Crowdsourcing Crime Control

Wayne A. Logan*

Crowdsourcing, which leverages the collective expertise and resources of (mainly online) communities to achieve specified objectives, today figures prominently in a broad array of realms, including business, human rights, and medical and scientific research. It also now plays a significant role in governmental crime control efforts. Web and forensic–genetic sleuths, armchair detectives, and the like are collecting and analyzing evidence and identifying criminal suspects, at the behest of and with varying degrees of assistance from police officials.

Unfortunately, as with so many other aspects of modern society, current criminal procedure doctrine is ill-equipped to address this development. In particular, for decades it has been accepted that the Fourth Amendment only limits searches and seizures undertaken by public law enforcement, not private actors. Crowdsourcing, however, presents considerable taxonomic difficulty for existing doctrine, making the already often permeable line between public and private behavior considerably more so. Moreover, although crowdsourcing promises considerable benefit as an investigative force multiplier for police, it poses risks, including misidentification of suspects, violation of privacy, a diminution of governmental transparency and democratic accountability, and the fostering of a mutual social suspicion that is inimical to civil society.

Despite its importance, government use of crowdsourcing to achieve crime control goals has not yet been examined by legal scholars. Like the internet on which it predominantly relies, crowdsourcing is not going away; if anything, it will proliferate in coming years. The challenge lies in harnessing its potential, while protecting against the significant harms that will accrue should it go unregulated. This Essay describes the phenomenon and provides a framework for its regulation, in the hope of ensuring that the wisdom of the crowd does not become the tyranny of the crowd.

---

* Steven M. Goldstein Professor of Law, Florida State University College of Law. Thanks to Susan Bandes, Andrew Ferguson, Richard Re, Stephen Schulhofer, Ric Simmons, Chris Slobogin, and Ron Wright for their very helpful comments.

"[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."[1]

"I might be an expert at Facebook. You might be an expert at Twitter. The cops are experts on their databases and the tools they have. But collectively, we are working together as one."[2]

Introduction

Historically, the job of investigating crimes and apprehending criminal suspects fell to community members: Upon hearing a "hue and cry," all were legally required to render assistance.[3] Not until the mid-to-late 1800s, when public police forces assumed more recognizable modern form, did law enforcement become a primarily governmental undertaking.[4]

Soon thereafter, the U.S. Supreme Court began invoking the Fourth Amendment to regulate police behaviors, holding in 1914 that unlawful searches and seizures by police (federal agents in particular) would be subject to the exclusionary rule.[5] Seven years later, the Court held that searches and seizures by private individuals, even if unlawful, were not subject to Fourth Amendment regulation.[6] This was because the Amendment was "intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon [anyone] other than governmental agencies."[7] In later cases, decided in the 1970s and 1980s, the Court elaborated that the Fourth Amendment only regulates private actors who serve as an "instrument" or "agent" of law enforcement in conducting searches.[8]

---

1. Coolidge v. New Hampshire, 403 U.S. 443, 488 (1971).

2. *Bay Area Police Rely on Crowdsourcing to Help Fight Crime*, KPIX 5 CBS SF BAYAREA (Oct. 23, 2013, 10:31 AM), https://sanfrancisco.cbslocal.com/2013/10/23/bay-area-police-rely-on-crowdsourcing-to-help-fight-crime/ [https://perma.cc/MK4P-ZNYX] (quoting Bay Area resident Joe Carpenter, who assisted in the recovery of a stolen bike and the apprehension of the alleged perpetrator).

3. George C. Thomas III, *Time Travel, Hovercrafts, and the Framers: James Madison Sees the Future and Rewrites the Fourth Amendment*, 80 NOTRE DAME L. REV. 1451, 1468–72 (2005).

4. *See* Seth W. Stoughton, *The Blurred Blue Line: Reform in an Era of Public and Private Policing*, 44 AM. J. CRIM. L. 117, 120–27 (2017) (describing the historical emergence of modern policing).

5. Weeks v. United States, 232 U.S. 383, 398 (1914).

6. Burdeau v. McDowell, 256 U.S. 465, 475 (1921).

7. *Id.*

8. *See* Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971) ("The test . . . is whether [the private actor], in light of all the circumstances of the case, must be regarded as having acted as an 'instrument' or agent of the state . . . ."); *see also* Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 615 (1989) (noting that if the "specific features of [a regulatory regime] combine" in a way that strongly encourages or facilitates private searching, then private searches may implicate the Fourth Amendment); United States v. Jacobsen, 466 U.S. 109, 113 (1984) (discussing the "agent of the Government" exception to the private search rule).

Much has changed, of course, since the Court issued its seminal "private search" decisions. Certainly, a foremost development has been the advent of the internet, which allows for the collection, aggregation, and analysis of enormous troves of data, which police now regularly use in their investigations.[9] Much of the data comes from private businesses, such as cell phone companies, which provide geolocation information on users,[10] and data brokers like ChoicePoint, which contribute vast volumes of personal information regarding individuals.[11] As commentators have noted, the efforts amount to an outsourcing by police of searches to private entities,[12] creating an environment where "private actors turn themselves into the 'eyes and ears' of law enforcement."[13] The "handshake" agreements between private data providers and police provide compelling reason to conclude that the Supreme Court's formalistic public–private search dichotomy is troublingly underinclusive.[14]

This Essay addresses another form of law enforcement outsourcing to civilians, which legal commentators have yet to explore: that concerning the

9. *See* Wayne A. Logan & Andrew Guthrie Ferguson, *Policing Criminal Justice Data*, 101 MINN. L. REV. 541, 548–49 (2016) (detailing the central role of data collection in crime control by law enforcement and the increasing data dependency of the criminal justice system); *see also* Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 658 (2015) (noting that digital "[d]ata is quickly becoming the main currency of law enforcement").

10. *See* Carpenter v. United States, 138 S. Ct. 2206, 2211–12, 2218 (2018) (explaining how wireless carriers acquire cell-site location information from users and noting that "the Government can access each carrier's deep repository of historical location information at practically no expense").

11. *See* Kiel Brennan-Marquez, *The Constitutional Limits of Private Surveillance*, 66 U. KAN. L. REV. 485, 486–87, 487 n.9 (2018) (counting data brokers like ChoicePoint among the commercial entities that sell "publicly available" information to law enforcement agencies); Amitai Etzioni, *Reining in Private Agents*, 101 MINN. L. REV. HEADNOTES 279, 284–85 (2016) (noting that commercial data brokers routinely sell personal information to the FBI and other law enforcement agencies); *see also* Mark Rasch, *Personal Data Collection: Outsourcing Surveillance*, SECURITY BOULEVARD (Feb. 25, 2020), https://securityboulevard.com/2020/02/personal-data-collection-outsourcing-surveillance/ [https://perma.cc/X77P-G2P5] (discussing the sale of individuals' information by private companies to law enforcement agencies).

12. Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1338 (2012); *see also* Kimberly N. Brown, *Outsourcing, Data Insourcing, and the Irrelevant Constitution*, 49 GA. L. REV. 607, 609–15 (2015) (exploring the ways in which outsourcing of government functions, paired with "data insourcing" by state agencies, permits the circumvention of various regulatory mechanisms, including constitutional rules).

13. Brennan-Marquez, *supra* note 11, at 503 (emphasis omitted); *see also* Brennan-Marquez, *supra* note 9, at 658–59 ("Fourth Amendment law must begin to think differently about collaboration between law enforcement and the private sector."); *cf.* Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEXAS L. REV. 467, 469–72 (2017) (discussing the close working relationships between private companies and the federal government in maintaining cybersecurity).

14. *See, e.g.*, Etzioni, *supra* note 11 (detailing the large amount of information collected by private companies that is shared with government actors); Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 104–05 (2018) (noting scholars' concerns about public–private partnerships between the government and corporate surveillants).

actual apprehension of criminal suspects.[15] As "wanted" posters of the American West in the late 1800s attest,[16] police have long encouraged public assistance in this regard. 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.[17] Police departments also encourage participation in and rely upon "Neighborhood Watch" and other similar programs in the name of public safety.[18]

The foregoing illustrations, however, ignore a critically important new form of public participation in crime control: crowdsourcing. The term, if not the concept,[19] was coined by *Wired* author Jeff Howe in 2006.[20] Although variously defined, one definition, as good as any, describes crowdsourcing as an "online, distributed problem-solving and production model that leverages the collective intelligence of online communities to serve specific organizational goals."[21] Today, crowdsourcing is evident in a great many

15. *See* Johnny Nhan, Laura Huey & Ryan Broll, *Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings*, 57 BRIT. J. CRIMINOLOGY 341, 344 (2017) (noting that the phenomenon "has yet to generate significant interest on the part of researchers"); *see also* David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1074 (2014) ("[P]reoccupation with data flows has led to the neglect of some important dimensions of privacy.").

16. *See generally* RACHEL HALL, WANTED: THE OUTLAW IN AMERICAN VISUAL CULTURE (2009) (surveying the history of the American "wanted" poster and its uses and patterns of circulation).

17. 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/WSF6-U2VP]. The show claims that it led to the arrest of 1,154 criminal suspects. *Id.*

18. *See* BUREAU OF JUST. ASSISTANCE, U.S. DEP'T OF JUST., NEIGHBORHOOD WATCH MANUAL 1, https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/NSA_NW_Manual.pdf [https://perma.cc/TX3S-N3FP] (explaining that the National Sheriffs' Association created the National Neighborhood Watch Program to prevent crime in residential areas).

19. *See, e.g.*, JAMES SUROWIECKI, THE WISDOM OF CROWDS xv (2005) ("[C]hasing the expert is a mistake, and a costly one at that. We should stop hunting and ask the crowd (which, of course, includes the geniuses as well as everyone else) instead. Chances are, it knows.").

20. Jeff Howe, *The Rise of Crowdsourcing*, WIRED (June 1, 2006, 12:00 PM), https://www.wired.com/2006/06/crowds/ [https://perma.cc/V6PV-KBYR].

21. DAREN C. BRABHAM, CROWDSOURCING xix (2013); *see also* 15 U.S.C. § 3724(c)(2) ("The term 'crowdsourcing' means a method to obtain needed services, ideas, or content by soliciting voluntary contributions from a group of individuals or organizations, especially from an online community.").

contexts, including business,[22] human rights,[23] national security,[24] cybersecurity,[25] medical[26] and scientific research,[27] and intellectual property.[28]

Crowdsourcing is also now playing a significant role in foundational governmental operations,[29] including criminal investigations. Variously described as "web,"[30] "armchair,"[31] "serial,"[32] "cyber,"[33] or "forensic–

22. *See, e.g.*, LARISSA KATHARINA SENNINGER, WISDOM OF THE CROWD IN EXPERIMENTS 2 (2018) (examining the use of crowdsourcing in experimental capital markets).

23. *See, e.g.*, Marta Poblet & Jonathan Kolieb, *Responding to Human Rights Abuses in the Digital Era: New Tools, Old Challenges*, 54 STAN. J. INTL. L. 259, 261 (2018) (discussing the role of crowdsourcing in assisting human rights monitoring).

24. *See, e.g.*, JENNIFER YANG HUI, CROWDSOURCING FOR NATIONAL SECURITY 3 (2015), https://www.rsis.edu.sg/wp-content/uploads/2015/03/PR150317_Crowdsourcing-for-National-Security.pdf [https://perma.cc/5Q7D-TGT5] (exploring how crowdsourcing has been used in gathering intelligence for national security efforts).

25. *See, e.g.*, Alison DeNisco Rayome, *Is Crowdsourcing Cybersecurity the Answer to CISOs' Problems?*, TECHREPUBLIC (Mar. 28, 2019, 6:40 AM), https://www.techrepublic.com/article/is-crowdsourcing-cybersecurity-the-answer-to-cisos-problems/ [https://perma.cc/HH2T-G88B] (noting that organizations are increasingly turning to crowdsourced security options to avoid data breaches).

26. *See, e.g.*, Jordan Paradise, *Exploring Precision FDA, an Online Platform for Crowdsourcing Genomics*, 58 JURIMETRICS J. 267, 268 (2018) ("Medical research, and cancer research specifically, has recently embraced open-source, crowdsourcing models . . . .").

27. *See, e.g.*, Eric Luis Uhlmann, Charles R. Ebersole, Christopher R. Chartier, Timothy M. Errington, Mallory C. Kidwell, Calvin K. Lai, Randy J. McCarthy, Amy Riegelman, Raphael Silberzahn & Brian A. Nosek, *Scientific Utopia III: Crowdsourcing Science*, 14 PERSP. ON PSYCHOL. SCI. 711, 727 (2019) (arguing that crowdsourcing can complement the standard model of scientific investigation and accelerate scientific discovery); *see, e.g.*, 15 U.S.C. § 3724 (designating the provision as the "Crowdsourcing and Citizen Science Act").

28. *See, e.g.*, Lisa Larrimore Ouellette, *The Google Shortcut to Trademark Law*, 102 CALIF. L. REV. 351, 353–54 (2014) (noting that Google results can help determine an important factual issue in trademark law: whether consumers associate a mark with a certain product).

29. *See* Jennifer Shkabatur, *Cities @ Crossroads: Digital Technology and Local Democracy in America*, 79 BROOKLYN L. REV. 1413, 1443 (2011) (defining "governmental crowdsourcing" as "the process of outsourcing certain governmental functions to the broad public, and soliciting back services, suggestions, solutions, and ideas").

30. Elizabeth Yardley, Adam George Thomas Lynes, David Wilson & Emma Kelly, *What's the Deal with 'Websleuthing'? News Media Representations of Amateur Detectives in Networked Spaces*, 14 CRIME, MEDIA, CULTURE 81, 82 (2018).

31. Vic Ryckaert, *ISP to Facebook Users: Stop 'Armchair Sleuthing' on Delphi Murders*, INDYSTAR (July 19, 2017, 5:03 PM), https://www.indystar.com/story/news/crime/2017/07/19/isp-facebook-users-stop-armchair-sleuthing-delphi-murders/491871001/ [https://perma.cc/W5BN-HAP6].

32. Jason Tashea, *California Police Release True-Crime Podcast in Hopes the Public Can Help Find a Fugitive*, ABA J. (Jan. 1, 2019, 2:35 AM), https://www.abajournal.com/magazine/article/california_police_true_crime_podcast [https://perma.cc/DUZ4-34WT] (describing how a California police department was inspired by the podcast *Serial* to produce its own podcast in order to boost public engagement).

33. Laura Huey, Johnny Nhan & Ryan Broll, *'Uppity Civilians' and 'Cyber-Vigilantes': The Role of the General Public in Policing Cyber-Crime*, 13 CRIMINOLOGY & CRIM. JUST. 81, 86 (2012).

genetic" sleuths (who scour open source DNA databases),[34] they reflect and embody an important shift toward "online civilian policing."[35]

Perhaps the best-known early example of crowdsourcing occurred in connection with the Boston Marathon bombings in 2013.[36] In the wake of the bombings, federal agents posted photos on the online community Reddit, requested public assistance, directed and redirected content concerning identification of the bombers, and publicly expressed hope that "[m]aybe crowd sourcing will help catch the suspects."[37] More recently, police in Newport Beach, California, created a podcast entitled *Countdown to Capture* that provided details about an unsolved murder and urged that "any constructive help . . . is much needed."[38] Similarly, the popular *Websleuths* website allows "[o]rdinary people from all walks of life [to] come together . . . to dissect clues to crimes and unravel real-life mysteries."[39] The website owner told one media outlet: "[Law enforcement] give[s] us something mundane that . . . [they've] looked at for 20 years, we're looking at it fresh and we're excited. That's the beauty of it. Thousands of fresh eyes looking at it for nothing. . . . We're just waiting for orders."[40]

34. *See, e.g.*, Heather Murphy, *How Volunteer Sleuths Identified a Hiker and Her Killer After 36 Years*, N.Y. TIMES (May 11, 2019), https://www.nytimes.com/2019/05/11/us/cold-case-genealogy-dna.html [https://perma.cc/E5B6-JG2R] (describing how a group of volunteers identified both a victim and her murderer with the help of genetic genealogy); *see also* Daniel Compton & J.A. Hamilton Jr., *An Examination of the Techniques and Implications of the Crowd-sourced Collection of Forensic Data*, IEEE INT'L CONF. ON PRIV., SEC., RISK, AND TRUST, AND IEEE INT'L CONF. ON SOC. COMPUTING 892 (2011), https://ieeexplore.ieee.org/document/6113236?denied= [https://perma.cc/9Q7S-HQ3T] (discussing crowdsourced forensic investigations).

35. Huey et al., *supra* note 33, at 85.

36. *See* Spencer Ackerman, *Data for the Boston Marathon Investigation Will Be Crowdsourced*, WIRED (Apr. 16, 2013, 1:18 PM), https://www.wired.com/2013/04/boston-crowdsourced/ [https://perma.cc/3HW7-RGPV] (describing how investigators, in an "unusual move," publicly requested images and video from any Boston Marathon spectators who witnessed the bombings).

37. Nhan et al., *supra* note 15, at 356; *see also* Richard DesLauriers, Special Agent in Charge, Federal Bureau of Investigation, Remarks of Special Agent in Charge Richard DesLauriers at Press Conference on Bombing Investigation (Apr. 18, 2013), https://archives.fbi.gov/archives/boston/press-releases/2013/remarks-of-special-agent-in-charge-richard-deslauriers-at-press-conference-on-bombing-investigation-1 [https://perma.cc/K4EN-WHT2] ("Today, we are enlisting the public's help to identify the two suspects. . . . We know the public will play a critical role in identifying and locating them.").

38. Tashea, *supra* note 32.

39. Tamara Gane, *Should Police Turn to Crowdsourced Online Sleuthing?*, OZY (Aug. 13, 2018), https://www.ozy.com/opinion/should-police-turn-to-crowdsourced-online-sleuthing/88691/ [https://perma.cc/YVS7-GZKV].

40. *Id.*

Tapping into the willingness, expertise, and resources of community members worldwide promises many benefits,[41] and has resulted in several arrests.[42] However, crowdsourcing also raises several important questions. As a constitutional matter, for instance, should citizen crowdsourcers, suspicious about a particular individual, be permitted to access the individual's computer files when the Fourth Amendment would prevent police from doing so without a warrant? Similarly, should they be permitted to access DNA databases for investigative purposes, notwithstanding the possible wishes of genetic database contributors[43] and Fourth Amendment constraints,[44] if and when they are imposed?

Crowdsourcing also presents significant practical risks. First and foremost, there is concern that an individual will be misidentified as a suspect, as occurred with the Boston Marathon crowdsourcing,[45] or that animus of some kind will cause an individual to be targeted.[46] In the often-

41. *See* Nhan et al., *supra* note 15, at 345 (noting that a community-fueled search engine has "the potential security capital of the public node when mobilized . . . and illustrates how public groups can, through countless connections across the web, draw upon a significant volume and diversity of individual knowledge and expertise to achieve their aims").

42. *See, e.g.*, Sara E. Wilson, *Cops Increasingly Use Social Media to Connect, Crowdsource*, GOV'T TECH (May 5, 2015), https://www.govtech.com/social/Cops-Increasingly-Use-Social-Media-to-Connect-Crowdsource.html [https://perma.cc/2M67-RYQ3] (describing various arrests made by police with the assistance of crowdsourcing).

43. *See* Jason Tashea, *Genealogy Sites Give Law Enforcement a New DNA Sleuthing Tool, but the Battle over Privacy Looms*, ABA J. (Nov. 1, 2019, 4:20 AM), https://www.abajournal.com/magazine/article/family-tree-genealogy-sites-arm-law-enforcement-with-a-new-branch-of-dna-sleuthing-but-the-battle-over-privacy-looms [https://perma.cc/9LH5-TLX9] (discussing the effect of law enforcement assistance "opt out" provisions in agreements signed by individuals providing DNA samples for analysis); *see also* Heather Murphy, *Why a Data Breach at a Genealogy Site Has Privacy Experts Worried*, N.Y. TIMES (Aug. 1, 2020), https://www.nytimes.com/2020/08/01/technology/gedmatch-breach-privacy.html#:~:text=Genealogists%20know%20that%20they%20cannot,who%20were%20not%20even%20real [https://perma.cc/5ZFU-4U58] (discussing hacking of site in which genealogy data of individuals who "opted out" was made accessible to law enforcement).

44. *See generally* Natalie Ram, *Genetic Privacy After* Carpenter, 105 VA. L. REV. 1357 (2019) (discussing the effect of the third-party doctrine on privacy rights regarding privately operated DNA analysis companies).

45. *See* Dave Lee, *Boston Bombing: How Internet Detectives Got It Very Wrong*, BBC NEWS (Apr. 19, 2013), https://www.bbc.com/news/technology-22214511 [https://perma.cc/BQW8-HJRM] (describing the misidentification of suspects in the internet crowdsourcing following the Boston Marathon bombing, including a wrongly accused man who had been missing since March).

46. *See* Hanna Kozlowska, *Are Neighborhood Watch Apps Making Us Safer?*, YAHOO! NEWS (Oct. 29, 2019, 9:00 AM), https://news.yahoo.com/amphtml/neighborhood-watch-apps-making-us-140042160.html [https://perma.cc/GUU4-AAZB?type=image] (describing instances of racial bias leading to improper suspicion or targeting of individuals by users of neighborhood watch apps); *see also* Belle Lin & Camille Baker, *Citizen App Again Lets Users Report Crimes—and Experts See Big Risks*, INTERCEPT (Mar. 2, 2020, 7:00 AM), https://theintercept.com/2020/03/02/citizen-app/ [https://perma.cc/8ZTX-A2ZS] (noting that experts have warned that crime-tracking apps like Citizen may encourage racial profiling and increase paranoia about criminal activity); Crime &

unconstrained echo chamber of the internet, in short, the wisdom of the crowd can readily become the tyranny of the crowd, with very significant negative consequences for wrongly targeted individuals. Second, crowdsourcing has serious implications for democratic governance and social cohesion. In China, where Mao advocated that the "masses have sharp eyes,"[47] reports have surfaced of widespread public use of a crowdsourcing "human flesh search engine," dedicated to outing and punishing unethical yet lawful behaviors.[48]

At the same time, it would be a mistake to view crowdsourcing in isolation. Rather, alongside developments such as police subsidization of civilian purchases of Amazon Ring doorstep cameras and collection of surveillance footage via the "Neighbors Portal,"[49] and Amazon's related "Neighbors App,"[50] it is part of a broader pluralization of crime control

Justice News, *Nextdoor Takes More Steps to Curb Its "Karen Problem*," CRIME REP. (July 2, 2020), https://thecrimereport.org/2020/07/02/nextdoor-takes-more-steps-to-curb-its-karen-problem/ [https://perma.cc/FV6B-KZBQ] (reporting that the neighborhood social media app NextDoor, which has been criticized for hosting racist comments, has vowed to increase monitoring of the app).

47. Simon Denyer, *China's Watchful Eye: Beijing Bets on Facial Recognition in a Big Drive for Total Surveillance*, 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/8W8F-YSHP].

48. *See* 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, 352–54 (2016) (describing the phenomenon as a goal-oriented collective activity in which users work together to achieve common goals, like tracking down norm transgressors); *see also* 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/PHE7-EER7] (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/B7S6-PJTB] (describing how grassroots "flesh-searching" is used in China in the absence of the rule of law).

49. *See* John Herrman, *Who's Watching Your Porch?*, N.Y. TIMES (Jan. 19, 2020), https://www.nytimes.com/2020/01/19/style/ring-video-doorbell-home-security.html [https://perma.cc/A7B3-5RDP] (noting that more than five hundred police departments have partnered with Amazon to gain access to the Neighbors Portal, which allows police to request video footage from Ring users, and that some departments have assisted in marketing efforts and offered discounted purchase prices for Ring cameras to local citizens).

50. *See* RING, *How Public Safety Agencies Use Neighbors*, https://support.ring.com/hc/en-us/articles/360031595491-How-Law-Enforcement-Uses-the-Neighbors-App [https://perma.cc/6JE9-MGWJ] (noting that police monitor postings and "use the video request feature . . . to request video recordings from Ring device owners who are in the area of an active investigation"); *see also, e.g.*, *Phoenix Police Can Now Crowdsource Evidence of Crimes from Residents*, KTAR NEWS (Dec. 13, 2018, 1:04 PM), https://ktar.com/story/2355129/phoenix-police-can-now-crowdsource-evidence-of-crimes-from-residents/ [https://perma.cc/6CZZ-QWVV] (reporting that the Phoenix Police Department joined the Neighbors App to monitor residents' feeds and to request video footage).

efforts,[51] entailing a "shift from *police* to *policing*,"[52] the constituent parts of which operate largely free of regulation and accountability. This evolution itself, moreover, is occurring amid justified concern over the increasing opacity and secrecy of the workings of the criminal justice system more generally,[53] and policing in particular.[54]

This Essay begins with an overview of recent crowdsourcing efforts and examines the benefits and risks they present. The discussion then turns to an examination of whether the Fourth Amendment, its private search doctrine in particular, can provide a basis for their regulation. As noted earlier, scholars of late have condemned the private search doctrine for its underinclusiveness when strictly applied to data collection.[55] With crowdsourcing, strict application of the doctrine is also problematic. But the problem actually lies in its overinclusiveness, which risks obliteration of the still important public–private actor distinction; if all private assistance is deemed public and subject to constitutional prohibition, the potential benefits of crowdsourcing will be unduly sacrificed. Modified in the manner suggested in Part III, however, the private search doctrine can still serve as a viable basis for the regulation of crowdsourcing, which is quickly becoming the hue and cry of the twenty-first century.

I. Crowdsourcing: Its Benefits and Risks

Crowdsourcing scenarios fall on a continuum of law enforcement instigation and citizen involvement.[56] On one extreme are efforts by citizens,

---

51. *See* Drew Harwell, *Ring and Nest Helped Normalize American Surveillance and Turned Us into a Nation of Voyeurs*, WASH. POST (Feb. 18, 2020, 7:00 AM), https://www.washingtonpost.com/technology/2020/02/18/ring-nest-surveillance-doorbell-camera/ [https://perma.cc/5L6Z-TDRV] (noting that Ring and Nest devices have allowed Americans to become their own "personal security force" and greatly enhanced the criminal surveillance powers of law enforcement).

52. Ian Loader, *Plural Policing and Democratic Governance*, 9 SOC. & LEGAL STUD. 323, 323 (2000) (emphasis in original).

53. *See, e.g.*, Stephanos Bibas, *Transparency and Participation in Criminal Procedure*, 81 N.Y.U. L. REV. 911, 917 (2006) (describing the opacity of the modern criminal justice system and urging greater transparency and participation in the system); Meghan J. Ryan, *Secret Conviction Programs*, 77 WASH. & LEE L. REV. 269, 274–76 (2020) (noting "the secrecy shrouding the algorithms and source codes leading to defendant convictions" and arguing that it is a problem of "constitutional proportions").

54. *See generally* Hannah Bloch-Wehba, *Visible Policing: Technology, Transparency, and Democratic Control*, 109 CALIF. L. REV. (forthcoming 2021) (discussing the lack of transparency of modern policing technology, methods, and techniques); Jonathan Manes, *Secrecy and Evasion in Police Surveillance Technology*, 34 BERKELEY TECH. L.J. 503 (2019) (discussing the secrecy surrounding novel policing technologies).

55. *See supra* notes 12–14 and accompanying text**.**

56. *See generally* Enrique Estellés-Arolas, *Using Crowdsourcing for a Safer Society: When the Crowd Rules*, 17 EUR. J. CRIMINOLOGY (SPECIAL ISSUE) 1, 2, 15 (2020) (discussing the results of a survey regarding crowdsourcing initiatives worldwide).

who on their own collect and analyze information that they provide police, such as "Project Cold Case"[57] and the "Reddit Bureau of Investigation," which in 2018 boasted over 70,000 online members.[58] Into this category, one can add the burgeoning number of true crime investigative podcasts such as *Serial*, which provide details on unsolved crimes[59] or cases where the guilt of a convicted individual is in question.[60] For those in need of assistance, self-enterprising sleuths even have a manual at their disposal.[61]

The foregoing can be easily categorized as private searches, based on conventional doctrine. The focus here, however, is on scenarios involving a greater degree of police involvement in mobilizing the masses.

As the examples provided at the outset highlight, law enforcement has awakened to the benefits of crowdsourcing.[62] By way of further example, the

---

57. *See Project: Cold Case FAQs*, PROJECT: COLD CASE, https://www.projectcoldcase.org/faqs/ [https://perma.cc/KZ5X-FE2J] ("[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."). Also, self-initiated individuals and groups seek to root out online sex predators who target children (or those they believe to be children). Debra Cassens Weiss, *Vigilante Child Predator Stings Are Dangerous and Illegal, Wisconsin Attorney General Says*, ABA J. (Sept. 4, 2019, 11:34 AM), https://www.abajournal.com/news/article/vigilante-child-predator-stings-are-dangerous-and-illegal-wisconsin-attorney-general-says#:~:text=Vigilante%20child%20predator%20stings%20are%20dangerous%20and%20illegal%2C%20Wisconsin%20attorney%20general%20says,By%20Debra%20Cassens&text=Kaul%20discouraged%20the%20practice%20in,the%20suspects%20and%20the%20public. [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?utm_source=Sailthru&utm_medium=email&utm_campaign=ebb%205/1/18&utm_term=Editorial%20-%20Early%20Bird%20Brief [https://perma.cc/KA4Y-ADPH].

58. David Myles, Chantal Benoit-Barné & Florence Millerand, *'Not Your Personal Army!' Investigating the Organizing Property of Retributive Vigilantism in a Reddit Collective of Websleuths*, 23 INFO., COMM. & SOC'Y 317, 318 (2018).

59. Ted Muldoon, *Investigative Podcasts Are Exploding. Here Are Six Great Ones to Get You Started*, WASH. POST (Jan. 2, 2020, 6:00 AM), https://www.washingtonpost.com/arts-entertainment/2020/01/02/investigative-podcasts-are-exploding-here-are-six-great-ones-get-you-started/ [https://perma.cc/3EU3-GNCR]; *see also, e.g.*, Dan Reilly, *How True Crime Podcast 'The Murder Squad' Will Crowdsource Investigations*, FORTUNE (Apr. 1, 2019, 8:00 AM), https://fortune.com/2019/04/01/murder-squad-podcast-crowdsource/ [https://perma.cc/6WCZ-LTJH] (discussing the debut of a new podcast in which listeners were invited to take part in its investigations of unsolved murders and disappearances).

60. *See, e.g.*, Michael Hall, *Crowdsourcing Justice*, TEXAS MONTHLY (Aug. 2019), https://www.texasmonthly.com/articles/truth-justice-podcast-army-free-ed-ates/ [https://perma.cc/4VTZ-E95E] (recounting the role of crowdsourcing in the exoneration of Texas inmate Edward Ates).

61. JENNIFER GOLBECK, INTRODUCTION TO SOCIAL MEDIA INVESTIGATION: A HANDS-ON APPROACH (Judith L. Klavans ed., 2015).

62. *See* Mark Velez, *See Something, Say Something, Send Something: Everyone Is a Cyber Detective*, POLICE CHIEF MAG. (2018), https://www.policechiefmagazine.org/see-something-say-something-send-something/ [https://perma.cc/2SYP-ANEA?type=image] ("The idea of thousands

FBI recently issued a public plea to "Help Break the Code" contained in two letters found on the body of a murdered Missouri man,[63] with the FBI cryptoanalysis chief explaining that "[s]tandard routes of cryptanalysis seem to have hit brick walls," and "[m]aybe someone with a fresh set of eyes might come up with a brilliant new idea."[64] The Johns Creek, Georgia, Police Department uses a mobile app, interoperable with social media platforms like Twitter and Facebook, that allows community members to obtain information from the department and assist in investigations. With its "Wanted Wednesday" series, the department posts pictures and related information regarding suspects, which often results in arrests.[65] Crowdsourcing can also occur in person. Illustrative is the recent inaugural "CrowdSolve" event in Seattle, overseen by the local sheriff and a retired U.S. marshal, where attendees heard from forensics experts about two unsolved area killings and split into three groups of one hundred to identify suspects.[66]

Crowdsourcing efforts have been shaped by a variety of forces, including the abiding interest in "true crime" stories, "do-it-yourself" (DIY) culture, and frustration with the crime-solving ability of police

---

of 'cyber detectives' capturing and submitting evidence to law enforcement has the potential to transform the way crimes are investigated, solved, and prosecuted."); *see also* Cole Zercoe, *Crowdsourcing Crime: Why the Public May Be Your Best Investigative Asset*, POLICE1 (Mar. 23, 2017), https://www.police1.com/police-products/video-storage/articles/crowdsourcing-crime-why-the-public-may-be-your-best-investigative-asset-WZIVQIirCG1XlMOU/ [https://perma.cc/8VN6-4FPA] (recounting instances where police relied on crowdsourcing to investigate crimes and suggesting techniques to improve the effectiveness of crowdsourcing for police).

63. *Help Break the Code*, FED. BUREAU INVESTIGATION, https://forms.fbi.gov/code#googtrans [https://perma.cc/4D22-MF8Y].

64. *Crime & Crowdsourcing – The Crowd Acts as Investigator*, CLICKWORKER (Nov. 5, 2011), https://www.clickworker.com/2011/05/11/crime-and-crowdsourcing-die-community-als-ermittler/ [https://perma.cc/C9MX-C5LW].

65. Wilson, *supra* note 42. Not surprisingly, private businesses have also employed crowdsourcing and have had considerable success identifying suspected shoplifters and suspects in property damage cases. *See, e.g.*, *About Us*, CAPTIS INTELLIGENCE, https://www.captisintelligence.com/company/aboutus.html [https://perma.cc/76W8-WG3K] (stating that over a dozen Fortune 500 companies have utilized the company's products, which incorporate crowdsourcing). Also, private entities such as "Solveacrime.com" utilize crowdsourcing to assist individual victims and businesses in identifying suspects. SOLVEACRIME, https://www.solveacrime.com/ [https://perma.cc/VBM2-L3ZK].

66. Andrea Cipriano, *My Weekend as an Amateur Cold Case Detective*, CRIME REP. (Nov. 12, 2019), https://thecrimereport.org/2019/11/12/my-weekend-as-an-amature-cold-case-detective/ [https://perma.cc/HJE8-E8YG]. The organizing entity, CrimeCon, planned similar events in Austin and Chicago and a "crimecruise" in the Caribbean that promises "hot sun and cold cases." CRIMECON, https://www.crimecon.com/events [https://perma.cc/9N4P-7XAM]; *see also* Heather Murphy, *Playing Catch a Killer with a Room Full of Sleuths*, N.Y. TIMES (Dec. 30, 2019), https://www.nytimes.com/2019/10/05/us/genetic-genealogy-guidelines-privacy.html [https://perma.cc/PA6Y-YKKV] (describing a similar crime-solving event).

(especially regarding "cold" cases).[67] The movement also bears the earmarks of the public's sense of informational entitlement, reflected in government-operated public sex offender registry websites,[68] and the advent of community policing, with its emphasis on citizens as "coproducers" of public safety.[69] Of late as well, sharp criticism and distrust of local police in the wake of the killing of civilians, fueling calls that departments be "defunded," are prompting reevaluation of the ways in which community members can shoulder greater responsibility in maintaining public safety.[70]

Harnessing the time, expertise, and resources of community members to solve crimes has obvious upsides. Doing so benefits from what is known in business as a "long tail" effect, whereby the power of probabilities is combined with the numeric wherewithal of the masses, increasing the chances of investigative success.[71] The probabilistic quality of crowdsourcing itself, however, raises concern over false positives—the misidentification of criminal suspects. As noted earlier, in the wake of the Boston Marathon bombings, crowdsourcers wrongly identified suspected bombers, including a missing college student who actually committed suicide before the bombings, subjecting his family to threatening messages and additional trauma.[72] Misidentification also occurred in the hours after the recent violence occurring amid demonstrations in Charlottesville, Virginia.[73]

---

67. *See generally* DEBORAH HALBER, THE SKELETON CREW: HOW AMATEUR SLEUTHS ARE SOLVING AMERICA'S COLDEST CASES (2014) (discussing the development of online communities dedicated to solving unsolved murders).

68. *See* WAYNE A. LOGAN, KNOWLEDGE AS POWER: CRIMINAL REGISTRATION AND COMMUNITY NOTIFICATION LAWS IN AMERICA 101–03 (2009) (describing how changes in popular sentiment resulted in feelings of public entitlement to registrant information).

69. *See generally* WESLEY G. SKOGAN & SUSAN M. HARTNETT, COMMUNITY POLICING, CHICAGO STYLE (1997) (discussing the role of community members as "coproducers" of public safety and evaluating the results of a community policing program in Chicago).

70. Nellie Bowles, *Why Is a Tech Executive Installing Security Cameras Around San Francisco?*, N.Y. TIMES (July 13, 2020), https://www.nytimes.com/2020/07/10/business/camera-surveillance-san-francisco.html [https://perma.cc/TN9U-2DL2].

71. *See generally* CHRIS ANDERSON, THE LONG TAIL: WHY THE FUTURE OF BUSINESS IS SELLING LESS OF MORE (2006) (describing the phenomenon in which obscure or niche products sell at least one unit, resulting in sizable collective market share).

72. *See supra* notes 36–37, 45 and accompanying text; *see also* Nhan et al., *supra* note 15, at 354 (describing the emotional trauma suffered by the family of the misidentified individual).

73. Maurice Chammah & Simone Weichselbaum, *Crowdsourcing the Charlottesville Investigation: The Mixed Blessing of an Internet Posse*, MARSHALL PROJECT (Aug. 14, 2017, 6:16 PM), https://www.themarshallproject.org/2017/08/14/crowdsourcing-the-charlottesville-investigation [https://perma.cc/ZY6P-ZV3K]; *see also, e.g.*, *Police Hold Wrong Woman After 'America's Most Wanted' Tip*, AP NEWS (Dec. 26, 1992), https://apnews.com/515f42c5341aa22d7802c4ad43a270e5 [https://perma.cc/5CFM-B93G] (noting that police kicked in the door of a woman's home and held her in handcuffs based on false identification provided by viewer of show who thought she was the sought-after murder suspect, and noting other arrests elsewhere based on viewers' false identifications).

As with so much else regarding the internet, the enabling of mass (often anonymous) communication can be problematic, a risk enhanced by the lack of regulation and quality control measures common to open source data pools.[74] Even well-meaning crowdsourcers can succumb to what data scientists call an "information cascade" dynamic, whereby instead of assessing the reliability of information on their own, they rely on what they assume others have reliably concluded and transmit the possibly false information,[75] which the internet relentlessly then perpetuates.[76] Moreover, citizen sleuths might lack key information that police alone possess,[77] an asymmetry also contributing to risk of misidentification as well as creation of false leads.[78] In short, however defensible risk tolerance might be in other crowdsourcing contexts, the dire consequences flowing from misidentification in criminal investigations raise significant concern.

Crowdsourcing can also jeopardize investigations. While police are quick to laud and encourage public input, they worry that information secured might be tainted, such as by chain-of-evidence problems.[79] Likewise, even if

74. Morgan Crider, Comment, *Corporate Genealogists: The New Homicide Detectives*, 22 SMU SCI. & TECH. L. REV. 153, 161–63 (2019). As in other contexts, in the internet era "[f]or better and worse, we live in a world in which there is simultaneously too much information and too little." GARY ALAN FINE & BILL ELLIS, THE GLOBAL GRAPEVINE: WHY RUMORS OF TERRORISM, IMMIGRATION, AND TRADE MATTER 4 (2010).

75. *See generally* DAVID EASLEY & JON KLEINBERG, NETWORKS, CROWDS, AND MARKETS: REASONING ABOUT A HIGHLY CONNECTED WORLD (2010) (discussing the psychology behind and effects of information cascades).

76. *See, e.g.*, Nicholas Confessore, Gabriel J.X. Dance, Richard Harris & Mark Hansen, *The Follower Factory*, N.Y. TIMES (Jan. 27, 2018), https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html [https://perma.cc/E7DW-T5QY] (noting that Facebook estimates that up to sixty million automated "bots" might roam its platform).

77. *See* Hannah Jane Parkinson, *Caleb Bratayley's Death Is Not a Mystery—Online Sleuths Should Stand Down*, GUARDIAN (Oct. 9, 2015, 8:32 AM), https://www.theguardian.com/technology/2015/oct/09/caleb-bratayley-vlogger-death-not-mystery-youtube [https://perma.cc/VZF9-WMT8] (noting that "[w]annabe sleuths have always existed . . . [b]ut broadband internet has made it easier for people to position themselves as detectives. . . . Mining social media leads people to believe they are in full possession of the facts . . . .").

78. *See, e.g.*, Stephanie Faris, *In an Internet Era, Can Armchair Detectives Actually Solve a Case?*, PAC. STANDARD (June 14, 2017), https://psmag.com/news/in-an-internet-era-can-armchair-detectives-actually-solve-a-case [https://perma.cc/U755-W7Q5] (noting that tips to law enforcement from amateur sleuths can waste time and resources).

79. *See, e.g.*, Virginia Pelley, *Who Done It? Citizen Investigators Mine Social Media for Crime Clues*, AL JAZEERA AM. (June 7, 2014, 5:00 AM), http://america.aljazeera.com/articles/2014/6/7/citizen-crime-sleuths.html [https://perma.cc/LEE8-38YM] (explaining that even seemingly irrefutable crowdsourced evidence may raise chain-of-evidence concerns when it is given to police by non-law-enforcement personnel).

accurate, information generated by a "smart mob" can,[80] when publicly disclosed, contaminate an investigation.[81]

For these reasons, and mindful that if they leave a vacuum, individuals will likely step in and perhaps behave even more recklessly,[82] departments have provided crowdsourcing fora and guidelines for input and assistance, for instance by discouraging public identification of specific suspects.[83] However, the Catch-22 of doing so is that the more engaged police are in regulating the crowd the stronger the case becomes for deeming the police effort a deputization of private parties as discussed below.

More broadly, as noted at the outset, the public–private convergence of crime control efforts has serious potential ramifications for democratic governance. Not only are private entities now providing surveillance and personal information to police,[84] but community members, by dint of crowdsourcing, are actively assisting in criminal investigations. In this environment, as Michel Foucault would put it, the citizen becomes at once the agent and object of surveillance and investigation.[85] We are not only

80. *See* HOWARD RHEINGOLD, SMART MOBS: THE NEXT SOCIAL REVOLUTION xi–xii (2002) (coining the term "smart mobs" to refer to the vast social network that mobile device users participate in when they communicate through their smartphones.)

81. *See, e.g.*, Pelley, *supra* note 79 (explaining the risks of this evidence being rendered useless).

82. As researchers have noted, "police failure to fully involve the general public and reciprocally share information regarding ongoing investigations can frustrate well-meaning digilantes. . . . Such frustrations may increase the likelihood of potentially problematic and even dangerous forms of vigilantism . . . ." Nhan et al., *supra* note 15, at 358 (citation omitted). "[I]f there is a public desire to collectively 'assist' the police in ongoing investigations, there is likely little the police can do to stop such efforts." *Id.*

83. *See, e.g.*, JOSHUA REEVES, CITIZEN SPIES: THE LONG RISE OF AMERICA'S SURVEILLANCE SOCIETY 37–40 (2017) (describing the efforts undertaken by the Philadelphia Police Department and other police departments); *see also* Nhan et al., *supra* note 15, at 358–59 (averring that "[p]olice management of public online investigational activities might not only potentially generate more useful information but minimize negative impacts," like the misidentification of suspects; urging that crowdsourcing "fill organizational holes"; and advocating that police "focus the public's attention on key areas of the investigation in which they are most in need of support," such as releasing a brief description of a suspect to facilitate crowdsourced review of photos). For similar efforts to guide criminal investigative crowdsourcing more generally, see Kemal Veli Açar, *OSINT by Crowd-sourcing: A Theoretical Model for Online Child Abuse Investigations*, 12 INTL. J. CYBER CRIMINOLOGY 206 (2018) and Antonio Vera & Torsten Oliver Salge, *Crowdsourcing and Policing: Opportunities for Research and Practice*, EUR. POL. SCI. & RES. BULL., Summer 2017, at 143. For discussion of efforts to guide crowdsourcing in the business context, see generally Ivo Blohm, Shkodran Zogaj, Ulrich Bretschneider & Jan Marco Leimeister, *How to Manage Crowdsourcing Platforms Effectively?*, CAL. MGMT. REV., Winter 2018, at 122.

84. *See supra* notes 10–14 and accompanying text.

85. *See* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 202–03 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977) ("He who is subjected to a field of visibility, and who knows it, . . . inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection."). Meanwhile, citizen-consumers are increasingly complicit in their own surveillance, such as by gadgets contained in the "Internet of Things" (e.g., Amazon's "Alexa" device), which allow them to effectively trade privacy for

asked to "see something, say something."[86] We are asked to *do something*: investigate and inform upon our fellow community members. In so doing, the government is achieving what Foucault called "responsibilization,"[87] "managing the public by having it manage itself."[88]

China appears to be working hard to achieve this goal,[89] and prior governments, such as the former East Germany,[90] attest to its possible attainment.[91] Here in the U.S., seeing a business opportunity, Vizsafe is marketing an app to motivate citizens to provide tips and video by providing blockchain incentives in the form of digital rewards that can be redeemed at participating vendors.[92] At the same time, popular crowdsourcing mobile apps such as Citizen (né Vigilante), provide users real-time data on crimes, which, while often inaccurate, fuel citizen surveillance efforts and involvement in crime-fighting, as well as perhaps instill unjustified anxiety

convenience, with information eagerly collected and analyzed by police. *See generally* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805 (2016) (discussing the advent of the "Internet of Things" and the resulting increase in the amount of private data generated and collected).

86. Hanson O'Haver, *How "If You See Something, Say Something" Became Our National Motto*, WASH. POST (Sept. 23, 2016), https://www.washingtonpost.com/posteverything/wp/2016/09/23/how-if-you-see-something-say-something-became-our-national-motto/ [https://perma.cc/S7X3-94C4]; *see also* JIM REDDEN, SNITCH CULTURE: HOW CITIZENS ARE TURNED INTO THE EYES AND EARS OF THE STATE (2000) (describing the advent of "snitch culture" in the United States and noting that "[w]e're so used to being tracked that we don't even notice how often we're being urged to report our friends, neighbors, family members and strangers to the authorities").

87. *See* Michel Foucault, *The Subject and Power*, in MICHEL FOUCAULT: BEYOND STRUCTURALISM AND HERMENEUTICS 208–26 (Hubert L. Dreyfus & Paul Rabinow eds., 2d ed. 1982) (discussing the roles of power, freedom, and strategy acting "at the level of the whole social body, [and] the locking together of power relations with relations of strategy and the results proceeding from their interaction"); *see also* David Garland, *The Limits of the Sovereign State*, 36 BRIT. J. CRIMINOLOGY 445, 452–53 (1996) (discussing the efforts of contemporary governments to encourage "responsibilization" social control strategies).

88. TOBY MILLER, THE WELL-TEMPERED SELF: CITIZENSHIP, CULTURE, AND THE POSTMODERN SUBJECT xiii (1993).

89. *See supra* notes 47–48 and accompanying text.

90. *See* Peter Wensierski, *East German Snitching Went Far Beyond the Stasi*, DER SPIEGEL (Oct. 7, 2015, 5:05 PM), https://www.spiegel.de/international/germany/east-german-domestic-surveillance-went-far-beyond-the-stasi-a-1042883.html [https://perma.cc/HXS8-QVDV] (describing a "finely woven web of surveillance" in which East German citizens voluntarily informed on fellow citizens).

91. For more on the important role that the Fourth Amendment plays in democratic governance more generally, see Thomas P. Crocker, *The Political Fourth Amendment*, 88 WASH. U. L. REV. 303 (2010).

92. *See* Jon Glasco, *How Crowdsourcing and Incentives Improve Public Safety*, BEE SMART CITY (Mar. 10, 2019, 10:44 PM), https://hub.beesmart.city/en/solutions/smart-living/public-safety/how-crowdsourcing-and-incentives-improve-public-safety [https://perma.cc/2VX5-MPWS] (discussing the business model of Vizsafe and its use of incentives to encourage citizen participation).

over public safety.[93] Crowdsourcing, in short, has a constitutive aspect, at once emblematic of and serving as a method of governance.[94]

Furthermore, requesting and securing investigative information from often anonymous crowdsourcers risks worsening the current troubling lack of transparency in law enforcement more generally. Today, police often use new data-collection devices without public knowledge, and even if their use is known, resist disclosure of any limits regarding their operation.[95] Worse yet, the private tech sector, which provides the devices, often resists disclosure by invoking trade secret and business confidentiality interests.[96] Such government secrecy, as scholars have noted, is problematic because it undermines the transparency needed for the effective regulation of police in a liberal democratic society.[97]

Finally, crowdsourcing carries risk of a dangerous displacement of responsibility for crime control and public safety. The shift is reminiscent of the sentiment voiced by the individual identified as having conceived of sex offender community notification, which is predicated on empowering communities with information regarding the location of convicted sex

93. *See* Abigail Weinberg, *"It Creates a Culture of Fear": How Crime Tracking Apps Incite Unnecessary Panic*, MOTHER JONES (Aug. 9, 2019), https://www.motherjones.com/politics/2019/08/it-creates-a-culture-of-fear-how-crime-tracking-apps-incite-unnecessary-panic/ [https://perma.cc/FM4C-A5S8] **(**discussing the functionality of the Citizen app and concerns about the effect on communities of the high-volume dissemination of crime information of at times questionable reliability).

94. On constitutive theories of law more generally see, for example, ALAN HUNT, EXPLORATIONS IN LAW AND SOCIETY: TOWARD A CONSTITUTIVE THEORY OF LAW (1993).

95. *See generally* Jonathan Manes, *Secrecy & Evasion in Police Surveillance Technology*, 34 BERKELEY TECH. L.J. 503 (2019) (examining various examples and noting argument by law enforcement that the disclosure of technologies would allow criminals to evade the law, concluding that this "anti-circumvention argument" results in "far more secrecy than it can justify"). Police also, inter alia, engage in "parallel construction," whereby they conceal a secret illegal investigative method by conducting a parallel, legal method that "discovers" the evidence previously obtained unlawfully. *Id.* at 512–13.

96. *See* Natalie Ram, *Innovating Criminal Justice*, 112 NW. L. REV. 659, 665–66 (2018) (discussing private companies' use of trade secret law to protect their proprietary technologies and their assertion of trade secret status in litigation to bar or limit discovery of protected information); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1361–63 (2018) (same); *cf.* Kate Crawford & Jason Schultz, *AI Systems as State Actors*, 119 COLUM. L. REV. 1941, 1957–60 (2019) (discussing the shortcomings of the current "state actor" doctrine, which is used to hold private businesses constitutionally accountable, as governments increasingly rely on vendors to provide artificial intelligence-based public services).

97. *See, e.g.*, Erik Luna, *Transparent Policing*, 85 IOWA L. REV. 1107, 1164 (2000) (noting that transparency is "a well-developed norm of democratic government"); Manes, *supra* note 95, at 534 ("[W]hile the public is in the dark about the scope of the police's investigatory power, the government has access to ever more information . . . . History suggests that this information asymmetry can readily breed abuse, particularly in the absence of strong external checks."); Anne Joseph O'Connell, *The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World*, 94 CALIF. L. REV. 1655, 1716 (2006) (identifying transparency as one of the core values "fundamental to our society").

offenders, who acknowledged that the strategy sought to absolve government of responsibility for community safety.[98] Such displacement can both undercut government accountability for public safety[99] and foster vigilantism.[100] As the high rates of unsolved murders and other serious crimes attest,[101] and continued troubling instances of police misconduct reflect,[102] public law enforcement is far from perfect. However, as the historic evolution of crime control itself highlights, organized, trained, and sworn public law enforcement officers, in theory at least democratically accountable and subject to constitutional regulation,[103] are preferable to privatized justice and mob rule (by "netizens" or others).[104]

To conclude, crowdsourcing marks an important development in the evolution of crime control efforts. It is, to again borrow a term from business, a disruptive innovation,[105] the full implications of which are not yet known.

---

98. Jolayne Houtz, *When Do You Unmask a Sexual Predator*, SEATTLE TIMES, Aug. 30, 1990, at B2.

99. *See* Jack M. Beermann, *Privatization and Political Accountability*, 28 FORDHAM URB. L.J. 1507, 1519 (2001) ("[I]f a private entity were entrusted with carrying out a government activity, it might be difficult for the public to know whom in the political system to blame when things go wrong.").

100. *See, e.g.*, LOGAN, *supra* note 68, at 126–27, 159 (discussing instances of community members engaging in vigilantism against actual or suspected sex offender registrants and efforts by governments providing registrants' information to avoid legal liability for harms).

101. *See* Shima Baradaran Baughman, *How Effective Are Police? The Problem of Clearance Rates and Criminal Accountability*, 72 ALA. L. REV. (forthcoming 2021) (calculating "true" police clearance rates as a function of solved crimes with respect to the total number of crimes, both reported and unreported, and finding that true clearance rates for the last thirty years are around 10%).

102. *See generally* Jeffrey Fagan & Alexis D. Campbell, *Race and Reasonableness in Police Killings*, 100 B.U. L. REV. 951 (2020) (discussing the prevalence of killings, noting inter alia that African-Americans are more than twice as likely to be killed by police as persons of other racial or ethnic backgrounds).

103. *See generally* LAWRENCE M. FRIEDMAN, CRIME AND PUNISHMENT IN AMERICAN HISTORY 174–75 (1993) (discussing the history of American violence that sparked the shift from private to public policing); SAMUEL WALKER, POPULAR JUSTICE: A HISTORY OF AMERICAN CRIMINAL JUSTICE 56–65, 133–45 (1980) (noting that the development of the criminal justice system in the United States, including police departments, was "a response to the extraordinary disorder wrought by social change"). Community members, moreover, are not subject to a professional code of ethics, unlike investigative journalists, who can also play a role in solving crimes. *See SPJ Code of Ethics*, SOC'Y OF PROF. JOURNALISTS (Sept. 6, 2014, 4:49 PM), https://www.spj.org/ethicscode.asp [https://perma.cc/NRL3-AK47] (specifying, inter alia, the duty to "[v]erify information before releasing it" and "[m]inimize [h]arm").

104. *See* Elizabeth E. Joh, *Conceptualizing the Private Police*, 2005 UTAH L. REV. 573, 582–85 (2005) (surveying negative consequences of prior eras marked by privatized justice, including vigilantism); *cf.* David Alan Sklansky, *Private Police and Democracy*, 43 AM. CRIM. L. REV. 89, 98 (2006) (noting the negative redistributive effects of increased reliance on private policing).

105. *See* David Orozco, *The Use of Legal Crowdsourcing ("Lawsourcing") to Achieve Legal, Regulatory, and Policy Objectives*, 53 AM. BUS. L.J. 145, 150 (2016) ("Given its unique ability to efficiently source talent and resources, crowdsourcing has become a disruptive innovation.").

As sociologist Gary Marx has written regarding police crowdsourcing more generally, "[i]t isn't enough to justify it by saying the goal is good. We must also ask where it might lead and how it might be abused."[106] The next parts consider possible frameworks for the regulation of crowdsourcing efforts, which are growing by the day and playing an ever more important role in criminal investigations.

II. Regulating Crowdsourcing

Crowdsourcing can and does result in the search and seizure of individuals, raising the obvious question of whether constitutional law—the Fourth Amendment in particular—can serve as a basis to regulate its participants. As with other Fourth Amendment questions, a key issue is whether the exclusionary rule will apply, which will turn on whether a crowdsourcer qualifies as a private or governmental actor under the Supreme Court's private search doctrine.

The Court's seminal modern private search doctrine decision is *Coolidge v. New Hampshire*.[107] In *Coolidge*, police suspected that the defendant kidnapped and murdered a teenage girl, and upon visiting his home spoke with his wife.[108] The wife voluntarily provided police with items that incriminated the defendant, who later contended that the items should be suppressed because she unlawfully acted as an "instrument" of the state for Fourth Amendment purposes.[109] The Court rejected the argument, reasoning that the police had not "coerce[d] or dominate[d] [Mrs. Coolidge], or, for that matter . . . direct[ed] her actions by the more subtle techniques of suggestion that are available to officials in circumstances like these."[110]

Skinner v. Railway Executives' Labor Association,[111] decided almost twenty years later, is the Court's other significant modern decision concerning private searches. In *Skinner*, the Court addressed whether private railroads were acting as government agents when they sought to subject their workers to suspicionless post-accident breath or urine tests that were authorized by federal law.[112] At the outset, the *Skinner* Court noted that "[w]hether a private party should be deemed an agent or instrument of the

106. Gary T. Marx, *The Public as Partner? Technology Can Make Us Auxiliaries as Well as Vigilantes*, IEEE SEC. & PRIV., Sept./Oct. 2013, at 56, 60, http://web.mit.edu/gtmarx/www/marx-publicas.pdf [https://perma.cc/QUB3-ELTD].

107. 403 U.S. 443, 488 (1971).

108. *Id.* at 445–46.

109. *Id.* at 487.

110. *Id.* at 489.

111. 489 U.S. 602 (1989).

112. *Id.* at 613–14. Another subpart of the applicable federal regulation required blood and urine tests in certain circumstances, which the Court summarily concluded was regulated by the Fourth Amendment. *Id.* at 614.

Government for Fourth Amendment purposes necessarily turns on the degree of the Government's participation in the private party's activities, a question that can only be resolved 'in light of all the circumstances.'"[113]

Applying the test, a seven-Justice majority concluded that "the Government did more than adopt a passive position toward the underlying private conduct."[114] The Court rejected the railroads' assertion that the tests would "be primarily the result of private initiative,"[115] and concluded that the searches would not be private because "[t]he Government has removed all legal barriers to the testing authorized by . . . [the applicable law], and indeed has made plain not only its strong preference for testing, but also its desire to share the fruits of such intrusions."[116]

Other than two additional cases concerning the related question of whether police engage in a search when they expand the scope of a previous private party search,[117] *Coolidge* and *Skinner* constitute the Court's modern corpus of private search cases. In one of the scope-related cases, *United States v. Jacobsen*,[118] the Court averred that a search is private if the actor is "not acting as an agent of the Government or with the participation or knowledge of any governmental official."[119]

Lower federal courts tasked with drawing the public–private actor distinction have used a variety of similarly articulated tests. In the First Circuit, for instance, public-actor status depends on "[(1)] the extent of the government's role in instigating or participating in the search, [(2)] its intent and the degree of control it exercises over the search and the private party, and [(3)] the extent to which the private party aims primarily to help the government or to serve its own interests."[120] The Ninth Circuit uses a two-part test that asks "(1) whether the government knew of and acquiesced in the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or further his own ends."[121] In

113. *Id.* at 614–15 (citations omitted).

114. *Id.* at 615; *see also id.* ("The fact that the Government has not compelled a private party to perform a search does not, by itself, establish that the search is a private one.").

115. *Id.*

116. *Id.*

117. *See* United States v. Jacobsen, 466 U.S. 109, 122 (1984) (determining whether the Federal Express employees "exceeded the scope of the private search" such that it was subject to Fourth Amendment protection); Walter v. United States, 447 U.S. 649, 657 (1980) (concluding that government agents exceeded the scope of the prior private search and that therefore the Fourth Amendment applied).

118. 466 U.S. 109 (1984).

119. *Id.* at 113 (quoting *Walter*, 447 U.S. at 662 (Blackmun, J., dissenting)).

120. United States v. D'Andrea, 648 F.3d 1, 10 (1st Cir. 2011) (citing United States v. Momoh, 427 F.3d 137, 140–41 (1st Cir. 2005)).

121. United States v. Reed, 15 F.3d 928, 931 (9th Cir. 1994) (citation omitted).

a later decision, *United States v. Jarrett*,[122] the Fourth Circuit agreed that these are the "two primary factors" in assessing whether a search is governmental,[123] and elaborated that "simple acquiescence by the Government does not suffice to transform a private search into a Government search. Rather, there must be some evidence of Government participation in or affirmative encouragement of the private search before a court will hold it unconstitutional. Passive acceptance by the Government is not enough."[124]

Applying the test in *Jarrett*, the Fourth Circuit addressed whether an anonymous computer hacker ("Unknownuser"), determined to identify consumers of child pornography and provide related incriminating information to police, was a private actor.[125] The *Jarrett* court found that the second part of the test was satisfied because the government conceded that the hacker was motivated by a desire to help law enforcement.[126] However, the first factor—whether the government knew of and acquiesced in the search—was not satisfied.[127] This was so even though several months earlier, after the hacker provided information in a different child pornography case, an agent engaged in an extensive email exchange with the hacker, with the agent relating that "[i]f you want to bring other information forward, I am available."[128] The Court reasoned that if it were

> to allow the . . . [agent's] communications to effect such an agency relationship, virtually any Government expression of gratitude for assistance well prior to an investigation would effectively transform any subsequent private search by the party into a Government search. We find no support for such a position in the existing case law, and we decline to extend the protections of the Fourth Amendment to embrace it.[129]

"Although the Government operated close to the line in this case," the Court wrote, "it did not . . . demonstrate the requisite level of knowledge and acquiescence sufficient to make Unknownuser a Government agent when he hacked into Jarrett's computer."[130] "In order to run afoul of the Fourth Amendment, therefore, the Government must do more than passively accept

---

122. 338 F.3d 339 (4th Cir. 2003).

123. *Id.* at 344.

124. *Id.* at 345–46.

125. *Id.* at 340–41.

126. *Id.* at 345; *see also id.* (stating that the "motivation for conducting the illicit searches stemmed solely from his interest in assisting law enforcement authorities"). Indeed, the hacker had previously provided information in another case. *See id.* at 341–43 (citing and discussing United States v. Steiger, 318 F.3d 1039, 1045 (11th Cir. 2003)).

127. *Jarrett*, 338 F.3d at 347.

128. *Id.* at 341. The Court also characterized interactions after the hacker's search of Jarrett's computer as "what can only be characterized as the proverbial 'wink and a nod.'" *Id.* at 343.

129. *Id.* at 346–47 (footnote omitted).

130. *Id.* at 347.

or acquiesce in a private party's search efforts. Rather, there must be some degree of Government participation in the private search."[131] Concluding, the Court stated:

> At the end of the day, in order to bring Unknownuser within the grasp of an agency relationship, Jarrett would have to show that the Government made more explicit representations and assurances . . . that it was interested in furthering its relationship with Unknownuser and availing itself of the fruits of any information that Unknownuser obtained. Although evidence of such "encouragement" would not have to target a particular individual, it would have to signal affirmatively that the Government would be a ready and willing participant in an illegal search.[132]

The outcome in *Jarrett* highlights the restrictive nature of the agent or instrumentality test. What of the test's application in the crowdsourcing context? The answer is that, if anything, the test is overinclusive.

With respect to the first prong, the Court in *Skinner* held that a party challenging a search need not establish that the government was the moving force of the search; it only need be shown that there is a "clear indic[ation] of the Government's encouragement, endorsement, and participation."[133] As the many examples of crowdsourcing noted earlier make clear, the police are often the moving force, and certainly "encourage[]," "endorse[]," and "participat[e]" in the public's investigative efforts.[134]

The second prong asks whether the private actor was motivated to help police, or rather had a personal, non-law-enforcement motivation. In *Coolidge*, for instance, the Court found that the defendant's wife provided police incriminating information because she believed it would exonerate, not inculpate, her husband.[135] In the case law to date, outside the crowdsourcing context, the motivation prong has proven to be as much, if not more, an obstacle to satisfying the agent or instrumentality test. Courts typically conclude that a search is private if any non-law-enforcement motivation is evidenced. As the Eighth Circuit put it in one case, "[t]hat a private citizen is motivated in part by a desire to aid law enforcement does

131. *Id.* at 344.

132. *Id.* at 347.

133. Skinner v. Ry. Lab. Exec. Ass'n, 489 U.S. 602, 615–16 (9th Cir. 1989); *see also id.* at 615 (explaining that a search is public if "the Government did more than adopt a passive position toward the underlying private conduct"); *see also, e.g.*, United States v. Smythe, 84 F.3d 1240, 1243 (10th Cir. 1996) (stating that "the government . . . must . . . affirmatively encourage, initiate or instigate the private action," or put otherwise, the question turns on whether "the government coerces, dominates or directs the actions of a private person" (citations omitted)).

134. *See supra* notes 36–38, 62–66 and accompanying text.

135. Coolidge v. New Hampshire, 403 U.S. 443, 489–90 (1971).

not in and of itself transform her into a government agent."[136] As a consequence, a search is private if partially motivated to avoid criminal liability[137] or to protect customers.[138] Some courts hold that a search is public only if it "aims primarily" to help the government,[139] and it is not always sufficient that an individual's "motive to aid law enforcement preponderates."[140]

With crowdsourcing, the motivation question is complicated by the fact that the information challenged is possibly the result of multiple individual efforts.[141] However, while at times perhaps motivated in part by a desire to secure internet fame and glory and the like, assisting police in closing cases appears to be the prime motivator of crowdsourcers.[142]

III. The Way Forward

The Supreme Court should, and perhaps soon will, consider revamping the private search doctrine in light of the role played by companies in

136. United States v. Smith, 383 F.3d 700, 705 (8th Cir. 2004); *see also* United States v. Koenig, 856 F.2d 843, 851 (7th Cir. 1988) ("[I]t should come as no surprise when the goals of private individuals or organizations coincide with those of the government. However, this happy coincidence does not make a private actor an arm of the government."). *But see* United States v. Bowers, 594 F.3d 522, 526 (6th Cir. 2010) (holding that for a search to be private, "the intent of the private party conducting the search . . . [must be] entirely independent of the government's intent to collect evidence for use in a criminal prosecution" (quoting United States v. Hardin, 539 F.3d 404, 418 (6th Cir. 2008))).

137. *See* United States v. Aldridge, 642 F.3d 537, 541–42 (7th Cir. 2011) (holding that an employee's actions in providing incriminating records to the SEC after being told "to keep a lookout for suspicious materials" were private because she "had a number of reasons why it was in her personal interest to help the government investigate" the corporation, including a desire "to exonerate herself"); United States v. Huber, 404 F.3d 1047, 1054 (8th Cir. 2005) (holding that even if a bookkeeper was "motivated, to some extent, by an urge to help the government, . . . [that] is not enough to make her a government agent" in the absence of instigation by law enforcement (citations omitted)); State v. Cohen, 409 S.E.2d 383, 386 (S.C. 1991) (holding that a UPS search of a package was private, despite earlier police request for assistance, because UPS "was not motivated to assist law enforcement . . . but appears to have been motivated by a concern that it was delivering contraband").

138. *See, e.g.*, United States v. Pervaz, 118 F.3d 1, 3, 6 (1st Cir. 1997) (holding that, where a secret service agent advised employees of a cellular phone company that the company's customers were being defrauded and asked if they had equipment to locate the source of cloned calls, the company's later use of such equipment was not a government search, as the company "had a legitimate independent motivation for its search: to prevent a fraud from being perpetrated on its customers").

139. *See, e.g.*, *id.* at 6 (noting that to determine whether a search is truly private a court must consider "the extent to which the private party aims primarily to help the government or to serve its own interests").

140. United States v. Leffall, 82 F.3d 343, 347 (10th Cir. 1996).

141. For an informative discussion of the difficulty of identifying motive, across different legal areas, and the tests employed by courts, including that focusing on "primary motive," see Andrew Verstein, *The Jurisprudence of Mixed Motives*, 127 YALE L. J. 1106, 1134–36 (2018).

142. *See, e.g.*, Huey et al., *supra* note 33, at 87–89 (discussing the results of a survey of motivations among those engaged in "online civilian policing").

providing data to law enforcement, as scholars have urged.[143] The Court's recent landmark decision in *Carpenter v. United States*,[144] which eschewed reliance on the third-party doctrine and required that police obtain a search warrant when securing geolocational information from private parties (cell phone companies),[145] provides hope that this will occur.

Because crowdsourcing is still taking shape, there is less reason to think that the Court will address its Fourth Amendment ramifications any time soon. If and when the Court does so, advocates will have a strong basis to argue that, as with the close relationship between private data companies and police,[146] existing doctrine is ill-suited to the internet age. However, the argument will not be based on underinclusiveness—it will be that the private search doctrine, as a taxonomic matter, can be overinclusive.

One option, gamely advanced several decades ago regarding "police bulletins," would be to take a causation-based approach: that "[w]hen a [police] bulletin can reasonably be expected to induce a private citizen to act on behalf of the police, his acts should fall within the purview of the [F]ourth and [F]ourteenth [A]mendments."[147] The author elaborated:

> Thus a bulletin requesting a private party to inform the police whenever he may come across criminal activity would not make the recipient a police agent when relaying information he would have gathered in the absence of the bulletin. But when the bulletin requests the private party to do something beyond the scope of his normal duties or activities (for example, to detain or open a particular trunk scheduled for a particular flight), or when such unusual activity is induced because of the bulletin, then the additional action may be treated as state action.[148]

---

143. *See supra* notes 12–14 and accompanying text; *cf.* Wayne A. Logan, *Dirty Silver Platters: The Enduring Challenge of Intergovernmental Investigative Illegality*, 99 IOWA L. REV. 293, 295–98 (2013) (discussing the Supreme Court's decades-long effort to identify and regulate impermissible "working arrangements" between state and federal agents, in a time when the exclusionary rule only regulated the latter).

144. 138 S. Ct. 2206 (2018).

145. *Id.* at 2220; *see also* Wayne A. Logan & Jake Linford, *Contracting for Fourth Amendment Privacy Online*, 104 MINN. L. REV. 101, 113–14 (2019) (discussing *Carpenter*'s analysis of whether the police activity constituted a search, including the majority's refusal to resolve the case on the basis of the third-party doctrine).

146. *See, e.g.*, Brennan-Marquez, *supra* note 11, at 488–89 (critiquing the "agent or instrument" agency test as being too limited when assessing the role of private companies providing surveillance information to police, and urging instead a test asking whether the assistance extends the "law enforcement infrastructure into the private sphere" (emphasis omitted)).

147. Comment, *Police Bulletins and Private Searches*, 119 U. PA. L. REV. 163, 173 (1970).

148. *Id.* at 167; *see also id.* at 168 ("The test, then, is essentially one of causation: but for the bulletin (or police request in any form), the private activity would not have occurred."). For advocacy of a similar but-for causation approach, see Anthony G. Scheer, Note, *A Search by Any Other Name: Fourth Amendment Implications of a Private Citizen's Actions in* State v. Sanders, 69 N.C. L. REV. 1449, 1465–66 (1991).

Such an approach raises obvious overinclusiveness concerns. As an initial matter, we can reasonably expect that police issue requests for assistance hoping and expecting that community members will take action and lend assistance.[149] At the same time, tying the determination to whether a person engages in behavior beyond the "scope of his normal duties or activities" would prove problematic in application. Should the test be satisfied, for instance, when police encourage community members to be watchful of suspicious activity, and a resident, as a rule not civic-minded, thereafter reports an individual he believes is reconnoitering a neighbor's home? Likely not, based on both constitutional doctrine and reasonable societal interests in crime prevention and detection.[150]

An alternative might lie in a more robust version of the current private search doctrine, such as employed by the First Circuit Court of Appeals. In *United States v. D'Andrea*, the court, as noted earlier, stated that whether the behavior in question is public depends on "[1] the extent of the government's role in instigating or participating in the search, [2] its intent and the degree of control it exercises over the search and the private party, and [3] the extent to which the private party aims primarily to help the government or to serve its own interests."[151]

The key distinguishing feature of this more robust test would be the more demanding nature of the second prong—the degree of control the police exercise over the investigative effort and the private party.[152] When police shape, direct, and control a crowdsourcing investigative effort, especially regarding specific tasks, the undertaking should be deemed public.[153] Otherwise, as then-Judge Neil Gorsuch wrote when sitting on the Tenth Circuit Court of Appeals, "[W]hat would have been the point of the [Fourth] Amendment if the government could have instantly rendered it a dead letter by the simple expedient of delegating to agents investigative work it was forbidden from undertaking . . . ?"[154]

149. *Cf.* California v. Hodari D., 499 U.S. 621, 627 (1991) (reasoning that the police do not issue orders to criminal suspects in the belief that they will be ignored).

150. *See, e.g.*, Georgia v. Randolph, 547 U.S. 103, 115–16 (2006) (noting that when citizens provide incriminating information to police, they serve the societal interest in "bringing criminal activity to light").

151. United States v. D'Andrea, 648 F.3d 1, 10 (1st Cir. 2011) (citing United States v. Momoh, 427 F.3d 137, 141 (1st Cir. 2005)).

152. *Id.* at 10.

153. Courts face a similar line-drawing challenge in determining whether a private party, acting undercover, is a government agent for purposes of the Sixth Amendment right to counsel. *See* State v. Marshall, 882 N.W.2d 68, 91–95 (Iowa 2016) (surveying the approaches that fall along a continuum of government involvement and degree of direction).

154. United States v. Ackerman, 831 F.3d 1292, 1300 (10th Cir. 2016) (Gorsuch, J.).

Applying the more robust test is also supported by what has become the singular purpose of the exclusionary rule: deterrence.[155] The Supreme Court has stated that the exclusionary rule should apply only to public actors because it will not deter private individuals.[156] A similar rationale undergirds reluctance to apply the rule to privately employed police and security guards. As one commentator remarked:

> Whether or not the evidence gathered by private security forces is admissible in the public courts might not matter much to the private police, nor to the individuals, organizations, and companies that hire them, nor even to the suspects that the private police apprehend. This is because as often as not, those who employ private police decide to opt out of the public criminal justice system altogether and merely take their own private action against the alleged perpetrator.[157]

The crowdsourcing public, however, typically operates under a different incentive structure, hoping that a criminal suspect, who they helped identify and apprehend,[158] will be held to account in the criminal justice system.[159] And police, mindful of crossing the crowdsourcing public–private line, would be loath to overstep its parameters, lest they jeopardize their criminal cases.[160]

---

155. *See* Davis v. United States, 564 U.S. 229, 236–37 (2011) ("The rule's sole purpose, we have repeatedly held, is to deter future Fourth Amendment violations.").

156. United States v. Janis, 428 U.S. 433, 456 n.31 (1976) ("[T]he exclusionary rule, as a deterrent sanction, is not applicable where a private party . . . commits the offending act.").

157. Ric Simmons, *Private Criminal Justice*, 42 WAKE FOREST L. REV. 911, 931 (2007) (footnotes omitted); *cf.* John Rappaport, *Criminal Justice, Inc.*, 118 COLUM. L. REV. 2251, 2251 (2018) (describing the phenomenon of retailers employing a private, for-profit system to settle store-related criminal disputes, and discussing the incentives behind their doing so).

158. *See, e.g., supra* notes 40–42, 92–94 and accompanying text. In line with conventional thinking, Professor LaFave reasons that the exclusionary rule will "not likely deter the private searcher, who is often motivated by reasons independent of a desire to secure criminal conviction and who seldom engages in searches upon a sufficiently regular basis to be affected by the exclusionary sanction." 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.8(a), at 361 (5th ed. 2012). As discussed, crowdsourcers do get involved to secure convictions and often are repeat players.

159. Retaining the third prong of the test—that the private actor be motivated to help police—is important in this deterrence-related respect. However, a sound argument exists in favor of jettisoning the criterion altogether, as the Hawaii Supreme Court did in *State v. Kahoonei*, 925 P.2d 294 (Haw. 1996), which held that the motivation of a private party is irrelevant because "a private individual's subjective motivation would not address the fundamental concern of either the [F]ourth [A]mendment . . . or . . . the Hawai'i Constitution, that is, to curb unconstitutional activity by *government* agents." *Id.* at 300 (emphasis in original). In short, the focus should instead be on the motivation and action of government agents. *Id.* at 300–02; *see also* Coolidge v. New Hampshire, 403 U.S. 443, 486–89 (1971) (assessing whether a private party was a state actor and attaching importance to whether police were seeking to control or direct her conduct).

160. Of course, not all crowdsourcing efforts will entail a search or seizure, at least as presently understood, for instance because the information in question is deemed "public" in nature. *See* Logan & Linford, *supra* note 145, at 108–17 (discussing Supreme Court doctrine concerning what qualifies as a "search" under *Katz v. United States*, 389 U.S. 347 (1967), and its progeny).

Modifying the private search doctrine in the way recommended will go a long way toward preventing police from using crowdsourcing as a way to evade Fourth Amendment protections and application of the exclusionary rule. Absent a willingness by the Court to extend formal Fourth Amendment coverage, hope might lie in rulemaking,[161] whereby administrative entities impose limits on police (in this instance, what they can and should ask of crowdsourcers),[162] as we are now seeing with the use of CCTV cameras, facial recognition technology, and drones.[163]

Time will tell whether any of these regulatory possibilities come to fruition, but it is hoped that the discussion here highlights the need for courts and policymakers to act.

Conclusion

Almost forty years ago, Professor John Burkoff accurately observed that "[t]he traditional treatment of all private searches as a separate and distinct activity untainted by 'state involvement' is more an exercise in semantics than a sound application of precedent, and it does not adequately account for contemporary policing practices."[164] What was true then is surely true now, as private businesses have come to play an ever more prominent role in amassing data on individuals and providing it to law enforcement.[165] Aggravating matters, courts have been reluctant to subject private police and security forces, which today significantly outnumber sworn public police,[166] to constitutional regulation and accountability.[167]

This Essay joins this chorus of criticism. However, it advances another claim: that current doctrine, applied to crowdsourcing, is not underinclusive,

---

161. *See generally* Maria Ponomarenko, *Rethinking Police Rulemaking*, 114 NW. U. L. REV. 1 (2019) (advocating for the use of regulatory intermediaries to help regulate the police). *But see* Wayne A. Logan, *Fourth Amendment Localism*, 93 IND. L. J. 369, 386–91 (2018) (noting the risks, such as capture and lack of expertise, associated with relying on local administrative rulemaking processes); Ira S. Rubinstein, *Privacy Localism*, 93 WASH. L. REV. 1961, 2005–06 (2018) (discussing the role played by the New York City Police Department in stalling city council action regarding a 2017 law designed to oversee police use of new surveillance technology).

162. We are now seeing departments doing this themselves in some localities, which can serve as a starting point. *See supra* note 83 and accompanying text.

163. Ponomarenko, *supra* note 161, at 39–40 (citing examples).

164. John M. Burkoff, *Not So Private Searches and the Constitution*, 66 CORNELL L. REV. 627, 627–28 (1981).

165. *See supra* notes 10–11 and accompanying text.

166. *See* Etzioni, *supra* note 11, at 294–95 (noting the massively greater number of private police and security guards in the U.S. compared to sworn public law enforcement); Stoughton, *supra* note 4, at 127–41 (delineating the categories of "private" police, "semi-public private" police, "semi-private public" police, and the activities they undertake, excepted from regulation).

167. Etzioni, *supra* note 11, at 298–303 (noting that private police are not subject to Fourth Amendment regulation, under the exclusionary rule and federal civil rights law, and otherwise evade public accountability mechanisms).

but rather is overinclusive, so much so that its strict application would result in most all crowdsourcing efforts being classified as public. Such an outcome would be unfortunate because public safety can certainly benefit from crowdsourcing,[168] given its promise as an investigative force multiplier for governments. Criminal investigations, however, are not like other crowdsourcing endeavors like selecting a restaurant for an evening meal based on Yelp reviews, or devising a new corporate insignia based on respondents' preferences. Rather, they have major importance for the lives of individuals singled out by the crowd and the health of civil society more generally.

Crowdsourcing crime control, like the internet, social media, and technological advances more generally on which it predominantly relies, is not going away; if anything, it will proliferate in the years to come. The challenge lies in harnessing its potential, while protecting against the significant harms that can and will result should it go unregulated. This Essay, it is hoped, has identified these risks and benefits and charted a course for this regulation to occur.

168. *See* Daren C. Brabham, *Crowdsourcing as a Model for Problem Solving: An Introduction and Cases*, 14 CONVERGENCE: INT'L J. RES. INTO NEW MEDIA TECHS. 75, 87 (2008) ("Crowdsourcing is not just another buzzword, not another meme. . . . It is a model capable of aggregating talent, leveraging ingenuity while reducing the costs and time formerly needed to solve problems.").