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, information that is often combined with other data to provide a comprehensive understanding of surveilled individuals (indeed, entire communities). Meanwhile, private companies and “data brokers” augment the data flow, usually free of Fourth Amendment constraints. This paper considers another information source: private citizens. Traditionally, the Fourth Amendment has imposed no limits on information provided to police by 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 and its agents do not expand on a search undertaken by the private party. 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. 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, most famously exemplified by the sexual assault and murder of Kitty Genovese in 1964, 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. Moreover, while police always welcome volunteered information that aids in their criminal investigations, 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. 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.

---

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. 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. A similar duty is imposed on care providers with respect to suspected elder abuse. In the federal context, laws require that financial institutions report suspicions that customers have committed money laundering offenses or other financial crimes. 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. 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.”

Outside these specialized contexts, many states have “Bad Samaritan” laws imposing a duty to report criminal activity. 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).


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, “[n]o 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 assault22 or violent or sexual assault against a child.23 Hawaii requires that physicians report any injury sustained in a suspicious or violent manner24 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).
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.”

Many providers, such as America Online, Google, and Facebook, however, wishing to be perceived as good corporate citizens, monitor their platforms for CSAM.

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”). 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).

The reporting regime has seemingly proved quite successful. In 2020 alone, Facebook submitted over twenty million reports. Penalties for knowing and willful failure to report evidence of CSAM are considerable, with fines up to
$150,000 for the first instance and $300,000 for any subsequent instance.\textsuperscript{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.\textsuperscript{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.\textsuperscript{37} A commission would be tasked with developing a series of best practices that providers should follow to combat CSAM.\textsuperscript{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.\textsuperscript{39} The bill was reintroduced in the Senate and reported out of committee in February 2022.\textsuperscript{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,\textsuperscript{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.\textsuperscript{42} Meanwhile, advocates urge implementing a reporting requirement on individuals who are aware of cyberbullying\textsuperscript{43} and child sexual

\textsuperscript{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. \textit{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.

\textsuperscript{36} 18 U.S.C. § 2258B(a)–(b).


\textsuperscript{38} Zakrzewski, supra note 37.

\textsuperscript{39} See id.; see also S. 3398, § 5 (2020) (describing activities that do not give rise to liability).

\textsuperscript{40} Zakrzewski, supra note 37.


assaults committed by Americans who are abroad, or observe violent criminal activity on the internet, sexual assaults on airplanes.

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. Efforts such as Project: Cold Case and websites dedicated to the detection of individuals seeking to have sex with children continue to grow in number. Vizsafe markets an app designed to motivate citizens to provide tips and videos by disbursing digital rewards that can be redeemed at participating vendors. Citizen Virtual Patrol, operated by the Newark (New Jersey) Police Department, allows community members to monitor live video feeds from the city’s network.

---

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.”).
of multiple surveillance cameras and report on suspicious activity. Together, the volunteered investigative inputs effectively serve as a “force multiplier” for police in their investigations. 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. 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. 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. 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. 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. Neighborhood groups also regularly employ private security forces to patrol and monitor areas, providing yet another information collection vector.

52 Logan, supra note 7, at 163.
54 Clark, Friedman, Heydari & Isaacs, supra note 53, at 12.
55 Id. at 10, 13.
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 and the monitoring of their employees, for instance by examining their internet browser histories.

Finally, information collection is now being monetized by the private sector, 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. 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.

Professor Joh predicts that government entry into the gig worker surveillance marketplace will generate additional forms of citizen surveillance. This is because, she reasons, “gig surveillance work requires few changes to the existing political economy of temporary, on-demand, freelance labor.” “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?” Moreover, she notes, “[n]one of these gig jobs require special investigatory skills; all can be outsourced cheaply.”

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

---


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, 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. 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.

Imposing a legal duty to provide information would also fit comfortably within historical traditions. As “wanted” posters of the late 1800s American West attest, 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. 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. Together, the strategies are part of the nation’s

68 See supra note 31 and accompanying text.
70 See supra notes 5–6 and accompanying text.
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.
ongoing pluralization of crime control efforts,\textsuperscript{74} entailing a “shift from police to policing.”\textsuperscript{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).\textsuperscript{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.\textsuperscript{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.\textsuperscript{78} And, as with 18 U.S.C. § 2258B, regarding service providers who provide reports of CSAM,\textsuperscript{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.\textsuperscript{80} The duty would perpetuate the sense that we are a nation of “citizen

\textsuperscript{74} See Drew Harwell, \textit{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/20200218/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).


\textsuperscript{77} See Dressler, supra note 36, at 982–83.

\textsuperscript{78} See Kaufman, supra note 45, at 1182–84.

\textsuperscript{79} See supra note 37 and accompanying text.

\textsuperscript{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 Germany82 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


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).

upon by one’s fellow community members would aggravate surveillance-generated psychic burdens already pervading modern life, including “surveillance capitalism,” and monitoring by private data brokers and the government itself.

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, as well physical and mental ability. 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. To date, government efforts to impose a duty to report investigative information has been limited. 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.

---

92 See supra notes 27–36 and accompanying text.