren Sarkesian & Spandana Singh, *How Data Brokers and Phone Apps Are Helping Police Surveil Citizens Without Warrants*, ISSUES IN SCI. & TECH. (Jan. 6, 2021), https://issues.org/data-brokers-police-surveillance/ [https://perma.cc/P9LB-25VZ] (describing how data brokers collect personal data and noting "government law enforcement agencies are rapidly becoming major buyers").

[4] The term "citizen," used here, is intended to refer to nongovernmental individuals and entities, rather than a legal designation, such as in the immigration law context.

citizens, so long as the information is not gathered at the behest of the government[5] and its agents do not expand on a search undertaken by the private party.[6] In a recent paper, I examined how this carve-out is being complicated by the increasing involvement of "web sleuths" and others who, acting individually or collectively, voluntarily seek out (or otherwise discover) and provide information to police, whether to aid active investigations or solve "cold" cases.[7] Against this backdrop, here I consider a potential correlate development: the imposition of a legal duty to report to police information useful to their criminal investigations.

Given the historic reluctance of U.S. jurisdictions to impose an affirmative duty to render aid to real-time crime victims,[8] most famously exemplified by the sexual assault and murder of Kitty Genovese in 1964,[9] one might think that no corresponding affirmative duty to notify police of criminal activity exists. Such a belief, however, is incorrect; in fact, state and federal laws often impose a legal duty to report criminal activity.[10] Moreover, while police always welcome volunteered information that aids in their criminal investigations,[11] one might think that precedent is lacking for imposition of a legal duty to provide information. Again, however, the assumption would be incorrect. Federal law, for instance, imposes on internet service providers, such as Google, a duty to report evidence of child sexual abuse material they detect on the internet.[12] Whether legislatures should impose such a legal duty on the broader public, and the ramifications of doing so, are important questions assuming corresponding greater importance in a time when opportunities for information collection are becoming increasingly available to us all.

---

[5] Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971); Burdeau v. McDowell, 256 U.S. 465, 475–76 (1921).

[6] United States v. Jacobsen, 466 U.S. 109, 113 (1984); Walter v. United States, 447 U.S. 649, 656–59 (1980).

[7] *See* Wayne A. Logan, Essay, *Crowdsourcing Crime Control*, 99 TEX. L. REV. 137, 143–46 (2020); *see also, e.g.*, Kashmir Hill, *The True Crime-Obsessed Philanthropists Paying to Catch Killers*, N.Y. TIMES, https://www.nytimes.com/2022/03/27/technology/dna-tests-crime-solving.html [https://perma.cc/3T3S-9SFG] (Apr. 4, 2022) (noting the presence of a "growing cohort of amateur DNA detectives, their hobby born of widespread consumer genetic testing paired with an unquenchable desire for true crime content"); Sarah Parvini & Melissa Gomez, *On Social Media, Amateur Digital Sleuths Try to Help Track Violent Capitol Rioters*, L.A. TIMES, (Jan. 17, 2021), https://www.latimes.com/california/story/2021-01-17/amateur-social-media-sleuths-track-violent-capitol-rioters [https://perma.cc/KD63-9XGJ].

[8] Joshua Dressler, *Some Brief Thoughts (Mostly Negative) About "Bad Samaritan" Laws*, 40 SANTA CLARA L. REV. 971, 975–77 (2000).

[9] *See* KEVIN COOK, KITTY GENOVESE: THE MURDER, THE BYSTANDERS, THE CRIME THAT CHANGED AMERICA 3–4 (2014).

[10] *See infra* notes 13–26 and accompanying text.

[11] *See* Coolidge v. New Hampshire, 403 U.S. 443, 488 (1971) ("[I]t is no part of the policy underlying the Fourth and Fourteenth Amendments to discourage citizens from aiding to the utmost of their ability in the apprehension of criminals.").

[12] *See infra* Part II.

## II. DUTY TO REPORT CRIMINAL ACTIVITY

Today, in multiple contexts, jurisdictions impose a duty to report criminal activity.[13] Most commonly, the duty applies to so-called mandatory reporters, such as childcare providers, school counselors, and teachers, to inform authorities of suspected child abuse or neglect.[14] A similar duty is imposed on care providers with respect to suspected elder abuse.[15] In the federal context, laws require that financial institutions report suspicions that customers have committed money laundering offenses or other financial crimes.[16] The Comprehensive Environmental Response, Compensation, and Liability Act ("CERCLA," or the "Superfund" law) requires that government officials be notified if hazardous waste is released without permission, allowing for investigation, cleanup, and possible evacuation of nearby residents.[17] The cruise ship industry must register a report with the FBI "as soon as possible after the occurrence on board the vessel of an incident involving homicide, suspicious death, a missing United States national, kidnapping, assault with serious bodily injury, [sexual crimes,] firing or tampering with the vessel, or theft of money or property in excess of $10,000."[18]

Outside these specialized contexts, many states have "Bad Samaritan" laws imposing a duty to report criminal activity.[19] Colorado law, for instance, provides

---

[13] The duty to report differs from misprision, which entails active concealment by an individual of a crime committed by a principal. *See, e.g.*, 18 U.S.C. § 4. The duty to report also differs from compounding, which entails a crime victim taking money or another thing of value in return for not prosecuting an offense or otherwise hampering prosecution of the offense. *See, e.g.*, FLA. STAT. § 843.14 (2021).

[14] Leonard G. Brown, III & Kevin Gallagher, *Mandatory Reporting of Abuse: A Historical Perspective on the Evolution of States' Current Mandatory Reporting Laws with a Review of the Laws in the Commonwealth of Pennsylvania*, 59 VILL. L. REV. TOLLE LEGE 37, 42 (2013); Alison M. Arcuri, Comment, *Sherrice Iverson Act: Duty to Report Child Abuse and Neglect*, 20 PACE L. REV. 471, 488–89 (2000).

[15] Sana Loue, *Elder Abuse and Neglect in Medicine and Law: The Need for Reform*, 22 J. LEGAL MED. 159, 172–79 (2001).

[16] Sandra Guerra Thompson, *The White-Collar Police Force: "Duty to Report" Statutes in Criminal Law Theory*, 11 WM. & MARY BILL RTS. J. 3, 3–5 (2002); Christopher J. Wilkes, Note, *A Case for Reforming the Anti-Money Laundering Regulatory Regime: How Financial Institutions' Criminal Reporting Duties Have Created an Unfunded Private Police Force*, 95 IND. L.J. 649, 649–50 (2020).

[17] 42 U.S.C. § 9603(a); *Summary of the Comprehensive Environmental Response, Compensation, and Liability Act (Superfund)*, EPA, https://www.epa.gov/laws-regulations/summary-comprehensive-environmental-response-compensation-and-liability-act [https://perma.cc/J882-C59K].

[18] 46 U.S.C. § 3507(g)(3)(A)(i).

[19] *See generally* Eldar Haber, *The Digital Samaritans*, 77 WASH. & LEE L. REV. 1559 (2020). Whereas "Good Samaritan" laws provide some form of civil immunity from tort liability to individuals who render aid to another person, presuming certain conditions are met (e.g., the actor was not reckless in rendering aid), "Bad Samaritan" laws impose a duty to report or rescue, penalizing failure to do so. *Id.* at 1568–71.

that "[i]t is the duty of every corporation or person who has reasonable grounds to believe that a crime has been committed to report promptly the suspected crime to law enforcement authorities."[20] In Ohio, "no person, knowing that a felony has been or is being committed, shall knowingly fail to report such information to law enforcement authorities."[21] States also impose a duty to report specific offenses, such as sexual assault[22] or violent or sexual assault against a child.[23] Hawaii requires that physicians report any injury sustained in a suspicious or violent manner[24] and Indiana requires that owners of car repair shops report that a car was struck by a bullet.[25] Computer repair technicians and commercial entities developing film have a duty to report evidence of child sexual abuse.[26]

In the federal context, the PROTECT Our Children Act, codified at 18 U.S.C. § 2258A, is a notable instance of a duty to report. Enacted by Congress in 2008, the law imposes a legal duty on "electronic communication service" and "remote computing service" providers to report if they have "actual knowledge of any facts or circumstances" of child sexual abuse material ("CSAM").[27] The report is to be filed with the CyberTipline operated by National Center for Missing and Exploited Children ("NCMEC").[28] Although the law does not impose an affirmative duty on service providers to detect evidence of CSAM,[29] it does

---

[20] COLO. REV. STAT. § 18-8-115 (2022).

[21] OHIO REV. CODE § 2921.22 (2022).

[22] *See, e.g.*, ALASKA STAT. §§ 11.56.765–.767 (2021); FLA. STAT. § 794.027 (2021); *see also, e.g.*, MASS. GEN. LAWS ch. 268, § 40 (2022) (stating that any person who witnesses an "aggravated rape, rape, murder, manslaughter or armed robbery" and fails to report it shall be punished with a fine up to $2,500); NEB. REV. STAT. § 28-1226 (2022) (stating that "[a]ny person who has knowledge of the theft or loss of explosive materials," and who does not report it to authorities, commits a misdemeanor).

[23] *See, e.g.*, NEV. REV. STAT. § 202.882 (2021).

[24] HAW. REV. STAT. § 453-14 (2022).

[25] IND. CODE § 9-26-5-1 to -2 (2022).

[26] *See, e.g.*, CAL. PENAL CODE § 11165.7(a)(29), (43)(A) (West 2020). *See generally* Corinne Moini, *Protecting Privacy in the Era of Smart Toys: Does Hello Barbie Have a Duty to Report?*, 25 CATH. U. J.L. & TECH. 281, 294–99 (2017).

[27] 18 U.S.C. § 2258A(a)(1); *see also id.* § 2258E(2), (5).

[28] *Id.* § 2258A(a), (c).

[29] *See id.* § 2258A(f) ("Nothing in this section shall be construed to require a provider to—(1) monitor any user, subscriber, or customer of that provider . . . (3) affirmatively search, screen, or scan for facts or circumstances . . . ."); *see also* United States v. Cameron, 699 F.3d 621, 637–38 (1st Cir. 2012) (holding that although duty to report discovery of CSAM exists, Yahoo! had no duty to search for it and therefore the government did not exercise control over Yahoo!'s actions, for purposes of the private search doctrine); United States v. Richardson, 607 F.3d 357, 367 (4th Cir. 2010) (holding that the statute pursuant to which AOL reported the defendant's activities did not convert AOL into an "agent of the Government" under the Fourth Amendment). *But see* United States v. Ackerman, 831 F.3d 1292, 1295–300 (10th Cir. 2016) (concluding that NCMEC qualifies as a government agent for Fourth Amendment purposes). "Providers may also voluntarily make a report to NCMEC's CyberTipline after learning that a violation of the statutes involving CSAM may be 'planned

criminalize failure to report suspected CSAM when a provider does detect it, requiring that the report be made "as soon as reasonably possible."[30] Many providers, such as America Online, Google, and Facebook, however, wishing to be perceived as good corporate citizens, monitor their platforms for CSAM.[31]

The material is detected by several strategies, including review of content by employees, photo scanning software, and hash tag matching, a process whereby a mathematical algorithm generates an alphanumeric sequence unique to a specific file that can be used to detect copies of the file (referred to as its "digital fingerprint").[32] NCMEC shares reports it receives with law enforcement, providing information regarding the suspected source of the CSAM (e.g., an email or IP address, payment information); when and where the CSAM was uploaded, transmitted, or received; the suspected CSAM itself; and the complete chain of communication containing the CSAM (such as emails).[33]

The reporting regime has seemingly proved quite successful. In 2020 alone, Facebook submitted over twenty million reports.[34] Penalties for knowing and willful failure to report evidence of CSAM are considerable, with fines up to

---

or imminent.'" Rachel Haney, *When "Safe at Home" Is Not Safe: Addressing the Increase of Online Child Sexual Abuse in the COVID-19 Pandemic*, SCITECH LAW., Summer 2021, at 22, 24 (footnotes omitted) (quoting 18 U.S.C. § 2258(f)).

[30] 18 U.S.C. § 2258A(a)(1)(A)(i). It is of course illegal to possess CSAM. However, § 230 of the Communications Decency Act provides civil immunity for its presence on providers' platforms. 47 U.S.C. § 230(c)–(e).

[31] As one court observed, "[n]o sane person, let alone a business that values its image and reputation, wants to be publicly associated with the sexual exploitation of children." United States v. Bebris, No. 19-CR-02, 2020 BL 85987, at *4 (E.D. Wis. Mar. 9, 2020) (decision and order denying motion to suppress).

[32] *See* Tyler O'Connell, Note, *Two Models of the Fourth Amendment and Hashing to Investigate Child Sexual Abuse Material*, 53 U. PAC. L. REV. 293, 301 (2021); *see, e.g.*, *PhotoDNA*, MICROSOFT, https://www.microsoft.com/en-us/photodna [https://perma.cc/2S7R-QQSF] (highlighting Microsoft's technology to scan photos to prevent the proliferation of CSAM); James Vincent, *Google Releases Free AI Tool to Help Companies Identify Child Sexual Abuse Material*, VERGE, (Sept. 3, 2018), https://www.theverge.com/2018/9/3/17814188/google-ai-child-sex-abuse-material-moderation-tool-internet-watch-foundation [https://perma.cc/7HPW-NKWW] (discussing Google's AI tool that helps front line "moderators" at non-profit organizations sift through images to identify potential CSAM).

[33] 18 U.S.C. § 2258A(b)(1)–(5).

[34] Tom Porter, *Facebook Reported More Than 20 Million Child Sexual Abuse Images in 2020, More Than Any Other Company*, BUS. INSIDER (Feb. 26, 2021), https://www.businessinsider.com/facebook-instagram-report-20-million-child-sexual-abuse-images-2021-2 [https://perma.cc/WEZ2-QUV3]. The volume, in itself, is not necessarily indicative of actual child pornography instances, as it likely includes false positives, for instance involving deepfakes and AI images. *See, e.g.*, BRACKET FOUNDATION, ARTIFICIAL INTELLIGENCE: COMBATTING ONLINE SEXUAL ABUSE OF CHILDREN 9–10 (2019), https://cdn.websiteeditor.net/64d2dad620fd41ba9cae7f5146793c62/files/uploaded/AI_Making_Internet_Safer_for_Children.pdf [https://perma.cc/BRX9-RFZ5]. Thanks to Zach Kaufman for noting this.

$150,000 for the first instance and $300,000 for any subsequent instance.[35] Service providers are immune from civil claims or criminal charges arising from a report, provided that they do not engage in intentional or reckless conduct.[36]

Recently, efforts have been undertaken to fortify the law's reporting requirements. In the spring of 2020, a bipartisan group in Congress proposed the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020, the EARN IT Act, which would require that providers do more to affirmatively detect and report evidence of CSAM online.[37] A commission would be tasked with developing a series of best practices that providers should follow to combat CSAM.[38] Those failing to adopt and implement recommended best practices would be unable to invoke immunity in a civil suit, and therefore be subject to potential massive liability.[39] The bill was reintroduced in the Senate and reported out of committee in February 2022.[40]

Imposing a kindred duty to report on the public at-large is not hard to imagine. Post-9/11, we are urged that "if [we] see something, say something" with respect to any potential terrorism threat,[41] and a leading national security law journal recently published an article urging application of something like 18 U.S.C. § 2258A to require that social media entities seek out and report terrorism-related posts.[42] Meanwhile, advocates urge implementing a reporting requirement on individuals who are aware of cyberbullying[43] and child sexual

---

[35] 18 U.S.C. § 2258A(e). Because the law penalizes failure to report, concerns exist that service providers might be discouraged from engaging in content review. *E.g.*, United States v. Ringland, 966 F.3d 731, 736 (8th Cir. 2020) ("[T]he penalties for failing to report child pornography may even discourage searches in favor of willful ignorance."). The enormous scale of reports noted in the text, however, suggests that the concern is unwarranted.

[36] 18 U.S.C. § 2258B(a)–(b).

[37] S. 3398 116th Cong. (2020); *see* Cat Zakrzewski, *A Bill Aiming to Protect Children Online Reignites a Battle Over Privacy and Free Speech*, WASH. POST (Feb. 10, 2022), https://www.washingtonpost.com/technology/2022/02/10/senators-earn-it-privacy-children-safety/ [https://perma.cc/39V3-PKAB].

[38] Zakrzewski, *supra* note 37.

[39] *See id.*; *see also* S. 3398, § 5 (2020) (describing activities that do not give rise to liability).

[40] Zakrzewski, *supra* note 37.

[41] *See If You See Something, Say Something*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/see-something-say-something [https://perma.cc/EZX6-7PJM].

[42] Susan Klein & Crystal Flinn, *Social Media Compliance Programs and the War Against Terrorism*, 8 HARV. NAT'L SEC. J. 53 (2017); *see also* Press Release, Dianne Feinstein, Senator for Cal., U.S. Senate, Bill Would Require Tech Companies to Report Online Terrorist Activity (Dec. 8, 2015), http://www.feinstein.senate.gov/public/index.cfm/2015/12/bill-would-require-tech-companies-to-report-online-terrorist-activity [https://perma.cc/A9s4-GK7V] (touting the capacity of social media companies to help prevent terrorism).

[43] *See generally, e.g.*, Heather Benzmiller, Note, *The Cyber-Samaritans: Exploring Criminal Liability for the "Innocent" Bystanders of Cyberbullying*, 107 NW. U. L. REV. 927 (2013).

assaults committed by Americans who are abroad,[44] or observe violent criminal activity on the internet,[45] sexual assaults on airplanes.[46]

## III. PRIVATE PARTY SOURCES

If a general duty to report information concerning criminal activity were to be imposed, there would be no shortage of information sources providing grist for its fulfillment. Already, multiple online entities afford opportunities for amateur sleuths to gather and share information regarding criminal activity.[47] Efforts such as Project: Cold Case[48] and websites dedicated to the detection of individuals seeking to have sex with children continue to grow in number.[49] Vizsafe markets an app designed to motivate citizens to provide tips and videos by disbursing digital rewards that can be redeemed at participating vendors.[50] Citizen Virtual Patrol, operated by the Newark (New Jersey) Police Department, allows community members to monitor live video feeds from the city's network

---

[44] Basyle J. Tchividjian, *Catching American Sex Offenders Overseas: A Proposal for a Federal International Mandated Reporting Law*, 83 UMKC L. REV. 687, 691 (2015).

[45] *See generally, e.g.*, Haber, *supra* note 19; Zachary D. Kaufman, *Digital Age Samaritans*, 62 B.C. L. REV. 1117 (2021); Sharon Yamen, Nanci K. Carr & Aaron Bartholomew, *Am I My Brother's Keeper? How Technology Necessitates Reform of the Lack of Duty to Rescue or Duty to Report Laws in the United States*, 28 B.U. PUB. INT. L.J. 117, 121 (2019).

[46] Madison L. George, Comment, *Accountability for Sexual Assault Aboard Airplanes: An Analysis of the Need for Reporting Requirements at 35,000 Feet*, 85 J. AIR L. & COM. 669, 669 (2020).

[47] *See, e.g.*, Tamara Gane, *Should Police Turn to Crowdsourced Online Sleuthing?*, OZY (Aug. 14, 2018), https://www.ozy.com/opinion/should-police-turn-to-crowdsourced-online-sleuthing/88691/ [https://perma.cc/YVS7-GZKV] (proclaiming that web platforms allow "ordinary people from all walks of life" to come together to "dissect clues to crimes and unravel real-life mysteries").

[48] *See Project: Cold Case FAQs*, PROJECT: COLD CASE, https://www.projectcoldcase.org/faqs/ [https://perma.cc/6W3R-4USG] ("[W]e are not an investigative firm and we do not collect tips on these cases, but instead ask those with information to provide it directly to law enforcement or anonymous tip lines like Crime Stoppers.").

[49] *See, e.g.*, Debra Cassens Weiss, *Vigilante Child Predator Stings Are Dangerous and Illegal, Wisconsin Attorney General Says*, A.B.A. J. (Sept. 4, 2019), https://www.abajournal.com/news/article/vigilante-child-predator-stings-are-dangerous-and-illegal-wisconsin-attorney-general-says [https://perma.cc/7CH2-LHQ7]. Similarly, "digital vigilantes" focus on computer hackers. Nicholas Schmidle, *The Digital Vigilantes Who Hack Back*, NEW YORKER (Apr. 30, 2018), https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back [https://perma.cc/KA4Y-ADPH].

[50] *See* Jon Glasco, *How Crowdsourcing and Incentives Improve Public Safety*, BEE SMART CITY (Mar. 10, 2019), https://hub.beesmart.city/en/solutions/smart-living/public-safety/how-crowdsourcing-and-incentives-improve-public-safety [https://perma.cc/6YXE-AYMZ] (discussing the business model of Vizsafe and its use of incentives to encourage citizen participation).

of multiple surveillance cameras and report on suspicious activity.[51] Together, the volunteered investigative inputs effectively serve as a "force multiplier" for police in their investigations.[52]

Moreover, to a greater extent than ever before, security conscious Americans obtain and use devices that collect information regarding their homes and neighborhoods. A foremost example is the Ring Video Doorbell, sold by Amazon, which has a high-definition camera and a microphone that allows live streaming (for less than $100), with a coverage of thirty feet, a device with over ten million users.[53] Owners of the device can direct it to take photos at certain set intervals, from every thirty seconds to one hour, even without detected motion.[54] And Ring is just one of several information-collection devices. According to one source, "there are hundreds of millions of privately-owned surveillance devices in use across the country," some of which have facial recognition capability.[55] Recently, the *New York Times* noted the availability and use of miniature tracking devices, some the size of a quarter, which provide information on the physical locations of others for extended periods of time.[56] In many neighborhoods, Flock auto license plate readers (which can be purchased for $2,500) are used, allowing among other things, real-time monitoring of cars.[57] Neighborhood groups also regularly employ private security forces to patrol and monitor areas, providing yet another information collection vector.[58]

---

[51] Rick Rojas, *In Newark, Police Cameras, and the Internet, Monitor You*, N.Y. TIMES (June 9, 2018), https://www.nytimes.com/2018/06/09/nyregion/newark-surveillance-cameras-police.html [https://perma.cc/24F2-5QZU].

[52] Logan, *supra* note 7, at 163.

[53] Julian Clark, Barry Friedman, Farhang Heydari & Max Isaacs, *Ring Neighbors & Neighbors Public Safety Service: A Civil Rights & Civil Liberties Audit* 12 (NYU Sch. of L. Policing Project, Working Paper No. 22-32, 2022); *Video Doorbells*, RING, https://ring.com/doorbell-cameras [https://perma.cc/6RZ4-T8SM] (highlighting the cost and use of the Ring Doorbell). It is estimated that sales in the home security camera market will approach $10 billion by 2023. TJ McCue, *Home Security Cameras Market to Surpass $9.7 Billion by 2023*, FORBES (Jan. 31, 2019), https://www.forbes.com/sites/tjmccue/2019/01/31/home-security-cameras-market-to-surpass-9-7-billion-by-2023/?sh=27f6a63623c2 [https://perma.cc/ZN9C-2W86].

[54] Clark, Friedman, Heydari & Isaacs, *supra* note 53, at 12.

[55] *Id.* at 10, 13.

[56] *See, e.g.*, Kashmir Hill, *I Used Apple AirTags, Tiles and a GPS Tracker to Watch My Husband's Every Move*, N.Y. TIMES (Feb. 11, 2022), https://www.nytimes.com/2022/02/11/technology/airtags-gps-surveillance.html [https://perma.cc/D73G-SYVN].

[57] Drew Harwell, *License Plate Scanners Were Supposed to Bring Peace of Mind. Instead They Tore the Neighborhood Apart*, WASH. POST (Oct. 22, 2021), https://www.washingtonpost.com/technology/2021/10/22/crime-suburbs-license-plate-readers/ [https://perma.cc/9Z7Z-NZKR]. Flock's customer base has increased roughly four-fold since 2019. *Id.*; *Price & Payment*, FLOCK SAFETY, https://www.flocksafety.com/faq/price-and-payment [https://perma.cc/7H5H-K75E].

[58] Elizabeth E. Joh, *Conceptualizing the Private Police*, 2005 UTAH L. REV. 573, 611.

Private businesses also secure information useful to criminal investigations. They can do so by means of their extensive use of video surveillance of their premises[59] and the monitoring of their employees, for instance by examining their internet browser histories.[60]

Finally, information collection is now being monetized by the private sector,[61] adding a new and potentially very significant information source. As Professor Elizabeth Joh recently noted, there is emerging a "gig surveillance economy" in which individuals gain financial benefit by collecting and reporting surveillance data.[62] One example she notes involved payment of $8–$10 an hour to freelance "spotters" who use their personal computers to see if there is a suspicious person or vehicle at a sensitive location, such as a power station, potentially vulnerable to sabotage.[63]

Professor Joh predicts that government entry into the gig worker surveillance marketplace will generate additional forms of citizen surveillance.[64] This is because, she reasons, "gig surveillance work requires few changes to the existing political economy of temporary, on-demand, freelance labor."[65] "Uber and Doordash drivers are pervasive; why not equip them with license plate readers? Instacart and Postmates shoppers are everywhere; why not give them body cameras?"[66] Moreover, she notes, "[n]one of these gig jobs require special investigatory skills; all can be outsourced cheaply."[67]

The foregoing examples by no means exhaust the myriad ways in which information is being collected by individuals and entities; there are many others that materialize every day. The point here is that pervasive information

---

[59] *See, e.g.*, *Security Cameras for Business*, BRICKHOUSE SEC., https://www.brickhousesecurity.com/hidden-cameras/business/ [https://perma.cc/B623-YFQ6].

[60] Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CALIF. L. REV. 735, 743 (2017). Surveillance by employers extends to gig economy workers as well. Mack DeGeurin, *In 2021, Gig Workers Were Forced to Endure 'Unprecedented Surveillance,'* GIZMODO (Dec. 14, 2021), https://gizmodo.com/in-2021-gig-workers-were-forced-to-endure-unprecedent-1848212656 [https://perma.cc/F28F-THAX].

[61] *See generally* JUSTIN SHERMAN, DATA BROKERS AND SENSITIVE DATA ON U.S. INDIVIDUALS (2021).

[62] ELIZABETH E. JOH, A GIG SURVEILLANCE ECONOMY 1–2 (Hoover Inst. Working Group on Nat'l Sec. Tech. & L., Aegis Paper Ser. No. 2108, 2021).

[63] *Id.* at 1.

[64] *Id.* at 8.

[65] *Id.* at 2.

[66] *Id.*

[67] *Id.* at 7; *see also, e.g.*, Michael Wilson, *$87.50 for 3 Minutes: Inside the Hot Market for Videos of Idling Trucks*, N.Y. TIMES (Mar. 19, 2022), https://www.nytimes.com/2022/03/19/nyregion/clean-air-idle-car.html [https://perma.cc/FDA7-GA25] (discussing New York City's Citizens Air Complaint Program whereby "citizen reporters" are paid for videos they take of trucks idling for more than three minutes (or one minute if outside a school), with the city paying $1.1 million for videos since 2019).

gathering is now normalized, raising the stakes of imposing a duty to report criminal investigative information, which are discussed next.

## IV. CONCERNS

Imposing a duty to report information pertinent to criminal activity, much as exists with reporting CSAM pursuant to 18 U.S.C. § 2258A, is not difficult to imagine. CSAM is of course horrific, but so too, a legislator might argue, is the harm caused by other criminal behaviors such as the sale of illegal drugs and violent gang activity. Moreover, much as internet service providers report information regarding CSAM in part because they wish to be seen as good corporate citizens,[68] the public will not likely need much encouragement. "Public safety is not free," and "we must each do our part to keep the community safe," the persuasive slogans might go.[69] And, because the command is generalized to the public at large, the provision of investigative information to government agents will not likely trigger Fourth Amendment constraints.[70]

Imposing a legal duty to provide information would also fit comfortably within historical traditions. As "wanted" posters of the late 1800s American West attest,[71] law enforcement has long encouraged public assistance in criminal investigations. Today, tip hotlines such as "Crime Stoppers" are common, and for over two decades *America's Most Wanted* provided television viewers information on unsolved crimes and urged their assistance.[72] Police departments also encourage participation in and rely upon "Neighborhood Watch" and other similar programs in the name of police and citizens being co-producers of public safety.[73] Together, the strategies are part of the nation's

---

[68] *See supra* note 31 and accompanying text.

[69] *Cf.* Georgia v. Randolph, 547 U.S. 103, 115–16 (2006) (stating that when private parties provide incriminating evidence to police it serves society's interest in "bringing criminal activity to light").

[70] *See supra* notes 5–6 and accompanying text.

[71] *See generally* RACHEL HALL, WANTED: THE OUTLAW IN AMERICAN VISUAL CULTURE (2009) (surveying history of the American "wanted" poster and its uses and patterns of circulation). The practice of informing on one's fellow citizens dates back to at least Roman times, with rewards ranging from pecuniary benefits and public praise to freedom for slaves and citizenship for foreigners. *Delator*, BRITANNICA, https://www.britannica.com/topic/delator [https://perma.cc/ZM6R-5H5K].

[72] Claire Martin, *The End of* America's Most Wanted*: Good News for Criminals, Bad News for the FBI*, TIME (July 29, 2011), http://content.time.com/time/arts/article/0,8599,2085343,00.html [https://perma.cc/DZ55-9VFM]. The show claims that it led to the arrest of 1,154 criminal suspects. *Id.*

[73] *See* NAT'L SHERIFFS' ASS'N & U.S. DEP'T OF JUST., NEIGHBORHOOD WATCH MANUAL 2 (2005) https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/NSA_NW_Manual.pdf [https://perma.cc/CU2F-KXPA] (explaining that the National Sheriffs' Association created the National Neighborhood Watch Program to prevent crime in residential areas).

ongoing pluralization of crime control efforts,[74] entailing a "shift from police to policing."[75]

Imposing a duty to report would have obvious upsides. The information provided could well aid investigations, helping to hold criminal offenders to account, and widespread knowledge of the duty might increase deterrence of would-be criminal actors. Imposing a legal duty could also provide "cover" for individuals fearful of "snitching" ("snitches get stitches," as the saying goes).[76]

The downsides, however, would be significant. For one, imposing a duty would pose practical difficulties. Say, for instance, that a law requires that "material" investigative information be provided to law enforcement when an individual or entity has "actual knowledge" of it. Both requirements present obvious line-drawing and factual proof challenges. Such challenges, of course, undermine existing laws penalizing a failure to report criminal activity, but the sheer scale of an investigative information duty to report would pose markedly greater concern.

At the same time, exemptions would need to exist, much as with "Bad Samaritan" laws.[77] For instance, an exemption from the duty would be warranted if reporting information would place an individual in danger of serious bodily injury or death; when the would-be reporter is a victim of the crime in question; or reporting would present risk of self-incrimination in violation of the Fifth Amendment.[78] And, as with 18 U.S.C. § 2258B, regarding service providers who provide reports of CSAM,[79] citizen information providers presumably would be immunized from civil liability.

More fundamentally, imposing an affirmative duty to report threatens major social harms. In addition to undercutting personal autonomy, the imposition of a legal duty to report could significantly diminish social trust and interpersonal relations.[80] The duty would perpetuate the sense that we are a nation of "citizen

---

[74] *See* Drew Harwell, *Ring and Nest Helped Normalize American Surveillance and Turned Us into a Nation of Voyeurs*, WASH. POST (Feb. 18, 2020), https://www.washingtonpost.com/technology/2020/02/18/ring-nest-surveillance-doorbell-camera/ [https://perma.cc/V3UX-KW4Y] (noting that Ring and Nest devices have allowed Americans to become their own "personal security force" and greatly escalated the criminal surveillance powers of law enforcement).

[75] Ian Loader, *Plural Policing and Democratic Governance*, 9 SOC. & LEGAL STUD. 323, 323 (2000); *see also* WESLEY G. SKOGAN & SUSAN M. HARTNETT, COMMUNITY POLICING, CHICAGO STYLE 8–9 (1997) (discussing role of community members as "coproducers" of public safety).

[76] *See* Breanna Trombley, *Criminal Law—No Stitches for Snitches: The Need for a Duty-To-Report Law in Arkansas*, 34 U. ARK. LITTLE ROCK L. REV. 813, 821–22 (2012).

[77] *See* Dressler, *supra* note 36, at 982–83.

[78] *See* Kaufman, *supra* note 45, at 1182–84.

[79] *See supra* note 37 and accompanying text.

[80] *Cf.* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (recognizing that an "[a]wareness that the government may be watching chills associational and expressive freedoms").

spies,"[81] as in the former East Germany[82] or modern China.[83] Ultimately, if allowed to come to full fruition, the duty to report would help promote what philosopher Michel Foucault called "responsibilization,"[84] a way of "managing the public by having it manage itself."[85] Worse yet, awareness of being reported

---

[81] *See* JOSHUA REEVE, CITIZEN SPIES: THE LONG RISE OF AMERICA'S SURVEILLANCE SOCIETY 2–3 (2017); *see also* JIM REDDEN, SNITCH CULTURE 1–2 (2000); Liam Day, *Teacher Spying Is Instilling Surveillance Culture into Students*, REASON (Feb. 15, 2022), https://reason.com/2022/02/15/teacher-spying-is-instilling-surveillance-culture-into-students/ [https://perma.cc/Z2S3-Z2RL]. *Cf.* Paulina Villegas, *These Police Departments Want You to Celebrate Valentine's Day by Turning in Your Ex*, WASH. POST (Feb. 10, 2022), https://www.washingtonpost.com/nation/2022/02/10/police-department-encourages-people-to-snitch-on-exes/ [https://perma.cc/VLC4-95UU].

[82] *See, e.g.*, Peter Wensierski, *East German Snitching Went Far Beyond Stasi*, SPIEGEL INT'L (July 10, 2015), https://www.spiegel.de/international/germany/east-german-domestic-surveillance-went-far-beyond-the-stasi-a-1042883.html [https://perma.cc/5FTX-3JKL] (describing a "finely woven web of surveillance" in which East German citizens voluntarily informed on fellow citizens). *See generally* Andreas Lichter, Sebastian Siegloch & Max Löffler, *The Long-Term Costs of Government Surveillance: Insights from Stasi Spying in East Germany*, 19 J. EUR. ECON. ASS'N 741 (2021); Marcus Jacob & Marcel Tyrell, *The Legacy of Surveillance: An Explanation for Social Capital Erosion and the Persistent Economic Disparity Between East and West Germany* (July 26, 2010) (unpublished manuscript), https://ssrn.com/abstract=1554604 or http://dx.doi.org/10.2139/ssrn.1554604 (on file with the *Ohio State Law Journal*).

[83] *See generally, e.g.*, Jue Jiang, *The Eyes and Ears of the Authoritarian Regime: Mass Reporting in China*, 51 J. CONTEMP. ASIA 828 (Sept. 11, 2020), https://doi.org/10.1080/00472336.2020.1813790 [https://perma.cc/HV55-8YXE]. In China, Chairman Mao advocated that the "masses have sharp eyes." Simon Denyer, *China's Watchful Eye*, WASH. POST (Jan. 7, 2018), https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/ [https://perma.cc/TWF6-MJFA]. Reports have surfaced of widespread public use of a "human flesh search engine," dedicated to outing and punishing unethical yet lawful behaviors. Li Gao, *The Emergence of the Human Flesh Search Engine and Political Protest in China: Exploring the Internet and Online Collective Action*, 38 MEDIA CULTURE & SOC'Y 349, 353 (2016), https://doi.org/10.1177/0163443715610493 (on file with the *Ohio State Law Journal*); Celia Hatton, *China's Internet Vigilantes and the 'Human Flesh Search Engine,'* BBC NEWS (Jan. 28, 2014), https://www.bbc.com/news/magazine-25913472 [https://perma.cc/KGA3-8GBN] (reporting on incidents of "flesh-searching" in China); Jessica Levine, *What Is a 'Human Flesh Search,' and How Is It Changing China?*, ATLANTIC (Oct. 5, 2012), https://www.theatlantic.com/international/archive/2012/10/what-is-a-human-flesh-search-and-how-is-it-changing-china/263258/ [https://perma.cc/R9G3-FL4W] (describing how grassroots "flesh-searching" is used in China in the absence of the rule of law).

[84] *See* Michel Foucault, *Afterword* of HUBERT L. DREYFUS & PAUL RABINOW, MICHEL FOUCAULT: BEYOND STRUCTURALISM AND HERMENEUTICS 208–26 (2d ed. 1982); *see also* David Garland, *The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society*, 36 BRIT. J. CRIMINOLOGY 445, 452 (1996) (discussing efforts by contemporary governments to encourage "responsibilization" to effectuate social control).

[85] TOBY MILLER, THE WELL-TEMPERED SELF: CITIZENSHIP, CULTURE, AND THE POSTMODERN SUBJECT, at xiii (1993).

upon by one's fellow community members would aggravate surveillance-generated psychic burdens already pervading modern life, including "surveillance capitalism,"[86] and monitoring by private data brokers[87] and the government itself.[88]

Finally, imposition of a duty to report would be problematic because its effects would not likely fall equally on all members of society. We know that privacy protection divides along racial, gender, and socioeconomic lines,[89] as well physical and mental ability.[90] It can be expected that individuals with less wherewithal to shield their privacy would be the subject of greater scrutiny, and therefore greater criminal suspicion (itself not always justified).

## V. CONCLUSION

To a greater extent than ever before, our everyday lives are subject to surveillance and monitoring by others. Given this reality, imposing a duty to provide law enforcement with information regarding the suspected criminal wrongdoing of others has assumed new importance.[91] To date, government efforts to impose a duty to report investigative information has been limited.[92] However, powerful social and political forces could well inspire laws imposing on citizens a duty to share such information, which as discussed here, should not be seen as an altogether welcome development.

---

[86] *See generally* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

[87] *See* Kiel Brennan-Marquez, *The Constitutional Limits of Private Surveillance*, 66 U. KAN. L. REV. 485, 486–87 (2018).

[88] *See, e.g.*, Brian Bennett & Joel Rubin, *Drones Are Taking to the Skies in the U.S.*, L.A. TIMES, (Feb. 15, 2013), https://www.latimes.com/world/la-xpm-2013-feb-15-la-na-domestic-drones-20130216-story.html [https://perma.cc/PN7A-4B5F].

[89] *See* Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 425, 441–50 (2017).

[90] *See* Matthew Tokson, *Inescapable Surveillance*, 106 CORNELL L. REV. 409, 431–33 (2021).

[91] *See supra* Part II. Of late, state lawmakers have acted to allow citizens to sue their fellow citizens who violate state laws, for instance those aiding or abetting an abortion, a shift toward what has been termed "legal vigilantism." *See, e.g.*, Kimberly Kindy & Alice Crites, *The Texas Abortion Ban Created a 'Vigilante' Loophole. Both Parties Are Rushing to Take Advantage*, WASH. POST (Feb. 22, 2022), https://www.washingtonpost.com/politics/2022/02/22/texas-abortion-law-vigilante-loophole-supreme-court/ [https://perma.cc/N9DF-UKBN]. *Cf.* Jon Michaels & David Noll, *We Are Becoming a Nation of Vigilantes*, N.Y. TIMES (Sept. 4, 2021), https://www.nytimes.com/2021/09/04/opinion/texas-abortion-law.html [https://perma.cc/MG6F-YB3V].

[92] *See supra* notes 27–36 and accompanying text.