LOOK UP AND SMILE FOR DADDY WARBUCKS'S SURVEILLANCE PLANE: REFORMING THE STANDARD FOR DETERMINING WHEN A PRIVATE SEARCH CONSTITUTES GOVERNMENT ACTION, AND WHY IT'S NEEDED TO MEET THE GROWING FOURTH AMENDMENT PROBLEM OF PRIVATIZED SURVEILLANCE

Lucius T. Outlaw III[*]

2021. MICH. ST. L. REV. 861

* Associate Professor & Supervising Attorney (Criminal Justice Clinic), Howard University School of Law (HUSL). This Article was made possible by financial support provided by HUSL. My thanks to the editors of the *Michigan State Law Review* for their invaluable support and contributions. A special thanks to my NPWD family (Sydney Briggs, Albert Smith, David Derryck, Erica Terry Derryck, and Kyla Kupferstein Torres) for their support, inspiration, and friendship.

INTRODUCTION

Sometime in 2015, the Baltimore Police Department (BPD) struck a secret three-way partnership to subject its city to continuous aerial surveillance by a private company.[1] Under the hush-hush partnership, Ohio-based Persistent Surveillance Systems (PSS) regularly flew a small plane equipped with high-powered cameras over Baltimore for months to capture and store hundreds of hours of footage that was analyzed by PSS's employees and contractors for

1. *See* Monte Reel, *Secret Cameras Record Baltimore's Every Move from Above*, BLOOMBERG BUSINESSWEEK (Aug. 23, 2016), https://www.bloomberg.com/features/2016-baltimore-secret-surveillance [https://perma.cc/S94N-J5WX].

information and leads to assist BPD investigations.[2] The effort was funded by the third party to the partnership—a wealthy married couple in Texas (Laura and John Arnold), who had taken an interest in PSS after hearing about the company and its aerial surveillance system on the radio.[3] The money ($360,000) the Arnolds donated for the effort was funneled through the Baltimore Community Foundation, a nonprofit organization that administers donations to a range of civic causes in the city.[4] BPD was able to keep the partnership and the resulting surveillance a secret from the Baltimore city council, the city's mayor, and the public because the project was funded by a private third party and not the city treasury.[5] Once the secret surveillance program was launched, the PSS plane that circled Baltimore recorded 100 hours of surveillance video between January and February 2016, and another 200 hours between June and August of that year.[6]

The secrecy came to an abrupt end on April 23, 2016, when *Bloomberg Businessweek* published an expose on PSS and its agreement with BPD.[7] The various reactions were largely predictable by source.[8] The BPD claimed that there was no conspiracy to keep the program secret and that the department was simply testing a promising crime investigation tool.[9] Local elected officials and politicians complained about being kept in the dark about the program, while simultaneously hedging their response to the program.[10] The public's reaction was mixed, with many members of the Baltimore City community expressing outrage at the secrecy surrounding the program and being subjected to continuous aerial surveillance, while others

2. *See id.*
3. *See id.*
4. *See id.*; *see also* Doug Donovan, *Donor to Baltimore Police Surveillance Program Calls Privacy Debate 'Healthy,'* WASH. POST (Aug. 31, 2016), https://www.washingtonpost.com/local/public-safety/donor-to-baltimore-police-surveillance-program-calls-privacy-debate-healthy/2016/08/31/b07b92ee-6fc8-11e6-8533-6b0b0ded0253_story.html [https://perma.cc/CNW8-MUMV].
5. *See* Reel, *supra* note 1; Donovan, *supra* note 4; *see also* Kevin Rector & Luke Broadwater, *Report of Secret Aerial Surveillance by Baltimore Police Prompts Questions, Outrage*, BALT. SUN (Aug. 24, 2016), https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-secret-surveillance-20160824-story.html [https://perma.cc/ZVX9-7H8X].
6. *See* Rector & Broadwater, *supra* note 5.
7. *See* Reel, *supra* note 1.
8. *See id.*
9. *See* Rector & Broadwater, *supra* note 5.
10. *See id.*

voiced support for the effort to address the city's spiking crime and violence.[11]

The public and political outcry led to the grounding of PSS's plane—temporarily.[12] Nearly four years later, the city's government approved a six-month pilot program that put three PSS surveillance planes back in the air above Baltimore with the $3.6 million price tag picked up by the Arnolds.[13] The approval came after a lawsuit filed by Baltimore residents, assisted by the American Civil Liberties Union, seeking a preliminary injunction preventing the surveillance flights was rejected by a Maryland federal judge, a decision that was initially backed by the Fourth Circuit.[14] However, in June 2021, the Fourth Circuit (en banc) reversed and remanded the district court's decision, holding that "[b]ecause the [aerial surveillance] program enables police to deduce from the whole of individuals' movements, . . . accessing its data is a search, and its warrantless operation violates the Fourth Amendment."[15]

The legal controversy and conflict over the PSS program in Baltimore centered on whether the program's aerial surveillance violated the Fourth Amendment rights of Baltimore's residents because it infringes on their privacy and constitutes warrantless and

---

11. *See id.*

12. *See* Luke Broadwater, *A Group is Trying to Get the Grounded Baltimore Police Surveillance Airplane Flying Again. The Pitch: It Can Catch Corrupt Cops*, BALT. SUN (Feb. 22, 2018), https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-police-plane-20180220-story.html [https://perma.cc/KNQ4-TNZ9].

13. *See* Emily Opilo, *Baltimore Spending Board Approves Surveillance Plane Pilot Program to Capture Images From City Streets*, BALT. SUN (Apr. 1, 2020), https://www.baltimoresun.com/news/crime/bs-md-ci-baltimore-surveillance-plane-approved-20200401-sskjob7dgrevpjfyygrlgitnqi-story.html [https://perma.cc/HP44-FHAU]; MICHAEL S. HARRISON, BALT. POLICE DEP'T, PROFESSIONAL SERVICE AGREEMENT ACCEPTANCE (2020).

14. *See* Tim Prudente, *Controversial Baltimore Police Surveillance Planes Will Take Flight Next Week, Police Say, Following Judge's Ruling*, BALT. SUN (Apr. 24, 2020), https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-police-spy-plane-lawsuit-20200424-2ncxogcqr5akjjfd2fvaotvnby-story.html [https://perma.cc/7FJH-VWQ9]; *see also* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 979 F.3d 219, 222 (4th Cir. 2020).

15. *See* Leaders of a Beautiful Struggle v. Balt. Police Dep't, No. 20-1495, 2021 U.S. App. LEXIS 18868, at *28 (4th Cir. June 24, 2021) (en banc); *see also* Tim Prudente, *Federal Appeals Court Rebukes Baltimore Spy Plane Program, Likely Blocks Access to Cache of Remaining Footage*, BALT. SUN (June 26, 2021), https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-cr-spy-plane-decision-20210624-avfotbqo5zdwjfutok3oz6hno4-story.html [https://perma.cc/H928-XE4Z].

indiscriminate government searches of Baltimore's residents without any individualized suspicion, probable cause, or judicial approval.[16] In this context, much has been written and argued about whether the program's aerial surveillance is a search under the Fourth Amendment and if it impedes on Baltimoreans' privacy rights.[17] The district court held that the program was not a search, but the Fourth Circuit disagreed.[18] In a stinging rebuke of the program, Fourth Circuit Chief Judge Roger Gregory proclaimed that "[a]llowing the police to wield this power unchecked is anathema to the values enshrined in our Fourth Amendment."[19]

What has received little to no discussion is whether the *private* funding of the aerial surveillance program and the execution of the program by a *private* company (i.e., PSS) affects the Fourth Amendment analysis, and if it should. The lack of discussion is likely because BPD and PSS entered into a formal contract, which arguably eliminated any dispute that the surveillance program is state action reached by the Fourth Amendment.[20] However, PSS's aerial surveillance program in Baltimore offers a glimpse into the quickly disappearing line between private surveillance and state surveillance and the Fourth Amendment implications of this evolution.

As every first-year law student learns, the Fourth Amendment's guarantee against unreasonable searches and seizures applies only to government action and not private conduct.[21] To delineate private search and seizure conduct from government conduct of the same, courts currently use standards modeled in, what Professor Brennan-Marquez has labeled, the "deputization framework" of the Fourth

16. *See* Complaint for Declaratory and Injunctive Relief at 19–20, Leaders of a Beautiful Struggle v. Balt. Police Dep't, 456 F. Supp. 3d 699 (D. Md. 2020) (No. 20-929); *see generally Leaders of a Beautiful Struggle*, 2021 U.S. App. LEXIS 18868.

17. *See Leaders of a Beautiful Struggle*, 2021 U.S. App. LEXIS 18868, at *11–20; *see also* Balt. Police Dep't & Police Comm'r Michael S. Harrison's Response in Opposition to Motion for Preliminary Injunction at 11–21, Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 456 F. Supp. 3d 699 (D. Md. 2020) (Civil Action No. 20-929); Prudente, *supra* note 14.

18. *See Leaders of a Beautiful Struggle*, 2021 U.S. App. LEXIS 18868, at *17.

19. *See id.* at 30.

20. *See* HARRISON, *supra* note 13.

21. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984) (noting "[the] Court has [] consistently construed [Fourth Amendment] protection as proscribing only governmental action" and not private searches by actors who are not acting as agents of the government).

Amendment.[22] In short, under the deputization framework a private search or seizure is reached by the Fourth Amendment only if the private searcher was "deputized" into acting as an agent or instrument of the government.[23]

There is a copious amount of scholarship that explores the private search limitation of the Fourth Amendment. There is also an abundance of scholarship focusing on the Fourth Amendment and the rise of the "surveillance-industrial Internet complex"[24] and "surveillance intermediaries"[25]—i.e., private third parties (e.g., Google, Facebook, Apple, cellphone service providers) who collect private information and data for their own business purposes (such as cellphone records, cellphone location data, social media data, internet search and use histories) that the government wants to obtain for its investigative and prosecution purposes.[26] This area of scholarship examines the implications and ramifications of the government obtaining (through consent, cooperation, or compulsion) personal information and data from "big tech" companies, and whether the "third party doctrine" that has historically been the government access lane to such data, needs to be reformed or abandoned.[27]

There has been less scholarship proposing new standards for determining when a private search is reached by the Fourth Amendment, particularly one that reaches searches by big tech, and

---

22. *See* Kiel Brennan-Marquez, *The Constitutional Limits of Private Surveillance*, 66 U. KAN. L. REV. 485, 488–89, 499–505 (2018).

23. *See id.* at 488.

24. *See* Christine Fuchs, *Surveillance and Critical Theory*, MEDIA & COMM., 2015, at 6, 6–7.

25. *See* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 99–100 (2018).

26. *See, e.g.*, Brennan-Marquez, *supra* note 22, at 486–87; Avidan Y. Cover, *Corporate Avatars and the Erosion of the Populist Fourth Amendment*, 100 IOWA L. REV. 1441, 1445 (2015); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1311 (2012); Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 8 (2008).

27. *See, e.g.*, Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 n.5 (2009) (identifying some of the key scholarship focused on the doctrine). Third party doctrine was firmly established by the Supreme Court in *United States v. Miller*, 425 U.S. 435, 446 (1976) (holding that the Fourth Amendment was not violated when the defendant's bank turned over the defendant's bank records in response to a government subpoena). The doctrine as summarized by the Court:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in a third party will not be betrayed.

Id. at 443.

searches by other concerning types of private searchers (discussed later): extremists, private militias, and private security guards.[28] It's a topic that desperately needs robust exploration and discussion. The line between government and private surveillance is increasingly blurry, if not disappearing.[29] Private citizens and companies are steadily becoming a principal provider of surveillance information and data to law enforcement.[30] This movement has significant Fourth Amendment implications that need to be explored, including how it is erasing the line between private and government surveillance, and how this erasure begs for new approaches and doctrines to reinforce and protect the Fourth Amendment's guarantee against government intrusions into our person, property, and private space.

Two works of scholarships in particular have filled the void to date and have heavily influenced this Article. The first is University of Pittsburgh School of Law Professor John Burkoff's seminal *Not So Private Searches and the Constitution*, which diligently argues for expanding the exclusionary rule to evidence collected by private actors using unlawful and unconstitutional means.[31] The second and more recent scholarly work is University of Connecticut School of Law Professor Keil Brennan-Marquez's *The Constitutional Limits of Private Surveillance*, which discusses how the current standard for addressing Fourth Amendment-based challenges to private searches is outdated, and proposes an "extended infrastructure" theory of extending Fourth Amendment protections to private surveillance.[32]

This Article not only relies heavily on Professors Burkoff's and Brennan-Marquez's scholarship, but seeks to build upon both to spark a much-needed conversation about how current Fourth Amendment jurisprudence fails to fully protect us from "unreasonable searches and seizures" done by private actors to benefit the government's crime enforcement and prosecution efforts.[33] While Professor Burkoff's article persuasively pushes for extending the exclusionary rule to private searches, he does not offer a uniform standard for measuring when a private search is reached by the Fourth Amendment.[34] Professor Brennan-Marquez does suggest a four-element structure for

28. *See infra* Sections IV.A, IV.B.
29. *See* Balkin, *supra* note 26, at 7.
30. *See id.*
31. *See* John M. Burkoff, *Not So Private Searches and the Constitution*, 66 CORNELL L. REV. 627, 627 (1981).
32. *See* Brennan-Marquez, *supra* note 22, at 488–89.
33. *See* U.S. CONST. amend. IV.
34. *See* Burkoff, *supra* note 31, at 627.

implementing his extended infrastructure theory, but he stops short of offering a deep analysis of the proposed elements and how they would operate in practice.[35]

This Article picks up where these scholarly works end by offering a new standard—the expanded deputization framework—for determining when private searches are reached by the Fourth Amendment.[36] The proposed expanded deputization framework builds on the existing deputization framework by adding factors that appreciate the evolving nature and sources of private searches and private searchers, in particular big tech companies, extremists, and private militias.[37]

This Article is comprised of five main parts. Parts I and II discuss the growth of privatized surveillance and its accompanying harms and dangers.[38] Parts III and IV explore the current deputization framework.[39] Part V explains, explores, and critiques the proposed expanded deputization standard and addresses expected criticisms of it.[40] In Part V, the expanded deputization standard is applied to a case that was decided using the existing deputization framework standard to see if a different outcome would result.[41]

I. PRIVATIZATION OF SURVEILLANCE TODAY

As with most things, the privatization of surveillance exists on a spectrum. On one far end are the private actors, such as PSS, who conduct surveillance solely to assist law enforcement.[42] While monetary profit is the ultimate end goal for these actors, their method for achieving it is to replace, supplement, or fill a void of government

35. *See* Brennan-Marquez, *supra* note 31, at 517 ("To summarize, then—the question of whether law enforcement infrastructure has been extended involves (at least) four elements: first, whether data-sharing is repeated or, instead, spontaneous; second, whether the data-transfer was aimed to assist law enforcement; third, how powerfully-equipped the private actor is to perform data surveillance; and fourth, whether law enforcement practice has evolved to reflect the availability of privately-collected data.").

36. *See infra* Part V.

37. *See infra* Part V.

38. *See infra* Parts I and II.

39. *See infra* Parts III and IV.

40. *See infra* Part V.

41. *See infra* Part V.

42. *See, e.g.*, *Markets*, PSS, https://www.pss-1.com/markets [https://perma.cc/UU83-LC58] (last visited Oct. 25, 2021).

surveillance.[43] For these actors, the business purpose and the government purpose are the same—finding, obtaining, and collecting data and information that can further government investigations and prosecutions.[44]

On the other end are the corporate actors, such as Google, Apple, Facebook, AT&T, and other cellphone service providers, who are the founders and vanguards of what Harvard Business School Professor Shoshana Zuboff has dubbed "surveillance capitalism."[45] In their effort to gain "unrivaled dominance" over digitized information, these surveillance capitalists have "built . . . the world's largest computer networks, data centers, populations of servers, undersea transmission cables, advanced microchips, and frontier machine intelligence."[46] To obtain the vast volumes of data needed to meet their goals, the surveillance capitalists offer gaslighting declarations of privacy, while secretly (or not so secretly) collecting and using user data for undisclosed purposes, sharing user data with corporate allies (e.g., cellphone application developers) and the government, and monetizing user data (e.g., selling user data to other companies).[47] Such gaslighting is exemplified by Facebook founder and leader Mark Zuckerberg's declaration during a company conference on April 30, 2019, that "[t]he future is private,"[48] while in federal court months later, the company declared in a privacy intrusion lawsuit that "[n]or does Facebook's collection and use of [Facebook users'] IP addresses to estimate user locations violate any reasonable expectation of privacy."[49] According to Facebook, collecting user IP addresses and

---

43. *See, e.g.*, *History*, PSS, https://www.pss-1.com/history [https://perma.cc/RM3Y-YJ6J] (last visited Oct. 25, 2021).

44. *See, e.g.*, *Privacy & Legality*, PSS, https://www.pss-1.com/copy-of-in-the-community [https://perma.cc/PN36-V6QE] (last visited Oct. 25, 2021) (noting that PSS data is used in the investigation of various crimes, including, *inter alia*, murder, rape, burglary, and drug offenses).

45. Shoshana Zuboff, *You are Now Remotely Controlled*, N.Y. TIMES (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html [https://perma.cc/JZR5-9PNB].

46. *Id.*

47. *See id.*

48. *Id.*; *see also* Issie Lapowsky, *Here's How Mark Zuckerberg Sees Facebook's New Era of Privacy*, WIRED (Apr. 30, 2019, 4:32 PM), https://www.wired.com/story/f8-zuckerberg-future-is-private/ [https://perma.cc/YP8B-P7GQ] (noting that at the same time Facebook outwardly embraced privacy at the April 30, 2019 conference, Facebook was already testing new products that had the potential to collect even more data about its users).

49. *See* Lapowsky, *supra* note 48; Notice of Motion and Motion to Dismiss First Amended Complaint; Memorandum of Points and Authorities in Support

using that data to estimate user location is "routine commercial behavior."[50] Facebook went as far to claim that there was no privacy interest even when a user takes affirmative steps to keep their IP address and location secret because "Facebook never represented that it would stop collecting or using IP addresses when Location Services or Location History was off."[51] These arguments are hard to reconcile with Zuckerberg's public comments that Facebook would be at the forefront of a new era of safeguarding privacy.[52]

Facebook, to be sure, is not alone in seeking, compiling, and monetizing vast amounts of user data. It has good company in Google, Apple, cellphone service providers (e.g., Sprint and AT&T), and the other "high tech" behemoths.[53] These companies have become surveillance intermediaries, not by design or intended business purpose, but because their activities involve the collection of private data and information that is so attractive to law enforcement.[54] Take for instance, the recent revelation that the Trump Administration's Department of Justice used subpoenas (which do not require court authorization) to compel Apple to produce records connected to 109 email addresses and phone numbers (but not tell the affected Apple customers/users about the production) as part of the administration's investigation into leaks of classified information.[55] It has come to light

---

Thereof at 1, Lundy v. Facebook Inc., No. 18-cv-06793 (N.D. Cal. Nov. 15, 2019), ECF No. 82 [hereinafter Motion to Dismiss].

50. Motion to Dismiss, *supra* note 49, at 13.

51. *Id.*

52. *See* Lapowsky, *supra* note 48.

53. *See Twitter Privacy Policy*, TWITTER, https://twitter.com/en/privacy [https://perma.cc/ED2J-M9HK] (last visited Oct. 25, 2021).

54. *See also* Byron Tau, *IRS Used Cellphone Location Data to Try to Find Suspects*, WALL ST. J. (June 19, 2020, 1:46 PM), https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815 [https://perma.cc/9476-P8V7] ("The episode demonstrates a growing law enforcement interest in reams of anonymized cellphone movement data collected by the marketing industry."). *See generally* Rozenshtein, *supra* note 25; Katherine J. Strandburg, *Home, Home, on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. Rev. 614 (2011).

55. *See* Jack Nicas et al., *In Leak Investigation, Tech Giants Are Caught Between Courts and Customers*, N.Y. TIMES (June 11, 2021), https://www.nytimes.com/2021/06/11/technology/apple-google-leak-investigation-data-requests.html [https://perma.cc/2447-8FDY]; Matt Zapotosky & Karoun Demrjian, *Trump Justice Dept. Secretly Subpoenaed Records of Two Democrats on House Intelligence Committee*, WASH. POST (June 11, 2021), https://www.washingtonpost.com/national-security/adam-schiff-leak-investigation-eric-swalwell/2021/06/11/ee935590-ca58-11eb-81b1-34796c7393af_story.html [https://perma.cc/5K7Q-VZQT].

that the data Apple provided in response included the data of congressional staff members and their families, at least two Democrat members of Congress (who were prominent critics of the Trump administration), and the Trump administration's own White House counsel to the former president.[56] This effort to obtain private data followed earlier subpoenas from the same Justice Department to obtain the phone and email records of reporters for the *New York Times*, *Washington Post*, and other media outlets as part of the same leak investigation.[57] It was also recently revealed that federal agencies, such as the Internal Revenue Service, are purchasing access to Americans' cellphone data from third-party contractors (who purchase the data from cellphone service providers) to use in criminal investigations.[58]

Flooding the surveillance intermediary industry recently are private actors seeking to profit from providing a service and/or product to the public, while simultaneously seeking to assist law enforcement in return for additional profit or other benefits.[59] Microsoft, for instance, constructed a database of 10 million facial images to help train and improve the facial recognition systems maintained by government and private clients.[60] The company built the database by collecting (without consent) photographs of people posted on the internet.[61]

A more notable and informative example of the government's law enforcement interest simultaneously being a business purpose is provided by Ring LLC (owned by Amazon.com, Inc.).[62] Ring is a

---

56. *See* Nicas, *supra* note 55.

57. *See* Charlie Savage & Katie Benner, *Trump Administration Secretly Seized Phone Records of Times Reporters*, NY TIMES, (June 2, 2021), https://www.nytimes.com/2021/06/02/us/trump-administration-phone-records-times-reporters.html [https://perma.cc/V6UC-RFKJ]; Devlin Barrett, *Trump Justice Department Secretly Obtained Post Reporters' Phone Records*, WASH. POST (May 7, 2021, 10:00 PM), https://www.washingtonpost.com/national-security/trump-justice-dept-seized-post-reporters-phone-records/2021/05/07/933cdfc6-af5b-11eb-b476-c3b287e52a01story.html [https://perma.cc/D5SZ-B6H2].

58. *See* Tau, *supra* note 54.

59. *See* Madhumita Murgia, *Microsoft Quietly Deletes Largest Public Face Recognition Data Set*, FIN. TIMES (June 6, 2019), https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2 [https://perma.cc/Y8S2-TTKP].

60. *See id.*

61. *See id.*

62. *See* Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-

popular maker and provider of home security products and systems, including its uber-popular "smart doorbell"—a replacement or auxiliary doorbell consisting of a small box containing a wi-fi enabled video camera that allows homeowners to observe (and record) what is occurring outside their door.[63] With the purchase of a Ring doorbell a homeowner can opt into the "Neighbor's App," an online neighborhood watch owned and operated by Amazon, where members of a neighborhood can share videos of suspicious or criminal activity.[64] Accompanying the Neighbors App is a "Law Enforcement Portal" that allows police departments who have partnered with Ring to request home security videos from residents through the app and get alerts when a homeowner in the department's jurisdiction posts a message in the Neighbor's App about criminal or suspicious activity.[65]

To secure partnerships with police departments, Ring has aggressively promoted its smart doorbell and the accompanying Law Enforcement Portal to law enforcement communities around the country.[66] Ring promotes the product and its portal at law enforcement conferences, conducts demonstrations and trainings for police departments, provides police departments with free Ring products to distribute to local homeowners, and offers discounts to cities and local community groups that purchase Ring's smart doorbells using public money.[67] The promotional push has been very successful with over 400 police departments and sheriff offices across the country entering into partnerships with the company.[68] Through these partnerships, and Ring purchasers opting into the Neighbor's App, Ring has created, as noted by law professor Andrew Ferguson, "a clever workaround for the development of a wholly new surveillance network, without the kind of scrutiny that would happen if it was coming from the police or government."[69]

---

ring-has-partnered-with-police-forces-extending-surveillance-reach/ [https://perma.cc/ABV2-FBU4].

63. *See* RING, https://ring.com/doorbell-cameras [https://perma.cc/A3CJ-UWQE] (last visited Oct. 25, 2021).

64. *See* Nicholas Chan, *The New Neighborhood Watch: Ring Cams Can Make Our Lives Safer—and a Lot Less Private*, SAN JOSE INSIDE (Oct. 31, 2019), https://www.sanjoseinside.com/news/the-new-neighborhood-watch-ring-cams-can-make-our-lives-safer-and-a-lot-less-private/ [https://perma.cc/BD7X-AWU2].

65. *See id.*; *see also* Harwell, *supra* note 62.

66. *See* Harwell, *supra* note 62.

67. *See id.*

68. *See id.*

69. *Id.*

Technology companies such as Ring are rapidly replacing traditional police surveillance efforts.[70] It is easy to see why and how. It starts with our growing dependence on technology and the conveniences it provides.[71] As our dependency deepens, technology companies further expand their collection of our personal data—everything from location data to heart rate to genealogy.[72] With this expansion comes a correlated desire by law enforcement to access and use the collected data for their own purposes and to relieve themselves of the burden of collecting the data using means subject to Fourth Amendment scrutiny.[73] It is an evolution predicted by Professor Paul Ohm in 2012:

> As the surveillance society expands, the police will learn to rely more on the products of private surveillance, and will shift their time, energy, and money away from traditional self-help policing, becoming passive consumers rather than active producers of surveillance. Private industry is destined to become the unwitting research and development arm of the FBI. If we continue to interpret the Fourth Amendment as we always have, we will find ourselves not only in a surveillance society, but also in a surveillance state.[74]

Professor Ohm's prediction has become our reality. Take for instance, Apple, the maker of smartphones, computers, smart watches, tablets, mobile media players, and other modern technology products that are now ubiquitous.[75] Through its products, Apple collects an ever-expanding and wide range of personal data that law enforcement is consistently trying to access.[76] The tech giant and law enforcement have engaged in a number of high-profile battles over access to Apple users' data.[77] Generally, however, the company has accepted its role

---

70. *See id.*; Ohm, *supra* note 26, at 1311.

71. *See* Ohm, *supra* note 26, at 1311.

72. *See* Rozenshtein, *supra* note 25, at 99–100; Sarah Zhang, *The Messy Consequences of the Golden State Killer Case*, ATLANTIC (Oct. 2019), https://www.theatlantic.com/science/archive/2019/10/genetic-genealogy-dna-database-criminal-investigations/599005/ [https://perma.cc/5D9Y-6PDY].

73. *See* Ohm, *supra* note 26, 1338.

74. *See id.* at 1311.

75. *See generally* APPLE, https://www.apple.com/ [https://perma.cc/8QSU-G975] (last visited Oct. 25, 2021).

76. *See* Julie Carrie Wong, *The FBI and Apple are Facing Off Over an iPhone Again. What's Going On?*, THE GUARDIAN (Jan. 14, 2020); *see also* LEANDER KAHNEY, TIM COOK: THE GENIUS WHO TOOK APPLE TO THE NEXT LEVEL 172–73 (2019) (describing the conflict between Apple and the FBI after the 2015 San Bernardino shooting).

77. *See* Wong, *supra* note 76; KAHNEY, *supra* note 76, at 172–73.

as a provider of surveillance data to the government.[78] This acceptance is aptly reflected by the company's "Law Enforcement Program."[79] Apple explains the program as follows:

> We believe that law enforcement agencies play a critical role in keeping our society safe and we've always maintained that if we have information we will make it available when presented with valid legal process. In recognizing the ongoing digital evidence needs of law enforcement agencies, we have a team of dedicated professionals within our legal department who manage and respond to all legal requests received from law enforcement agencies globally. Our team also responds to emergency requests globally on a 24/7 basis.[80]

To further facilitate law enforcement requests for user data, Apple announced that the company is "in the process of launching an online portal for authenticated law enforcement agencies globally to submit lawful requests for data, check request status, and obtain responsive data from Apple."[81]

To promote "transparency," Apple periodically publishes an accounting of the requests for information and data it receives from law enforcement.[82] These accounting reports further show how correct is Professor Ohm's observation that law enforcement is increasingly moving from being a provider to a consumer of surveillance data.[83] In the six months between July and December 2020, Apple received 4,025 requests for device data, 5,995 requests for user account data, and 537 requests for "financial identifiers" from law enforcement departments and agencies across the country.[84] This equates to Apple receiving just over fifty-seven requests for customer data every day during the time span.[85] Because most of these requests were subpoenas, the significance of these numbers is even more apparent (for the issue of privatized surveillance) because subpoenas, unlike warrants, do not require judicial approval before being served.[86]

78. *See Privacy*, APPLE, https://www.apple.com/privacy/government-information-requests/ [https://perma.cc/N3FY-2Z3C] (last visited Oct. 25, 2021).

79. *See id.*

80. *Id.*

81. *Id.*

82. *See, e.g.*, *U.S. Government Requests by Legal Process Type, July-December 2020*, APPLE, https://www.apple.com/legal/transparency/us.html [https://perma.cc/F4U7-J339] (last visited Dec. 18, 2021).

83. *Compare id.*, *with* Ohm, *supra* note 26, at 1311.

84. *See* APPLE, *supra* note 82.

85. *See id.*

86. *See id.* By way of comparison, warrant backed requests for the same time period: 496 warrants for device data, 92 warrants for financial identifiers, and 1,937 warrants for account data. *Id.*

Before serving a tech company (or any company) a subpoena for user data, the government is not required to demonstrate to a judge that there is probable cause to believe that a crime has been committed or that the sought after user data is likely evidence of criminality.[87] A subpoena really is a fishing expedition backed by the force of law.[88]

Apple is not alone. Many technology companies that collect and maintain user data are now regular providers of surveillance data to law enforcement.[89] Tech behemoth Google, in fact, has become a provider of user data in quantities and regularity that far outpaces its big tech colleagues and competitors.[90] During the July to December 2019 time span, the government served Google with 12,110 subpoenas for user data.[91] This equates to 65.8 subpoenas for user data each day during the period.[92] The subpoenas concerned 65,931 user accounts.[93] Google provided user data in response to 80% of the subpoenas.[94]

Google epitomizes how the growth of private surveillance is becoming the outsourced life-blood of law enforcement investigations.[95] Between July and December 2009, the tech giant received just (in hindsight) 3,580 requests for user data from the government.[96] In just three years (i.e., July to December 2012) that number more than doubled to 8,438 requests (concerning 14,791 user accounts), which included 5,784 subpoenas (or 31.4 subpoenas per day).[97] The total request number nearly doubled again over the next five years, with Google receiving 23,025 government requests (concerning 50,930 user accounts), which included 9,320 subpoenas

87. *See* Jay Greene, *Tech Giants Have to Hand over Your Data When Federal Investigators Ask. Here's Why*, WASH. POST (June 15, 2021, 6:00 AM), https://www.washingtonpost.com/technology/2021/06/15/faq-data-subpoena-investigation/ [https://perma.cc/N6NA-G6G2].

88. *See id.*

89. *See Global Requests for User Information*, GOOGLE, https://transparencyreport.google.com/userdata/overview?hl=en&user_requests_report_period=series:requests,accounts;authority:US;time:&lu=user_requests_report_period [https://perma.cc/8E3H-RNKK] (last visited Oct. 25, 2021).

90. *See id.*

91. *See id.*

92. *Id.*

93. *Id.*

94. *Id.* During this same period, Google received 14,652 warrants concerning 21,856 user accounts. *Id.* The company provided user data in response to 83% of the warrants. *Id.*

95. *See id.*

96. *Id.* Google's transparency report does not specify the type or form of the request for this time period.

97. *Id.*

for user data (or 51.5 subpoenas per day), during the January to June 2017 time period.[98]

Ironically, the big tech companies periodically battle among themselves about who controls the data they amass and how and when the companies can access users' data when their technology is dependent on another company's technology, platform, or hardware.[99] One such battle is brewing currently between Apple and Facebook.[100] Apple recently announced a plan to incorporate a feature into its iPhones and iPads that notifies owners when applications (or apps) are tracking them, and allow users to opt out of the tracking.[101] This has angered Facebook, which depends on its apps' tracking capability to distribute targeted advertisements to Facebook users.[102] Apple's change, therefore, presents a multiple billion-dollar threat to Facebook.[103] In one recent quarter, for example, nearly 99% of the social media company's $20 billion in revenue came from advertising.[104] In response to Apple's tracking change, Facebook launched a website dedicated to criticizing the move, took out full page ads in the *New York Times* and *Wall Street Journal* criticizing the move, and publicly stated that it would provide information hurtful to Apple in a pending antitrust lawsuit against Apple.[105]

Technologies companies, however, do not solely account for the explosive expansion of surveillance intermediaries.[106] The exponential growth of companies providing private security contractors and guards is also a significant contributor.[107] It is estimated that there are as many private security guards employed in the United States as there are high school teachers—with the private guard labor force exceeding

98. *Id.*

99. *See, e.g.*, Jack Nicas & Mike Issac, *Facebook Takes the Gloves Off in Feud with Apple*, N.Y. TIMES (Dec. 16, 2020), https://www.nytimes.com/2020/12/16/technology/facebook-takes-the-gloves-off-in-feud-with-apple.html [https://perma.cc/5YLU-D6ZV].

100. *See id.*

101. *See id.*

102. *See id.*

103. *See* Steve Kovach, *Facebook-Apple Skirmish Is the Latest in a Fight that Stretches Back More than a Decade*, CNBC (Dec. 23, 2020, 12:12 PM), https://www.cnbc.com/2020/12/23/facebook-vs-apple-ten-year-war-over-internet-business.html [https://perma.cc/RS7Y-84Y5].

104. *See id.*

105. *See* Nicas & Issac, *supra* note 99.

106. *See* KEVIN STROM ET AL., THE PRIVATE SECURITY INDUSTRY: A REVIEW OF THE DEFINITION, AVAILABLE DATA SOURCES, AND PATHS MOVING FORWARD § 8-1 (Dec. 2010).

107. *See id.*

one million people.[108] This privatized labor force is used widely.[109] Private security guards now protect government institutions, buildings, and infrastructure.[110] Private companies invest heavily in private security to protect company property (real and intellectual), conduct internal investigations, conduct pre-employment screenings and post-employment monitoring, and to protect information technology systems.[111] Under current law, private security guards and privatized security providers are largely outside the reach of the Fourth Amendment.[112] This is so even when courts find that that private security forces are "organized in quasi-military ranks, similar to a police department" and hired and paid to "provide patrolling and law enforcement services," or even when state law allows private security officers to exercise arrest powers.[113] In short, the old saying of "walks like a duck, and talks like a duck," has no bearing under current law when it comes to private security forces walking, talking, and acting like police officers.[114]

II. THE GROWING PRIVATIZATION OF SURVEILLANCE: PROBLEMS AND HARMS

So, what is the problem with law enforcement evolving from being active producers of surveillance to being surveillance consumers? In other words, why should we care that private actors are

108. *See* Samuel Bowles & Arjun Jaydev, *One Nation Under Guard*, N.Y. TIMES (Feb. 15, 2014, 4:20 PM), https://opinionator.blogs.nytimes.com/2014/02/15/one-nation-under-guard/?mtrref=www.google.com&gwh=E9853B235BEA3859D3D8DCD34233E74F&gwt=regi&assetType=REGIWALL [https://perma.cc/3VUQ-47UH].

109. *See* STROM ET AL., *supra* note 106, at § 1-1.

110. *See id.* at § 4.4.5.

111. *See id.* at § 2-1.

112. *See, e.g.*, United States v. Green, 975 F.3d 653, 655 (7th Cir. 2020) (explaining that "a private security guard, even when authorized to use deadly force in self-defense and arrest trespassers pending police arrival, [is] not a state actor"); United States v. Cintron, No. 11-6316, 482 Fed. Appx. 353, 356, 358 (10th Cir. June 5, 2012) (holding that private security guard was not acting as a government agent when he searched and detained the defendant); United States v. Abney, No. 03 CR, 60(JGK), 2003 WL 22047842, at *6 (S.D.N.Y. Aug. 29, 2003) (holding that an off-duty officer working as a security guard acted as a private party not subject to Fourth Amendment when he seized and searched the defendant).

113. United States v. Talton, No. 18-cr-20599, 2019 WL 6486171, at *1 (E.D. Mich. Dec. 3, 2019) (holding that Fourth Amendment did not reach two private security guards who stopped, seized, and searched the defendant) (internal quotation marks omitted); *see, e.g.*, United States v. Day, 591 F.3d 679, 687, 689 (4th Cir. 2010).

114. *See, e.g.*, *Abney*, 2003 WL 22047842, at *6.

increasingly providing surveillance services, information, and data to the government for use in criminal investigations and prosecutions? A natural first reaction is that we should not care because increased privatized surveillance is only a danger to those engaging in criminal conduct, which is a danger most of society would applaud. Moreover, because Americans are increasingly aware that our movements in public, internet use, electronic communications, spending activities, and much of our lives are being monitored and tracked by private companies, it comes as no surprise or concern that the government has access to the tracking data. We also understand that law enforcement and the government deploy and operate street cameras and other technology to monitor public streets, government buildings, and other public spaces. We equally understand that in pursuing their non-law-enforcement business objectives, private companies, particularly companies in the internet and technology spaces, amass troves of information and data that can be accessed and obtained by law enforcement under particular circumstances.

However, what is not universally recognized, understood, or appreciated is that the diminishing line between private and government surveillance is eroding the privacy protection offered by the Fourth Amendment to *all* citizens and incentivizing private actors to violate the privacy and property of others.[115] The resulting consequences, as explained next, are a direct and present danger to our democracy and to the stability of national community.

First and foremost, with the growth of privatized surveillance comes a corresponding devaluation and weakening of the Fourth Amendment and its privacy protections.[116] The principal purpose of the Fourth Amendment is to shield us from unwarranted government invasions into our daily lives, persons (bodies), homes, and other personal property.[117] The privacy the Fourth Amendment protects is not only personal, but critical to personal existence, growth, and thought.[118] "Privacy is [indeed] the basis of individuality," and

115. *See* Bert-Jaap Koops & Ronald Leenes, *'Code' and the Slow Erosion of Privacy*, 12 MICH. TELECOMMS. & TECH. L.R. 115, 118 (2005).

116. *See* U.S. CONST. amend. IV (indicating the privacy protections of the Fourth Amendment); Brennan-Marquez, *supra* note 22, at 486–89; Rozenshtein, *supra* note 25, at 99100; Cover, *supra* note 26, at 1445; Ohm, *supra* note 26, at 1311; Balkin, *supra* note 26, at 8; Burkoff, *supra* note 31, at 627.

117. *See* Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) ("The 'basic purpose of this Amendment,' our cases have recognized, 'is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.'" (quoting Camera v. Mun. Ct. of City and Cnty. of S.F., 387 U.S. 523, 528 (1967))).

118. *See* Brennan-Marquez, *supra* note 22, at 494.

therefore, unjustified "[i]nvasions of privacy demean the individual."[119] The unjustified and unwarranted intrusions into privacy are no less demeaning or devaluing of a person's individuality because the intrusion is by the hand of a private actor versus a government one.[120] The effect is the same, particularly if the spoils of the private intrusion are used to fuel government action (such as a criminal prosecution) against a person.[121]

But protecting individual privacy from government intrusion is only half of the dual-purposed Fourth Amendment.[122] The amendment's other primary purpose is to promote citizen engagement with society and democratic life by protecting the balance of power relationship between the people and the government.[123] This balance is disrupted if the government is allowed to surveil and monitor without sufficient limits or restraints, and the disruption chills free discourse and civic involvement.[124] One can (and should) look to how the FBI surveilled civil rights activists during the 1960s and 1970s to understand how government surveillance can be weaponized to disrupt the democratic process, sabotage collective association, discourage participation in the democratic process, and chill oppositional speech.[125] The chilling effect harm is not avoided or

---

119. United States v. White, 401 U.S. 745, 763–64 (1971) (Douglas, J. dissenting).

120. *See* Brennan-Marquez, *supra* note 22, at 497.

121. *See id.* at 498.

122. *See White*, 401 U.S. at 762 (Douglas, J. dissenting) ("Monitoring, if prevalent, certainly kills free discourse and spontaneous utterances.").

123. *See* United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J. concurring); *see also* Harris v. United States, 331 U.S. 145, 160–61 (1947) (Frankfurter, J. dissenting) ("If one thing . . . can be said with confidence it is that the protection afforded by the Fourth Amendment against search and seizure by the police, except under the closest judicial safeguards, is not an outworn bit of Eighteenth Century romantic rationalism but an indispensable need for a democratic society.").

124. *See White*, 401 U.S. at 762 (Douglas, J. dissenting) ("Monitoring, if prevalent, certainly kills free discourse and spontaneous utterances.").

125. *See, e.g.*, Deena Zaru, *FBI, Which Conducted Surveillance on MLK, Sees Backlash After Social Media Post*, ABCNEWS.COM (Jan. 21, 2020, 3:27 PM), https://abcnews.go.com/Politics/backlash-fbi-post-honoring-martin-luther-king-jr/story?id=68425778 [https://perma.cc/P9LH-HBF3]; David J. Garrow, *The FBI and Martin Luther King*, ATLANTIC (July/August 2002), https://www.theatlantic.com/magazine/archive/2002/07/the-fbi-and-martin-luther-king/302537/ [https://perma.cc/8Z5P-VAVH]; John Kifner, *F.B.I. Sought Doom of [Black] Panther Party*, N.Y. TIMES (May 9, 1976), https://www.nytimes.com/1976/05/09/archives/fbi-sought-doom-of-panther-party-senate-study-says-plot-led-to.html [https://perma.cc/9PSW-CY2R]; Fred P. Graham, *F.B.I. Files Tell of Surveillance of Students, Blacks, War Foes*, N.Y. TIMES (March 25, 1971),

mitigated because the perpetrator of the invasive surveillance is a private actor as opposed to a government one.[126] This is particularly true when the private surveillance is used to fuel government efforts to suppress speech or political opposition.[127]

The harm and dangers associated with privatized surveillance are not limited to how the surveillance disturbs the balance between citizen and government. It also deleteriously affects how citizens relate to, and act towards each other.[128] For starters, privatized surveillance encourages class-based factionalism where the "chilling effects of [privatized] surveillance are not evenly distributed."[129] By this it is meant that today private surveillance is often employed for the benefit of, and at the direction of, the economically privileged at the expense (some would say exploitation) of those with less economic means and status.[130] The purpose of such surveillance is to monitor and police the "others" who fall on the lower rungs of the financial status hierarchy.[131] The usual end result: people with the least economic resources being subjected to privately funded and operated surveillance schemes that are far more rigorous, ubiquitous, and intrusive than their financially well-off neighbors.[132] The aerial surveillance of Baltimore is a perfect example.[133] In short, the growth

---

https://www.nytimes.com/1971/03/25/archives/fbi-files-tell-of-surveillance-of-students-blacks-war-foes-fbi.html [https://perma.cc/M8S4-AV8K].

126. *See* Brennan-Marquez, *supra* note 22, at 497.

127. *See id.*

128. *See generally, e.g.*, James P. Walsh, *Watchful Citizens: Immigration Control, Surveillance and Societal Participation*, 23 SOC. & LEGAL STUD. 246 (2014).

129. *See* Brennan-Marquez, *supra* note 22, at 495.

130. *See* Walsh, *supra* note 128, at 246.

131. *See id.*

132. *See* Barton Gellman & Sam Adler-Bell, *The Disparate Impact of Surveillance*, CENTURY FOUND. (Dec. 21, 2017), https://tcf.org/content/report/disparate-impact-surveillance/?agreed=1 [https://perma.cc/D4TN-HMSG].

133. Nearly 25% of Maryland's poor live in Baltimore City, even though the city comprises 11% of the state's total population. *See* OFF. OF POL'Y ANALYSIS, MD. DEP'T OF LEG. SERVS., HISTORY, PUBLIC POLICY, AND THE GEOGRAPHY OF POVERTY 3 (Jan. 2016). Black Baltimoreans account for more than 75% of the city's residents living in poverty. *See* CIV. RTS. DIV., U.S. DEP'T OF JUST., INVESTIGATION OF THE BALTIMORE CITY POLICE DEPARTMENT 14 (Aug. 10, 2016). The median income for black households in Baltimore is $33,610, which is slightly higher than half the median income for white households in the city ($60,550), and less than half the median income of all Maryland households ($73,538). *See* Jordan Malter, *Baltimore's Economy in Black and White*, CNN MONEY (Apr. 29, 2015, 8:59 PM), http://money.cnn.com/2015/04/29/news/economy/baltimore-economy/ [https://perma.cc/49XM-PAJQ].

of privatized surveillance is creating a tiered system of Fourth Amendment protection based on class and wealth.

Another citizen-to-citizen harm is that judicial acceptance and use of material seized by private actors in violation of another person's privacy or in violation of the law, "invites every man to become a law unto himself; it invites anarchy."[134] Vigilantism, and the encouragement of it, is the foreseeable and inevitable consequence of further limiting the Fourth Amendment's ability to reach private search conduct.[135] A glimpse of this consequence, and the harm it inflicts, was provided when private individuals assumed police powers to "investigate" alleged voting-related fraud during the 2020 presidential election.[136] These private "investigations" often consist of private persons violating the privacy rights of others in ways that would certainly trigger a Fourth Amendment violation if done by law enforcement officers.[137] The fall 2020 plot by thirteen men affiliated with an anti-government group to kidnap Michigan's governor and subject her to a secret trial previews the dangerous anarchy that accompanies this brand of vigilantism.[138]

This leads to the most frightening danger—when surveillance privatization mixed with vigilantism is taken to the extreme.[139] Imagine very wealthy individuals funding, directing, and deploying armies of private citizens as surveillance contractors to communities of the wealthy backers' choosing.[140] While these private contractors would be civilly and criminally liable for their surveillance actions that exceeded the law, any materials or information they collected could not be excluded as evidence in court on Fourth Amendment grounds.[141] Unrestricted by the Fourth Amendment, to collect

---

134. *See* Mapp v. Ohio, 367 U.S. 643, 659 (1961) (speaking about unlawful searches and seizures by state law enforcement officers and agents).

135. *See* Walsh, *supra* note 128, at 240, 249.

136. *See* Andrea Salcedo, *An Ex-cop Held an A/C Repairman at Gunpoint over a False Claim He Had 750,000 Fake Ballots, Police Said*, WASH. POST (Dec. 16, 2020, 7:34 AM), https://www.washingtonpost.com/nation/2020/12/16/aguirre-texas-cop-election-fraud/ [https://perma.cc/2JS2-23S4].

137. *See id.*

138. *See* Nicholas Bogel-Burroughs, *What We Know About the Alleged Plot to Kidnap Michigan's Governor*, N.Y. TIMES (Oct. 9, 2020), https://www.nytimes.com/2020/10/09/us/michigan-militia-whitmer.html [https://perma.cc/JCU5-TX9C].

139. *See id.*

140. *See id.*

141. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984) (stating that "[t]his Court has [] consistently construed [Fourth Amendment] protection as

evidence and information to provide to law enforcement, these private armies (and any private actor) can forcibly and/or surreptitiously enter people's homes; wiretap people's phones, offices, and homes; hack or otherwise access people's cellphones; place GPS trackers on people and their vehicles; and engage in similar privacy and property invading activity.[142] Any person charged and facing conviction based on the evidence collected using these tactics would have no Fourth Amendment recourse.[143]

Such a draconian state of affairs is not far-fetched, far-off, or paranoia. Baltimore's aerial surveillance program shows that uber-wealthy individuals are willing to use their wealth to fund the surveillance of communities in which they do not live.[144] The financing is there and available. So too are the masses of people willing to fill the ranks of private surveillance armies. In 2019, the Southern Poverty Law Center identified 576 extremist anti-government groups operating in the United States, of which 181 were armed militias.[145] It is currently estimated that there are 15,000 to 20,000 active militia members, of which at least 25% of them being active-duty or veteran members of the military.[146] These numbers show that there are plenty of Americans willing to serve in private armies.[147]

Recent events have ended the debate if there ever was one. In 2014, heavily armed teams of Oath Keepers, a far-right extremist group populated by former members of the military, law enforcement, and first-responders, descended on Ferguson, Missouri to "protect" local businesses during the protests and unrest over police brutality following the killing of Michael Brown.[148] Local police did not take

---

proscribing only government action" and not private searches by actors who are not acting as agents of the government).

142. *See id.*

143. *See id.*

144. *See* Rector & Broadwater, *supra* note 5.

145. *See Michigan 'Plot': Who are the US Militia Groups*, BBC NEWS (Oct. 9, 2020), https://www.bbc.com/news/world-us-canada-54483973 [https://perma.cc/95SZ-EV3Z].

146. *See* Jennifer Steinhauer, *Veterans Fortify the Ranks of Militias Aligned with Trump's Views*, N.Y. TIMES (Jan. 20, 2020), https://www.nytimes.com/2020/09/11/us/politics/veterans-trump-protests-militias.html [https://perma.cc/8K2G-888N].

147. *See id.*

148. *See* Mike Giglio, *A Pro-Trump Militant Group has Recruited Thousands of Police, Soldiers, and Veterans*, ATLANTIC (Nov. 2020), https://www.theatlantic.com/magazine/archive/2020/11/right-wing-militias-civil-war/616473/ [https://perma.cc/QJ7G-9D5D]; Cassandra Vinograd, *Oath Keepers*

any action or confront the Oath Keepers even though their open carrying and displaying of automatic and other firearms was legally questionable.[149] As mentioned earlier, in October 2020, thirteen men affiliated with an anti-government group were charged with plotting to kidnap Michigan's governor and have her tried in a secret trial over the measures she imposed to slow the spread of the coronavirus.[150] As part of their planning and preparation, the men surveilled the governor's home and engaged in firearms training and combat drills for months.[151] The now-infamous insurrectionist storming of the U.S. Capitol to prevent the certification of the 2020 presidential election has put a spotlight on the rise of organized extremist groups who model themselves after the military and consider themselves to be armies of "patriots."[152]

It is only a matter of time before these two forces come together, and America's streets see privately funded armies conducting surveillance for the benefit of law enforcement. In fact, we may be closer to this state of affairs than we think, which should concern and frighten us all. The connections between law enforcement and militant groups, particularly extreme far right-wing and racist groups, are expanding and growing.[153] The connections include law enforcement officers who are actual members or open supporters of such groups.[154]

Turn up at Michael Brown Protests in Ferguson, Missouri, NBC NEWS (Aug. 11, 2015, 5:52 AM), https://www.nbcnews.com/storyline/michael-brown-shooting/oath-keepers-turn-michael-brown-protests-ferguson-missouri-n407696 [https://perma.cc/UD2G-MM28].

149. *See id.*

150. *See* Bogel-Burroughs, *supra* note 138.

151. *See id.*

152. *See* Spencer S. Hsu et al., *Self-Styled Militia Members Planned on Storming the U.S. Capitol Days in Advance of the Jan. 6 Attack, Court Documents Say*, WASH. POST (Jan. 19, 2021, 8:28 PM), https://www.washingtonpost.com/local/legal-issues/conspiracy-oath-keeper-arrest-capitol-riot/2021/01/19/fb84877a-5a4f-11eb-8bcf-3877871c819d_story.html [https://perma.cc/YA7E-JHEM]; Julian E. Barnes & Hailey Fuchs, *White House Orders Assessment on Violent Extremism in U.S.*, N.Y. TIMES (Jan. 22, 2021), https://www.nytimes.com/2021/01/22/us/politics/capitol-riot-domestic-extremism.html [https://perma.cc/P7CC-J62T].

153. *See* Sam Levin, *White Supremacists and Militias Have Infiltrated Police Across US, Report Says*, GUARDIAN (Aug. 27, 2020, 10:13 AM), https://www.theguardian.com/us-news/2020/aug/27/white-supremacists-militias-infiltrate-us-police-report [https://perma.cc/W4FU-QZX9].

154. *See* Michael German, *Report: Hidden in Plain Sight: Racism, White Supremacy, and Far-Right Militancy in Law Enforcement*, BRENNANCENTER.ORG (Aug. 27, 2020), https://www.brennancenter.org/our-work/research-reports/hidden-plain-sight-racism-white-supremacy-and-far-right-militancy-

It is not paranoia. A federal judge took the extraordinary step of declaring a group of Los Angeles police officers to be a "neo-Nazi, white supremacist gang" that had the support of their supervisors.[155] Two officers in Alabama were discovered to be active members of the League of the South, a neo-confederate white supremacist group that advocates for a repeat southern succession dominated by "European Americans."[156] In a five-year span, three officers with the Fruitland Park Police Department in Florida resigned or were fired after it was discovered that they were members of the Ku Klux Klan, including one officer who admitted to holding a leadership position in the infamous hate group.[157] Ironically, the internet, social media, and advanced computer technology is making it easier to identify and expose law enforcement officers who are affiliated with, or support, extremist and racist groups. A Prince County, Virginia, sheriff's deputy was fired after internet sleuths uncovered his social media posts pledging support for the Proud Boys and advocating violence against Supreme Court Chief Justice John Roberts.[158]

These stories are just a small sample of a large and growing problem. According to a recent report documenting the issue, "[s]ince 2000, law enforcement officials with alleged connections to white supremacist groups or far-right militant activities have been exposed in Alabama, California, Connecticut, Florida, Illinois, Louisiana,

---

law#footnote5_m12yydl [https://perma.cc/683M-K44G]; *see generally also* Vida B. Johnson, *KKK in the PD: White Supremacist Police and What to Do About It*, 23 LEWIS & CLARK L. REV. 205 (2019).

155. *See* Hector Tobar, *Deputies in 'Neo-Nazi' Gang, Judge Found: Sheriff's Department: Many at Lynwood Office Have Engaged in Racially Motivated Violence Against Blacks and Latinos, Jurist Wrote*, L.A. TIMES (Oct. 12, 1991, 12:00 AM), https://www.latimes.com/archives/la-xpm-1991-10-12-me-107-story.html [https://perma.cc/T6T9-TBE4].

156. Becky Bratu, *Two Alabama Officers Put on Leave for Alleged Ties to Hate Group*, NBC NEWS (June 17, 2015, 9:12 PM), https://www.nbcnews.com/news/crime-courts/two-alabama-officers-put-leave-alleged-ties-hate-group-n377421 [https://perma.cc/BD34-KBP7].

157. Michael Winter, *KKK Membership Sinks 2 Florida Cops*, USA TODAY (July 14, 2014, 6:23 PM), https://www.usatoday.com/story/news/nation/2014/07/14/florid-police-kkk/12645555/ [https://perma.cc/78TV-DUPP].

158. *See* Robert Klemko, *A Small Group of Sleuths Had Been Identifying Right-Wing Extremists Long Before the Attack on the Capitol*, WASH. POST (Jan. 10, 2021, 6:23 PM), https://www.washingtonpost.com/national-security/antifa-far-right-doxing-identities/2021/01/10/41721de0-4dd7-11eb-bda4-615aaefd0555_story.html [https://perma.cc/2WN6-C943].

Michigan, Nebraska, Oklahoma, Oregon, Texas, Virginia, Washington, West Virginia, and elsewhere."[159]

It is a problem the FBI has long known existed. An FBI assessment in 2006 noted that white supremacist groups have a "'historical' interest in infiltrating law enforcement communities or recruiting law enforcement personnel."[160] The assessment also explained how the agency had discovered the term "ghost skin" used by white supremacists to describe "those who avoid overt display of the [white supremacist] beliefs to blend into society and covertly advance white supremacist causes."[161] The problem has only grown in the years since, and the FBI knows this as well.[162] An FBI counterterrorism report from April 2015 notes that "domestic terrorism investigations focused on militia extremists, white supremacist extremists, and sovereign citizen extremists often have identified active links to law enforcement officers."[163]

III. THE CURRENT DEPUTIZATION FRAMEWORK: PRIVATE SURVEILLANCE, SEARCHES, AND THE FOURTH AMENDMENT

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[164]

Generally, the amendment's protection only extends to searches and seizures made by the government and not private actors.[165] This limitation has been the subject of much debate and litigation. Indeed, the entanglement of the Fourth Amendment and private actors

159. German, *supra* note 154.

160. Alice Speri, *The FBI Has Quietly Investigated White Supremacist Infiltration of Law Enforcement*, INTERCEPT (Jan. 31, 2017, 7:10 AM), https://theintercept.com/2017/01/31/the-fbi-has-quietly-investigated-white-supremacist-infiltration-of-law-enforcement/ [https://perma.cc/4NG9-Z6PG].

161. *Id.*

162. *See id.* (explaining that FBI Counterterrorism policy guides included reference to white supremacist extremists).

163. *Id.*

164. U.S. CONST. amend. IV.

165. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984) (stating that "[t]his Court has also consistently construed [Fourth Amendment] protection as proscribing only government action" and not private searches by actors who are not acting as agents of the government).

conducting searches and surveillance to assist law enforcement is not new. The issue has existed well before the advent of the internet, email, and cellphones.[166] The constitutional problem was well developed in the "analog" age, when courts confronted the Fourth Amendment implications of searches of hotel rooms by hotel staff, searches of the workplace conducted by employers, and searches of packages by mail and parcel carriers.[167]

The foundation for this area of Fourth Amendment jurisprudence, as explored in this section, was set by four Supreme Court cases concerning the relationship between the Fourth Amendment and searches by private actors that were decided in 1921, 1971, 1980, and 1984, respectively.[168] Together the four cases are the foundation and boundary setters of what Professor Brennan-Marquez has labeled the "deputization framework" of Fourth Amendment jurisprudence concerning private searches.[169] In short, under the deputization framework a private search or seizure is reached by the Fourth Amendment only if the private searcher was "deputized" into acting as an agent or instrument of the government.[170] Without the requisite deputization, private searches do not constitute Fourth Amendment searches, regardless if the search was unreasonable or violated another person's privacy or property interests.[171]

The first foundational case, *Burdeau v. McDowell*, involved McDowell's employer entering and searching (without permission) his personal (noncompany affiliated) office following McDowell's termination for suspicion that he was involved with mail fraud.[172] During the search the employer found documents incriminating McDowell, which the employer promptly provided to the Department of Justice.[173] The search involved the employer's representatives blowing open two safes in the office to collect their contents and forcibly opening McDowell's desk and taking all documents found in

166. *See* Brennan-Marquez, *supra* note 22, at 499–502.
167. *See id.*
168. *See id.* at 499.
169. *See id.* at 499–502.
170. *See id.* at 488.
171. *See id.*; *see also* United States v. Silva, 554 F.3d 13, 18 (1st Cir. 2009) ("The Fourth Amendment's protection against unreasonable searches and seizures applies only to government action and not 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government.'").
172. Burdeau v. McDowell, 256 U.S. 465, 472–73 (1921).
173. *See id.* at 473–74.

it.[174] McDowell petitioned the federal court for an order requiring the return of the seized documents before they were submitted to a federal grand jury, arguing in part, that the employer's search and seizure conduct was a Fourth Amendment violation.[175] The district court granted McDowell's motion "solely upon the ground that the government should not use stolen property for any purpose after demand made for its return."[176] The Supreme Court reversed and explained its Fourth Amendment-based reasons for doing so in two brief paragraphs.[177] According to the seven-justice majority, the Fourth Amendment's "origin and history clearly show[s] that it was intended as a restraint upon the activities of [the] sovereign authority," and therefore the amendment's protection against unlawful searches and seizures "applies to governmental action" only.[178] Since the search of, and seizure from, McDowell's office did not involve a government official, the high court concluded, "it is manifest that there was no invasion of the security afforded by the Fourth Amendment."[179] The majority was sensitive to the fact that McDowell's employer had unlawfully taken documents from his private office.[180] But because the former employer was a private actor and not a governmental one, the remedies that McDowell could pursue against his former employer according to the Court, were those "we are not now concerned."[181]

Burdeau is regarded as the case that first established the Fourth Amendment's government-action-only limitation.[182] The Court would not confront the issue again until nearly fifty years later in *Coolidge v. New Hampshire*, a case involving the "brutal murder" of a fourteen-year-old girl during a heavy snowstorm.[183] The case involved a myriad of Fourth Amendment issues.[184] Of relevance here, is Coolidge's claim that a Fourth Amendment violation occurred when investigating

174. *See id.*
175. *See id.* at 470–71.
176. *Id.* at 472.
177. *See id.* at 475.
178. *Id.*
179. *Id.*
180. *See id.*
181. *See id.*
182. *See, e.g.*, Burkoff *supra* note 31, at 628 ("The Supreme Court first established that private searches are not covered by the [F]ourth [A]mendment in *Burdeau v. McDowell*.").
183. Coolidge v. New Hampshire, 403 U.S. 443, 445 (1971).
184. For instance, Coolidge claimed that the warrant authorizing the search of his automobile was invalid because it was signed and issued by the state attorney general and not a "neutral and detached magistrate" as the Fourth Amendment requires. *Id.* at 449.

officers obtained a rifle and articles of clothing from Coolidge's wife during an interview at Coolidge's home while Coolidge was being interrogated at the police station.[185]

Coolidge argued that the Fourth Amendment reached and invalidated the seizure of his rifle and clothing because in turning over the items, his wife "was acting as an 'instrument' of the [officers, and] complying with a 'demand' made by them."[186] A thin five-justice majority rejected his "interpretation of the facts."[187] The key, according to the majority, was that Coolidge's wife freely and voluntarily offered to provide the police with the rifle and clothing because (as she admitted) she was motivated to clear her husband and believed they had nothing to hide.[188] "Without more," the Court explained, such powerful motivations were not "constitutionally suspect."[189] The "more" was lacking in Coolidge's case because the officers treated his wife with "perfect courtesy" and without the "slightest implication" of coercion or domination.[190] Therefore, according to the Court, "[t]o hold the conduct of the police here was a search and seizure [reached by the Fourth Amendment], would be to hold, in effect, that a criminal suspect has a constitutional protection against the adverse consequences of a spontaneous, good-faith effort by his wife to clear him of suspicion."[191] From *Coolidge* comes the doctrine that private searches and seizures trigger Fourth Amendment protections only if the private actor is serving as an "instrument" of the government.[192]

Less than a decade after *Coolidge*, the Supreme Court faced another private search challenge that would result in a split-decision.[193]

---

185. *Id.* at 484. The articles of clothing were those Coolidge's wife said Coolidge was likely wearing the night the victim disappeared. *Id.* at 486. Prosecutors used the results of a microscopic analysis of the clothing to argue that the clothes had been in close contact with the victim. *Id.* at 448. They also argued that the rifle provided by Coolidge's wife was the murder weapon. *Id.*

186. *Id.* at 487.

187. *Id.*

188. *See id.* at 489–90.

189. *Id.* at 488.

190. *Id.* at 489.

191. *Id.* at 489–90.

192. *See, e.g.*, United States v. Seidlitz, 589 F.2d 152, 158–59 (4th Cir. 1978) ("[T]he Fourth Amendment and the exclusionary rule by which it is enforced come into play only where it appears from all the circumstances that in a particular case the challenged evidence was obtained as a result of a search conducted by government officers or by private persons acting as agents or instrumentalities of the government." (citing *Coolidge*, 403 U.S. at 487–90)).

193. *See generally* Walter v. United States, 447 U.S. 649 (1980).

The case, *Walter v. United States*, involved a slew of "bizarre facts" that resulted in a privately-owned package carrier misdelivering multiple boxes of sexually explicit videos to a private company with a name that was similar to the addressed recipient.[194] The packing of the videos caused the unintended recipient's employees to suspect that the videos were illegal pornography.[195] The employees contacted the FBI, who took possession of the tapes and confirmed their sexual content by watching the videos without first obtaining a warrant.[196] Walter and his codefendants (the intended recipients) were charged with obscenity-related offenses.[197] The issue that reached the Supreme Court was whether the FBI's warrantless viewing of the videos was a search that violated the Fourth Amendment.[198] The Court issued a split-decision.[199] The Court held that the opening and inspection of the boxes by the private company employees did not constitute a Fourth Amendment violation (reaffirming the private search principle established in *McDowell* and *Coolidge*).[200] But the majority also held that the FBI's warrantless viewing of the videos was a violation because it constituted a separate search that "was not supported by any exigency, or by a warrant even though one could have easily been obtained."[201] *Walter* now stands for the principle that when a government agent expands or adds to a search conducted by a private actor, the "additional invasions of [a person's] privacy by the Government agent must be tested by the degree to which they exceeded the scope of the private search."[202]

The Fourth Amendment principles set by these foregoing cases were cemented in 1984 by *United States v. Jacobsen*.[203] Similarly to

194. *See id.* at 651–52.
195. *See id.*
196. *See id.* at 652.
197. *See id.*
198. *See id.* at 651.
199. *See id.* at 660–62.
200. *See id.* at 656 ("It has, of course, been settled since *Burdeau v. McDowell* that a wrongful search and seizure conducted by a private party does not violate the Fourth Amendment and that such private wrongdoing does not deprive the government of the right to use evidence that it has acquired lawfully.") (internal citation omitted).
201. *See id.* at 657 ("The projection of the films [by the FBI] was a significant expansion of the search that had been conducted previously by a private party and therefore must be characterized as a separate search. That separate search was not supported by any exigency, or by a warrant even though one could have easily been obtained.").
202. United States v. Jacobsen, 466 U.S. 109, 115 (1984).
203. *See generally id.*

Walter, *Jacobsen* involved the inspection of a package, but this time the inspection was done by a private package carrier (i.e., Federal Express) and not an unintended recipient.[204] The package at issue had been damaged while in the Federal Express facility, so employees of the carrier opened and examined the package to identify and document the damage to its contents.[205] Inside the package, the employees found four zip-lock bags containing a white powder the employees suspected was illegal drugs.[206] In response to a call about the discovery from Federal Express, an agent of the Drug Enforcement Agency (DEA) went to the facility and opened each of the four bags to get samples to conduct a drug field test.[207] The test indicated that the white powder was cocaine, and this finding was confirmed when additional agents arrived at the facility and conducted a second field test.[208] The agents subsequently obtained a warrant to search the residence that the package was addressed to, i.e., the residence of Jacobsen and his codefendants.[209]

After Jacobsen and his codefendants were charged with a drug distribution offense, they moved to suppress the cocaine evidence on the ground that the warrantless field tests constituted a Fourth Amendment violation (which also tainted the search warrant used to search their residence).[210] When the challenge reached the Supreme Court, it was rejected.[211] Relying principally on *Walter* (while also citing *Coolidge* and *McDowell*), first the Court held that the Fourth Amendment did not reach the search of the package by the Federal Express employees because the employees were private actors and not government agents.[212] According to the Court, it was of no consequence whether the search of the package by the carrier's employees was reasonable or unreasonable, or would be unlawful if

204. *See id.* at 111 (describing how the package at issue was opened and inspected at a Federal Express by a Federal Express office manager).

205. *See id.* (explaining that the employees opened the package "in order to examine its contents pursuant to a written company policy regarding insurance claims").

206. *See id.*

207. *See id.* at 111–12.

208. *See id.*

209. *See id.* at 112.

210. *See id.*

211. *See id.* at 126.

212. *See id.* at 113–14 ("This Court has also consistently construed this protection as proscribing only governmental action; it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.'" (quoting Walter v. United States, 447 U.S. 649, 662 (1980))).

done by a DEA agent; the end conclusion was the same—the employees' searching conduct "did not violate the Fourth Amendment because of their private character."[213] Moreover, the Court explained, once the Federal Express employees opened and searched the package, and then invited a federal agent to view the suspicious contents, the "agent's viewing of what [the private carrier employees] had freely made available for his inspection did not violate the Fourth Amendment."[214]

Harking back to *Walter*, the only question that remained was "whether the additional intrusion occasioned by the field test, which had not been conducted by the Federal Express [agents] and therefore exceeded the scope of the private search, was an unlawful 'search' or 'seizure' within the meaning of the Fourth Amendment."[215] The Court concluded that it was not, primarily because "[a] chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy."[216]

IV. THE (GROWING) LIMITATIONS AND PROBLEMS WITH THE DEPUTIZATION FRAMEWORK

Historically, the benefit of the deputization framework was that it provided a clear line of demarcation that separated private and public searches for Fourth Amendment purposes, and defined when private searches cross that line and therefore are subject to Fourth Amendment scrutiny.[217] Today though, that line is less clear, and where it can be seen, it provides a weak enforcement of the Fourth Amendment's role of prohibiting the government from benefiting from private intrusions, including unlawful ones, into our persons, property, and privacy.[218] This Section explores why this is happening.

213. *See id.* at 115.
214. *Id.* at 119.
215. *Id.* at 122.
216. *Id.* at 123. The Court also held that while the defendants/respondents had a possessory interest in the package and its contents that is protected from seizure by the Fourth Amendment, the use and destruction of a small amount of the cocaine during the field test was reasonable and had only a *de minimis* impact on the defendants'/respondents' possessory interests. *See id.*
217. *See supra* Part III.
218. *See infra* Section IV.B.

A. Overreliance on Agency Principles

A critical flaw in the current deputization framework is its overreliance on agency principles.[219] The overreliance renders the framework incapable of addressing situations where a private searcher's status and conduct falls short of casting the person as an "agent" of the law enforcement, but whose surveillance conduct is nonetheless inextricably linked to law enforcement and benefits the government.[220] Agency principles define the fiduciary relationship where one party (the agent) agrees to act on another's (the principal) behalf and be controlled by that other party.[221] Such principles do not securely fit or address the relationship between the government and the types of private searchers that are of concern today, like the big tech surveillance intermediaries, extremist vigilantes, militias, and private security guards.[222] Traditional agency is not present because these types of private searchers will forever remain separate from a fiduciary and command-and-control standpoint from the government.[223] Therefore, more beyond an agency model is needed to protect against the erosion of the Fourth Amendment posed by these types of private searchers in particular.

B. Over-Focus on Government's Role and Influence

The agency-based deputization framework today overly focuses on the government's role in the private search and influence over the private searcher.[224] Not enough bandwidth or weight is focused on the private searcher, particularly the private searcher's importance to the government, and the private searcher's intrusion into a person's private space.[225]

---

219. *See, e.g.*, United States v. Koenig, 856 F.2d 843, n.1 (7th Cir. 1988) (explaining that "[a]n agency relationship 'results from the manifestation of consent by one person to another that the other shall act on his [or her] behalf and subject to his [or her] control, and consent by the other so to act'" (quoting Restatement (Second) of Agency § 1 (1958))).

220. *See infra* Section IV.B.

221. *See* Restatement (Third) of Agency § 1.01.

222. *See supra* Part I.

223. *See supra* Part I.

224. *See* United States v. Keith, 980 F. Supp. 2d 33, 40 (D. Mass. 2013) (quoting United States v. Silva, 554 F.3d 13, 18 (1st Cir. 2009)).

225. *See id.*

The First Circuit standard for determining when a private searcher has become an agent of the government is representative of the problem.[226] The standard consists of the following three factors:

> (1) 'the extent of the government's role in instigating or participating in the search'; (2) '[the government's] 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 interest.'[227]

Two (the first and second) of the three factors focus on the government's role, influence, and intent.[228] Only the last explores the role and interests of the private searcher.[229]

This wide imbalance is a problem.[230] The nearly myopic focus ignores (or at least fails to understand) that the transformation of the government from suppliers to consumers of surveillance has come with the government taking a diminished role in instigating, encouraging, and controlling private searches.[231] Indeed, the private searchers of concern in this Article voluntarily intrude on the privacy of others and do so beyond the control or direction of the government.[232] The current deputization framework vastly under-appreciates "systemic but informal private surveillance [where] private actors turn *themselves*, into the 'eyes and ears' of law enforcement."[233] With the rise of the surveillance intermediaries (e.g., Google); private benefactors bank rolling private surveillance efforts (e.g., the PSS surveillance program in Baltimore); and extremists, private security guards, and private militias exercising police powers, there needs to be a corresponding shift in the focus toward the role, intent, and interest of the private searcher.[234] Absent such shift, the

226. *See id.*
227. *Id.*
228. *See id.*
229. *See id.*
230. *See id.*
231. This focus is not surprising since many of the precedents that form the foundation of the government-focused approach were decided before the tech companies and other modern surveillance intermediaries existed or had grown into the data collecting and sharing giants they are today. *See, e.g.*, United States v. Smythe, 84 F.3d 1240, 1243 (10th Cir. 1996) ("The totality of the circumstances guides the court's determination as to whether 'the government coerces, dominates, or directs the actions of a private person.'" (quoting United States v. Miller, 688 F.2d 652, 796 (9th Cir. 1982))).
232. *See supra* Part I.
233. Brennan-Marquez, *supra* note 22, at 503 (emphasis in original).
234. *See* discussion *supra* Part I.

existing deputization framework will continue to be a backdoor loophole within the Fourth Amendment that allows the government to benefit from unlawful invasions and intrusions into private spaces that the Fourth Amendment was designed to prevent.[235] This loophole will only grow as we move further into the digital age and as the police shift to "becoming passive consumers, rather than active producers of surveillance."[236]

C. Lack of Uniformity

Another pressing problem with the deputization framework is the absence of a uniformed standard that courts use to determine whether a private search constitutes government action that is subject to the Fourth Amendment.[237] What exists now is a patchwork of different standards that are not always consistent.[238] The lack of uniformity means that whether a private searcher will be found to be a government agent greatly depends on where (which circuit) a case resides.[239]

As discussed earlier, the First Circuit employs a three-factor standard:

> (1) 'the extent of the government's role in instigating or participating in the search'; (2) '[the government's] 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 to primarily help the government or to serve its own interest.'[240]

In comparison, the Fourth, Seventh, Ninth, and Tenth Circuits apply a two-factor standard: "(1) whether the Government knew of and acquiesced in the private search; and (2) whether the private individual intended to assist law enforcement or had some other independent

---

235. *See* Reid v. Pautler, 36 F. Supp. 3d 1067, 1149 (D.N.M. 2014) ("Fourth Amendment 'establishes a simple baseline, one that for much of our history formed the exclusive basis for its protections: When the 'Government obtains information by physically intruding' on persons, houses, papers, or effects, 'a 'search' within the original meaning of the Fourth Amendment' has 'undoubtedly occurred.'" (quoting Florida v. Jardins, 133 S. Ct. 1409, 1414 (2013))).

236. Ohm, *supra* note 26, at 1311.

237. *See* United States v. Ackerman, 831 F.3d 1292, 1301 (10th Cir. 2016) (noting the lack of uniformity in the number and substance of factors among courts).

238. *See id.*

239. *See id.*

240. United States v. Keith, 980 F. Supp. 2d 33, 40 (D. Mass. 2013) (quoting United States v. Silva, 554 F.3d 13, 18 (1st Cir. 2009)).

motivation."[241] The Sixth Circuit also employs a two-factor standard, but one that replaces the knowledge factor with whether law enforcement "instigated, encouraged, or participated in the search."[242] While there is some overlap among the various standards, there are some significant differences.[243]

There is also a lack of uniformity on the individual factor level.[244] Take the government's knowledge factor. For some courts, whether the government knew the private search was going to occur is a stand-alone factor to consider.[245] For others, the inquiry is did "the government [know] of *and acquiesce[]*" to the private search, which "encompass[es] the requirement that the government agent must also affirmatively encourage, initiate or instigate the private action."[246] Two widely different approaches to the government's knowledge factor, which can lead to widely different outcomes given the same set of facts.[247]

There is another troubling consequence resulting from the lack of uniformity: courts convoluting the factors to apply.[248] By this it is meant that the lack of uniformity is causing courts to *sua sponte* read conditions and prerequisites into factors that should not exist and combine factors that should be weighed separately.[249] A prime

241. United States v. Richardson, 607 F.3d 357, 364 (4th Cir. 2010) (quoting United States v. Jarrett, 338 F.3d 339, 344 (4th Cir. 2003)); *see also* United States v. Black, 767 F.2d 1334, 1339 (9th Cir. 1985) (explaining two-factor inquiry); United States v. Smythe, 84 F.3d 1240, 1242 (10th Cir. 1996) (same).

242. United States v. Hardin, 539 F.3d 404, 419 (6th Cir. 2008).

243. For instance, the First Circuit's three-factor standard examines the government's role in originating the private search and the government's active control over the private search, two important factual circumstances ignored by the two-factor standard of the Fourth, Seventh, Ninth, and Tenth Circuits. *See Keith*, 37 F. Supp. 2d at 40.

244. *Compare* United States v. Livesay, 983 F.2d 135 (8th Cir. 1993), *with* United States v. Smythe, 84 F.3d 1240 (10th Cir. 1996).

245. *See Livesay*, 983 F.2d at 136 ("[A] search by a private party with no government knowledge or participation does not violate the [F]ourth [A]mendment.").

246. *Smythe*, 84 F.3d at 1242–43 (emphasis added).

247. *Compare Livesay*, 983 F.2d 135, *with Smythe*, 84 F.3d 1240.

248. *See* Orin S. Kerr, *How Important is the Uniformity of Federal Law?* VOLOKH CONSPIRACY (Sept. 29, 2009), https://volokh.com/2009/09/29/how-important-is-the-uniformity-of-federal-law/ [https://perma.cc/XM7C-YXLJ].

249. *See, e.g.*, United States v. Highbull, 894 F.3d 988, 992 (8th Cir. 2018) ("Even when government officials know of and acquiesce in a warrantless search, we have been unwilling to impute agency where the private actor was not 'motivated solely or even primarily by the intent to aid the officers' and where the government did not request the challenged search." (quoting United States v. Smith, 383 F.3d 700,

example is the Tenth Circuit, which has decided that that the second prong of its two-prong standard, i.e., did the private searcher intend to assist law enforcement, "does not mean that the court simply evaluates the private person's state of mind—whether his motive to aid law enforcement predominates."[250] Instead, the circuit court has explained, "this part of the test also requires that the court weigh the government's role in the search. A government agent must be involved either directly as a participant . . . or indirectly as an encourager" of the private search.[251] It is a profound interpretation (I would argue misinterpretation) of the private searcher's intent prong of the circuit's standard.[252] It is an interpretation that reads requirements into the prong that is unsupported by the plain language and the intended purpose of the prong.[253] It also flips the focus of the prong from the motivation of the private searcher to the participation of the government, which is clearly contrary to the language and intent of the prong.[254]

Uniformity is greatly needed for such an important issue.[255] Uniformity would bring consistency and prevent courts from redefining factors to fit particular situations.[256] A uniform standard, over time, would have well-defined factors with established boundaries and reach.[257]

---

705 (8th Cir. 2004))); United States v. Peterson, 294 F. Supp. 2d 797, 804–05 (D.S.C. 2003) ("With regard to the first factor, 'evidence of Government encouragement or participation is of course relevant in determining the existence of the first factor, i.e., Government knowledge and acquiescence sufficient to make a private person a Government agent.'" (quoting United States v. Jarrett, 338 F.3d 339, 345 n.3 (4th Cir. 2003))); United States v. Longo, 70 F. Supp. 2d 225, (W.D.N.Y. 1999) ("Knowledge and acquiescence, *simpliciter*, however, will be insufficient to attribute the private party's action to the government unless the circumstances demonstrate the government explicitly or implicitly instigated the search.").

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

251. *Id.*

252. *See id.*

253. *See* United States v. Black, 767 F.2d 1334, 1339 (9th Cir. 1985).

254. *See id.*

255. *See* Henry J. Friendly, *Indiscretion about Discretion*, 31 EMORY L.J. 747, 758 (1982).

256. *See* Martha Dragrich, *Uniformity, Inferiority, and the Law of the Circuit Doctrine*, 56 LOY. L. REV. 535, 542–43 (2010).

257. *See id.*

V. THE EXPANDED DEPUTIZATION STANDARD—A PROPOSAL

As the name reflects, the expanded deputization standard is not a complete abandonment of the deputization framework. The expanded deputization standard recognizes that its predecessor offers important benefits, namely that it "deals well with cases of overt influence by the state," and is good at "excluding certain types of 'spontaneous' private searches" that are fully divorced and distant from the government.[258] For these reasons, the expanded deputization standard incorporates many of the factors that populate existing deputization framework tests employed by courts.[259]

But the expanded deputization standard reforms the current approach by greatly expanding the number of factors a court is to consider.[260] The expansion is needed, as discussed earlier, because the current deputization framework tests used by courts are limited and too focused on the government and its role in the private search.[261] The expanded deputization standard appreciates that the role and influence of the private searcher is not only growing, but growing beyond the control and direction of the government.[262] This is particularly true when it comes to big tech companies, who are quickly becoming the principal providers of surveillance data and information to law enforcement.[263]

The expanded deputization standard consists of ten factors (discussed next). A number of the factors come from existing

---

258. *See* Brennan-Marquez, *supra* note 22, at 502–03.

259. *See* discussion *infra* Sections V.A–B (discussing case established elements of trespass for searches and government encouragement of the private action, respectively).

260. See *supra* Part IV, for a discussion of the flawed standard that needs expanding.

261. *See, e.g.*, United States v. Smythe, 84 F.3d 1240, 1242 (10th Cir. 1996) ("[A] search by a private citizen may be transformed into a government search implicating the Fourth Amendment 'if the government coerces, dominates or directs the actions of a private person' conducting the search or seizure." (quoting Pleasant v. Lovell, 876 F.2d 787, 796 (10th Cir. 1989))); United States v. Jarrett, 338 F.3d 339, 345 (4th Cir. 2003) ("Determining whether the requisite agency relationship exists 'necessarily turns on the degree of the Government's participation in the private party's activities.'").

262. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 532 (2005).

263. *See* Matt O'Brien & Michael Liedtke, *How Big Tech Created a Data 'Treasure Trove' for Police*, DENVER POST (Aug. 11, 2019), https://www.denverpost.com/2021/06/26/big-tech-data-police/ [https://perma.cc/6ST2-DAMJ].

standards applied by courts.[264] Some are inspired by, or taken directly from, the scholarship of Professors Burkoff and Brennan-Marquez that have greatly influenced this Article.[265] Some are factors that courts have considered even though they are not formally a component of the standard that courts apply.[266] Other factors are new creations that address the dangers posed by the modern private searcher.[267]

As with any multiple-factor test, the existence of any one factor would not necessarily transform a private search into a government action.[268] A court employing the expanded deputization standard would need to decide whether the totality of circumstances, after weighing all the factors, indicate that the private search was closely aligned with the government to be considered state action.[269] It is an approach that courts are well-experienced with when addressing Fourth Amendment-based challenges and issues.[270]

The expanded deputization standard consists of the following factors:

> (1) Did the private searcher trespass on the defendant's property or intrude into a constitutionally protected area?
> (2) Did the government instigate, incite, or otherwise encourage the private search?
> (3) Does the private searcher have a means of communicating with the state/law enforcement that is not readily available to the average person?
> (4) Was the government present for the private search?
> (5) Did the government/law enforcement provide the private searcher with any direction in conducting the search?
> (6) Did the private searcher receive, or expect to receive, any benefit for conducting the search or providing search material to law enforcement?

---

264. *See Smythe*, 84 F.3d at 1243.

265. *See* Burkoff, *supra* note 31; Brennan-Marquez, *supra* note 22.

266. *See* United States v. Keith, 980 F. Supp. 2d 33, 41 (D. Mass. 2013).

267. *See* Kerr, *supra* note 262, at 533.

268. *See, e.g.*, United States v. Black, 767 F.2d 1334, 1339 (9th Cir. 1985) (government's inducement of the private search alone did not transform search into a government one reached by the Fourth Amendment); *see also* United States v. Veatch, 674 F.2d 1217, 1221 (9th Cir. 1981) (wishing to assist law enforcement, standing alone, did not convert the private searcher into a government agent).

269. *See* Samson v. California, 547 U.S. 843, 848 (2006).

270. *See, e.g.*, United States v. Weikert, 504 F.3d 1, 3 (1st Cir. 2007); United States v. Weaver, 282 F.3d 302, 309 (4th Cir. 2002); United States v. Smythe, 84 F.3d 1240, 1243 (10th Cir. 1996).

(7) Has the private searcher previously provided search material to the government?
(8) Was assisting law enforcement a primary motivation of the private searcher?
(9) Did the government know the private searcher was going to conduct a search or seizure?
(10) Did the private searcher transfer information or data to assist law enforcement?

Each of these factors are discussed in detail next.

A. Did the Private Searcher Trespass on the Defendant's Property or Intrude into a Constitutionally Protected Area?

Trespass, i.e., whether the government trespassed on a defendant's property to effectuate a search or seizure, has been a staple basis for applying the Fourth Amendment since 1928.[271] Whether there was an intrusion into a constitutionally protected area has equally been long recognized as a basis for Fourth Amendment protection.[272] These two foundational Fourth Amendment principles combine to form a valuable factor for reviewing private surveillance—a factor that reflects the "longstanding protection for privacy expectations inherent in items of property that people possess or control."[273]

The value of this factor also flows from its reflection of whether the private searcher committed a crime to gather the material the

271. *See* Olmstead v. United States, 277 U.S. 438 (1928) (holding that the government wiretapping was not a Fourth Amendment search because there was no trespass on the defendant's property by the federal officers). It was a question whether the trespass doctrine survived following the Supreme Court's decision in *Katz v. United States*, 389 U.S. 347, 353 (1967) ("[T]he 'trespass' doctrine . . . can no longer be regarded as controlling."). The question was answered in 2012 by *United States v. Jones*, 565 U.S. 400, where the high court stated that *Katz* "did not erode the principle 'that when the government does engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.'" *Id.* at 407 (quoting United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J. concurring)).

272. *See* United States v. Jones, 565 U.S. 400, 407 (2012) ("*Katz* did not erode the principle 'that, when the government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.'" (quoting United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring))).

273. *See id.* at 414 (Sotomayor, J., concurring).

searcher obtained and provided to the state.[274] Trespass is a crime.[275] To not extend the protections of the Fourth Amendment to reach private searches done through criminal conduct is to make law enforcement and the courts "accomplices in [the] willful disobedience of the law."[276] To paraphrase Professor Burkoff, the state cannot with equanimity prosecute law breakers while simultaneously condoning, encouraging, and benefitting from law breaking.[277] When the state readily accepts illegally obtained evidence from private actors, it encourages such illegality.[278] Such encouragement constitutes "the unmistakable imprimatur of the State."[279] Indeed, it was "the imperative of judicial integrity" that caused the Supreme Court to cast the silver platter doctrine (which allowed evidence illegally obtained by state law enforcement to be admitted in federal trials) to the dustbin of history.[280] Just as the high court reasoned when the issue was illegal searches by state agents, "[c]rime is contagious," and courts countenancing criminal trespass to further government prosecutions, "breeds contempt for the law," "invites every man to become a law unto himself," and "invites anarchy."[281]

Some may criticize or reject this factor because of its unilateral focus on the private searcher.[282] This criticism misunderstands that under the proposed standard this factor alone cannot transform a private search into a government one.[283] This factor must be weighed with the other factors present and against those that are lacking.[284]

B. Did the Government Instigate, Incite, or Otherwise Encourage the Private Search?

This factor should be noncontroversial. It has long been recognized as a sign that private conduct crossed over into government

274. *See* Elkins v. United States, 364 U.S. 206, 223 (1960).
275. *See* N.Y. PENAL LAW § 140.05 (1969); MICH. COMP. LAWS § 750.552 (2013).
276. *See Elkins*, 364 U.S. at 223.
277. *See* Burkhoff, *supra* note 31, at 642 ("The State cannot with equanimity process law breakers while participating in [the] law breaking itself.").
278. *See id.*
279. *Id.* at 666.
280. *Elkins*, 364 U.S. at 222–23.
281. *See id.* at 223.
282. *See* Burkhoff, *supra* note 31, at 671.
283. *See id.* at 628.
284. *See id.* at 645.

conduct.[285] Understandably so. To not consider instigation by law enforcement as a key sign that a private searcher acted as a government agent would be to create a wide Fourth Amendment loophole that incentivized law enforcement to outsource the bulk of their search and seizure responsibility to private actors not restricted by the amendment.[286]

The importance of this factor is seen in *United States v. Young*.[287] In *Young*, hotel employees suspected that Young, a hotel guest, had stolen items from the room of another guest.[288] Hotel security used a master key to enter and search Young's room while he was not there.[289] During their search, hotel security did not find the reported stolen items, but they did find a backpack containing a firearm.[290] The discovery led hotel security to contact the police.[291] Before being informed about the firearm, the responding officer confirmed that Young had a criminal record.[292] After detaining Young in the hotel security office, the officer called his supervising sergeant for guidance.[293] The sergeant informed the officer that he could not enter and search Young's hotel room, but that "[hotel] security staff could enter a guest's room."[294] Subsequently, hotel security entered Young's room, while the officer waited in the hallway in a position that allowed him to see into the room.[295] The officer watched as hotel security opened Young's backpack to display the firearm in "plain sight" of the officer.[296] The trial court concluded that the second search

285. *See* United States v. Powell, No. 19-6461, 2020 WL 7054135, at *3 (6th Cir. Dec. 2, 2020) ("First, the police must [have] instigate[d], encourage[d], or participate[d] in the search."); *see also* United States v. Smythe, 84 F.3d 1240, 1243 (10th Cir. 1996) ("the requirement that the government agent must also affirmatively encourage, initiate or instigate the private [search]"); United States v. Lambert, 771 F.2d 83, 89 (6th Cir. 1985) ("First, the police must have instigated, encouraged or participated in the search.").

286. *See* United States v. Hardin, 539 F.3d 404, 417–20 (6th Cir. 2008) (finding apartment manager was government agent when police officers told him about the defendant's criminal record and suggested that manager use a water-leak ruse to enter the defendant's apartment).

287. *See generally* United States v. Young, 573 F.3d 711 (9th Cir. 2009).

288. *See id.* at 713.

289. *See id.* at 714.

290. *See id.*

291. *See id.*

292. *See id.* at 715.

293. *See id.*

294. *See id.*

295. *See id.*

296. *See id.*

conducted by hotel security "was done in collusion" with the police officer, and therefore the security guards were "state actors" during the second search.[297]

C. Does the Private Searcher Have a Means of Communicating with the State/Law Enforcement that Is Not Readily Available to the Average Person?

No court has directly or explicitly endorsed this factor. It is often subsumed by the examination into whether the government encouraged or instigated the private search. But ample cases addressing the private versus public search debate provide sufficient justification for the means of communication being a stand-alone factor.[298]

One such case is *United States v. Keith*, a child pornography case, which involved an emailed file from the defendant's computer being opened and examined by the National Center for Missing and Exploited Children (NCMEC), a nonprofit organization that "works in partnership" with federal prosecutors to combat the sexual exploitation and victimization of children.[299] After opening and analyzing the file, NCMEC concluded that it was child pornography, determined the internet protocol address from which the email with the file originated, and provided law enforcement with a report of their findings and investigation.[300]

---

297. *See* Appellee's Responding Brief at 13, United States v. Young, No. 07-10541, 2008 WL 2623357 at *12 (9th Cir. May 22, 2008); *see also* United States v. Young, 573 F.3d at 717 ("The Government does not dispute the district court's conclusion that [hotel] security should be considered state actors for the purposes of the second search of [Young's hotel room].").

298. *See e.g.*, United States v. Keith, 980 F. Supp. 2d 33, 36 (D. Mass. 2013).

299. *See id.* at 38. Two searches were at issue in the case. *Id.* at 36. The first search involved AOL's email scanning technology flagging a suspect file in an email of the defendant, and then AOL forwarding the file (without opening or viewing it) to the NCMEC. *Id.* at 37–38. The second search consisted of NCMEC opening and examining the forwarded file, determining that it consisted of child pornography, determining which internet protocol address the email with the file originated, and then providing law enforcement with a report of their findings and investigation. *Id.* The federal judge held that AOL did not act as an agent of the government in searching the defendant's email because the internet provider was not legally required to scan emails for child pornography, the government exercised no control over AOL's monitoring capabilities, and AOL's scanning was motivated solely by its private business interest to protect against its networks being used to transmit child pornography. *Id.* at 46–47.

300. *See id.* at 47–48.

The presiding federal trial judge held that NCMEC had acted as a government agent for Fourth Amendment purposes when it examined the defendant's email and the attached file.[301] While the judge's finding largely rested on other grounds, the judge took care to highlight how much contact there is between NCMEC and law enforcement and how that contact is through direct lines that are not available to the public.[302] As noted by the *Keith* judge, law enforcement members serve on NCMEC's various boards, law enforcement personnel provide NCMEC with on-site support services, and "NCMEC makes the results of its examination of suspected files available exclusively to federal and state law enforcement officials by means of a dedicated [virtual privacy network], accessible only to law enforcement personnel."[303]

As the *Keith* court recognized, a key hallmark of an agency relationship is the ability of the relationship partners to regularly and efficiently communicate and share information—that communication is a prerequisite for cooperation.[304] This is hardly a novel concept.[305] It is widely accepted that "an agency relationship may be implied by the conduct, actions, or *communications* of the principal."[306] Communication (frequency, substance, and ability) is regularly an inquiry focus where the existence of an agency relationship is at issue, such as whether an attorney–client relationship exists,[307] contract and

301. *See id.* at 41, 46–47.

302. The judge found that the First Circuit Court's three factor test, had been satisfied. *See supra* Section IV.C; *Keith*, 980 F. Supp. 2d at 41.

303. *See Keith*, 980 F. Supp. 2d at 41.

304. *See id.* at 40–41.

305. *See, e.g.*, *In re* Coupon Clearing Serv., Inc., 113 F.3d 1091, 1099 (9th Cir. 1997) (quoting Magnecomp Corp. v. Athene Co., 257 Cal. Rptr. 278, 283 (Cal. App. 2d Dist. 1989)) ("Proof of an agency relationship may be 'established by evidence of the acts of the parties and their oral and written communications.'").

306. *See* United States v. LaGrou Distrib. Sys., Inc., 466 F.3d 585, 591 (7th Cir. 2006) (emphasis added); *see also* Bridas S.A.P.I.C. v. Gov't of Turkm., 345 F.3d 347, 357 (5th Cir. 2003) ("An agency relationship may be demonstrated by 'written or spoken words or conduct, by the principal, communicated either to the agent (actual authority) or to the third party (apparent authority).'" (quoting Hester Int'l Corp. v. Fed. Republic of Nigeria, 879 F.2d 170, 176 (5th Cir. 1989))).

307. *See* Maples v. Thomas, 565 U.S. 266, 282-83 (2012) (attorneys' failure to inform Maples that the court had denied his petition and that he had forty-two days to appeal was a lack of communication that favored finding that the attorneys had "severed their agency relationship with Maples").

business disputes,[308] and assigning criminal liability.[309] Given this wide acceptance, there is no reason why communications (and the ability to communicate) should not be a factor of consideration when the question is whether a private searcher acted as a government agent for Fourth Amendment purposes.[310]

This factor is important, moreover, because it reaches activity that is of particular concern here: surveillance intermediaries, especially big tech companies, who share their customers' personal information and data with the government.[311] The big tech companies have direct lines of communication with the government, specifically in-house legal and other departments dedicated solely to handling government requests.[312] Apple, for instance, has a "team of dedicated professionals within [its] legal department who manage and respond to all legal requests received from law enforcement agencies globally."[313] Apple's team "responds to emergency requests globally on a 24/7 basis."[314] Through their lobbying efforts, moreover, the big tech companies have developed close relationships with law makers and regulators.[315] And

---

308. *See, e.g.*, Kolchinsky v. W. Dairy Transp., LLC, 949 F.3d 1010, 1013-14 (7th Cir. 2020) (finding that the "strongest facts in support of an agency relationship are that WD Logistics required Bentley to contact it at various times when carrying its loads, including a daily status call and a call upon delivery" but holding that it was not enough to establish an agency relationship here); MJR Int'l, Inc. v. Am. Arb. Ass'n, Inc., No. 09-4169, 2010 WL 3927310, at *1 (6th Cir. Sept. 21, 2010) ("The court also found that MJR had engaged in communications with Victoria's Collection that reasonably led Victoria's Collection to believe that Oxford was acting as MJR's agent."); Caldas & Sons v. Willingham, No. 95-60263, 1996 WL 459748, at *2 (5th Cir. July 22, 1996) ("A reasonable juror could disbelieve every statement in the 1984 letter and still conclude that Schlegel was attempting to create an agency relationship.").

309. *See, e.g.*, United States v. LaGrou Distrib. Sys., Inc., 466 F.3d 585, 591 (7th Cir. 2006) ("The district court also instructed the jury that to be qualified as an agent of a corporation, the person must be explicitly or implicitly authorized to act for the principal. Further, an agency relationship may be implied by the conduct, actions, or communications of the principal.").

310. *See, e.g.*, *Kolchinski*, 949 F.3d 1010, 1013 (7th Cir. 2020) (describing communication as the "strongest fact[] in support of an agency relationship").

311. *See Law Enforcement Support Program*, APPLE, https://www.apple.com/privacy/government-information-requests/ [https://perma.cc/7DC2-CG5J] (last visited Sept. 25, 2021).

312. *See id.*

313. *See id.*

314. *See id.*

315. *See* Lauren Feiner, *Google Ramps Up Lobbying and Facebook Outspends Big Tech Peers in the Third Quarter Ahead of Antitrust Revelations*, CNBC (Oct. 21, 2020), https://www.cnbc.com/2020/10/21/google-ramps-up-lobbying-facebook-outspends-peers-in-third-quarter.html [https://perma.cc/4288-5EHC].

due to their wealth, position in the commercial sector, and power, these companies have multiple lines of access and communications with the government (at all levels) that cannot be replicated or matched by the individual citizen.[316]

D. Was the Government Present for the Private Search?

Surprisingly, the more commonly accepted and applied standards for determining whether a private searcher acted as an instrument of the government do not explicitly include or address the presence of law enforcement during the search as a factor.[317] Some indirectly touch on the factor with prongs that explore whether law enforcement had prior knowledge of the private search; and some courts have held that the presence of law enforcement alone is insufficient government participation "to taint the otherwise private search."[318] But as a stand-alone factor, the government's presence is largely absent from accepted standards of analyzing Fourth Amendment challenges involving private searches.[319]

This absence is a mistake. The psychological effect of the presence of law enforcement has been acknowledged by the law in similar contexts.[320] The effect was key, for notable instance, in the Supreme Court establishing, in *Miranda v. Arizona*, the requirement that law enforcement inform suspects of their silence and attorney rights before being interrogated.[321] Writing for the majority in the seminal case, Chief Justice Warren used an appreciable portion of the opinion to explore and explain how law enforcement was trained to understand and manipulate "the principal psychological factor contributing to a successful interrogation," which is "privacy – [an officer] being alone with the person under interrogation."[322] The

316. *See id.* (explaining that in the third quarter of 2020, Facebook spent $4.9 million on lobbying, Amazon spent $4.4 million, Google spent $1.9 million on lobbying, and Apple spent $1.6 million).

317. *See supra* Section IV.C.

318. United States v. Krell, 388 F. Supp. 1372, 1374 (D. Alaska 1975); *see also* United States v. Walther, 652 F.2d 788, 792 (9th Cir. 1981) (stating that "[t]he presence of law enforcement" during a private search alone "has been held insufficient to implicate fourth amendment interests.").

319. *See* Miranda v. Arizona, 384 U.S. 436, 448 (1966).

320. *See generally id.*

321. *See id.* at 448 ("Again we stress that the modern practice of in-custody interrogation is psychologically rather than physically oriented.").

322. *See id.* at 449 (quoting INBAU & REID, CRIMINAL INTERROGATION AND CONFESSIONS 1 (1962)).

privacy of the interrogation environment, the Chief Justice acknowledged, "is created for no purpose other than to subjugate the individual to the will of his [law enforcement] examiner."[323]

The presence of law enforcement has a similar psychological effect in the private search circumstance.[324] The effect is on the private searcher who feels emboldened, encouraged, and authorized to trespass on another person's property because the witnessing officer(s) takes no steps to stop the trespass.[325] The effect also reaches the witnessing officer who eagerly awaits the results of the private search knowing that she has escaped the burden of obtaining probable cause or a warrant.[326]

In fact, when the private search involves a trespass the law enforcement officers present serve a "vital purpose: they [are] lookouts."[327] Law enforcement officers who are present for and witness a criminal trespass under the guise of a private search are indeed coconspirators in the trespass.[328] Arguably, they are also aiders and abettors of the trespass because their lack of action to disrupt or stop the criminal trespass facilitates and encourages the criminal conduct.[329] The psychological encouragement effect of the presence of law enforcement officers who eagerly await and accept the fruit of a crime, while taking no steps to stop the crime, cannot be ignored or divorced from consideration when the issue is if a private searcher acted as an instrument of the government in committing that crime.[330]

---

323. *See id.* at 457.

324. *See* United States v. Reed, 15 F.3d 928, 932 (9th Cir. 1994).

325. *See id.* ("However, in this case, Officer Rose and Sponholz's presence was more than 'incidental.' Watson would not have felt comfortable searching Reed's room had police officers not been standing guard in the doorway.").

326. *See id.* at 933.

327. *See id.* at 932.

328. *See id.*

329. *See* United States v. Perry, 643 F.2d 38, 46 (2d Cir. 1981) ("To convict a defendant as an aider and abettor the Government must show only 'that he in some sort associate himself with the venture, that he participate in it as in something that he wishes to bring about, that he seek by his action to make it succeed.'") (citation omitted); *see also* Rodriguez v. Davey, No. 12-CV-2260 TLN, 2017 WL 90355, at *15 (E.D. Cal. Jan. 9, 2017) ("Someone *aids and abets* a crime if he or she knows the perpetrator's unlawful purpose and he or she specifically intends to, and does in fact, aid, facilitate, promote, encourage, or instigate the perpetrator's commission of the crime."). *See generally* United States v. Partida, 385 F.3d 546, 560–61 (5th Cir. 2004) (finding sufficient evidence to support conviction of two police officers for aiding and abetting possessing illegal drugs with the intent to distribute).

330. *See supra* note 329 and accompanying text.

A comparison of two different approaches and outcomes in cases involving searches conducted by airline employees highlight the need for law enforcement presence to be a stand-alone factor. The first, *United States v. Newton*, started with Newton going to the Continental Airline lost baggage counter to report that her luggage did not arrive with her flight.[331] The Continental employee who took Newton's claim became suspicious when Newton refused to provide some identifying information, and she later returned to the counter with a man who advised Newton to not provide the employee with any information about herself or the lost luggage.[332] The employee relayed her suspicions to her supervisor and the Drug Enforcement Administration (DEA), which dispatched two local DEA agents to the airport.[333] The arriving agents informed the Continental employees that they (the agents) lacked sufficient probable cause to search Newton's luggage (which had since been located and retrieved by the employees).[334] Hearing this, the two Continental employees, in the presence of the two DEA agents, opened Newton's luggage, searched it, and retrieved from the contents a brown paper bag containing two plastic bags filled with a brown substance.[335] The employees handed the plastic bags to the DEA agents, who conducted a field test that showed the brown substance to be heroin.[336] Newtown was arrested while trying to leave the airport.[337]

Rejected by the district court, Newton's argument that the search of her luggage violated her Fourth Amendment rights because the Continental employees acted as government agents reached the Seventh Circuit.[338] In reversing the district court, the circuit court found that the facts clearly indicated that there "was joint participation by the private airline employees and the federal agents in the search and seizure sufficient to taint the use of the contraband seized" as evidence against Newton.[339] In reaching this conclusion, the appellate court stressed how the employees contacted the DEA for assistance and how the DEA honored the request by dispatching agents who not only witnessed the searching of Newton's luggage, but also

331. *See* 510 F.2d 1149, 1151 (7th Cir. 1975).
332. *See id.*
333. *See id.*
334. *See id.*
335. *See id.* at 1151–52.
336. *See id.* at 1152.
337. *See id.*
338. *See id.* at 1153.
339. *Id.* at 1154.

participated in the search by field testing contents of the luggage.[340] To the Seventh Circuit, "[t]his was not a 'hands-off' participation by the federal agents," but instead a joint search between private employees and government drug agents.[341]

With similar facts (and involving the same airline), the Tenth Circuit reached an opposite conclusion in *United States v. Leffall*.[342] Like *Newton*, this case started with a Continental Airlines air freight employee becoming suspicious about an incoming package due to the multiple inquiries he received from Leffall about the package.[343] When the package arrived, the airline employee decided to open it even though the box itself did not appear suspicious.[344] Before doing so, the employee took the package to the police station within the airport.[345] There the employee told the witnessing officer his concerns about the package, his intention to open and inspect the package's contents, and that the airline's company policy authorized him to do both, which the officer confirmed.[346] The officer then watched the airline employee open the package, remove the packing material wrapped around the sealed envelope inside, and then open the sealed envelope to discover sheets of fraudulent securities (for which Leffall was convicted of possessing).[347]

The Tenth Circuit affirmed the lower court's holding that the circumstances of the search did not convert the Continental Airline employee into a government agent.[348] The appellate court endorsed the district court's finding that the witnessing officer was "neither 'a direct participant or an indirect encourager of the search,'" and that the airline employee had a "legitimate independent motivation" for searching the package separate from assisting law enforcement.[349]

340. *See id.* at 1153.
341. *See id.*
342. *See* United States v. Leffall, 82 F.3d 343, 347 (10th Cir. 1996).
343. *See id.* at 345.
344. *See id.* at 345–46.
345. *See id.* at 346.
346. *See id.*
347. *See id.* 346–47.
348. *See id.* at 349.
349. *See id.* at 347 (explaining district court's findings); *see also id.* at 349 ("But under the facts of this case, it is not difficult to uphold the district court's ruling that [the airline employee] acted with independent aim and not as a surrogate for the government.").

With factual chains of events so similar, it is perplexing that the two circuit courts reached such different conclusions.[350] However, it is important to know that the divergent outcomes did not turn on the presence of law enforcement during the search, but rather how the Tenth Circuit in *Leffal* interpreted the second prong of its standard, i.e., the intent of the private searcher to assist law enforcement.[351] Indeed, if presence of law enforcement was a universally-recognized stand-alone factor of consideration, it is likely the airline employees in both *Leffal* and *Newton* would have been found to be agents for the government.[352]

In both cases the airline employee invited the presence of law enforcement *because they were law enforcement.*[353] Law enforcement officers and agents, "whether uniformed or not, necessarily exert some moral and administrative authority."[354] This psychological effect reaches the private searcher in that it emboldens the private searcher that what she is doing is proper, legal, and supported by the state, and therefore, the community as well. This includes the airline employees in *Leffal* and *Newton*, who did not seek the presence of the officers and agents for a reason unrelated to their status as law enforcement.[355] By conducting the search in front of the officers and agents, the airline employees were implicitly seeking and obtaining the approval and support of law enforcement to conduct the search, otherwise they could have simply conducted the search outside the presence of law enforcement and provided the results and fruits of the search afterward.[356]

If presence was a stand-alone factor considered by the Tenth Circuit in *Leffall*, the court's analysis would look very different and lean closer to the court's analysis *Newton*.[357] The airline employee's search of Leffall's property was done *in a police station*, and only *after* the witnessing officer confirmed that the airline's policy authorized

350. *See id.* at 349; *see also* United States v. Newton, 510 F.2d 1149, 1154 (7th Cir. 1975).

351. *See Leffall*, 82 F.3d at 347 ("Only the second prong is at issue in the instant appeal, as the government concedes it knew of and acquiesced in the search"). The problems with the Tenth Circuit's interpretation of the second prong in this case has been discussed earlier, *see supra* Section IV.C.

352. *Compare Leffall*, 82 F.3d at 346, *with Newton*, 510 F.2d at 1151.

353. *See Leffall*, 82 F.3d at 346; *see also Newton*, 510 F.2d at 1151.

354. *See* United States v. Zamoran-Coronel, 231 F.3d 466, 469 (8th Cir. 2000).

355. *See Leffall*, 82 F.3d at 346; *see also Newton*, 510 F.2d at 1151.

356. *See Leffall*, 82 F.3d at 346; *see also Newton*, 510 F.2d at 1151.

357. *See Leffall*, 82 F.3d at 347.

the employee to search the property.[358] This is as close to an official sanctioning of a private search as one can get without law enforcement explicitly asking a private person to conduct a search. It certainly weighs in favor of finding that the airline employee acted as a government agent, than not.[359]

E. Did the Government/Law Enforcement Provide the Private Searcher with Any Direction in Conducting the Search?

Arguably, this factor is subsumed by the instigate, incite, or encouragement factor. But it is the view here that providing direction needs to be a stand-alone factor because providing direction more closely aligns a law enforcement officer with being a participant in a private search, than providing encouragement.[360]

United States v. Lichtenberger illustrates the point.[361] After learning that the defendant had previously been convicted of child pornography offenses, his girlfriend had police remove Lichtenberger from the residence they shared.[362] Afterward, the girlfriend retrieved Lichtenberger's laptop, bypassed its password protection, searched it, and found numerous disturbing images of child pornography.[363] She subsequently called the police, and when the officer arrived, she explained her discovery and how she had accessed the laptop.[364] The officer then directed the girlfriend to boot up the computer and show him the child pornography images that she had discovered.[365]

Lichtenberger conceded that the first search that his girlfriend did alone was purely private action not reached by the Fourth Amendment.[366] But he did move to suppress the fruits of the second search of the laptop, i.e., the search done by his girlfriend at the direction of the responding officer, which the trial court granted.[367] The second search "constitutes government action," according to the court, because the officer gave Lichtenberger's girlfriend "several

358. *See id.* at 346.
359. *See id.*
360. *See* United States v. Lichtenberger, 19 F. Supp. 3d 753, 759 (N.D. Ohio 2014).
361. *See id.*
362. *See id.* at 754–55.
363. *See id.* at 755.
364. *See id.*
365. *See id.*
366. *See id.* at 758.
367. *See id.*

directions" to facilitate and guide the search.[368] These directions included directing her to boot-up the laptop and show him particular images.[369] The court stressed that because the officer was not physically handling or touching the laptop, "he would have not seen the [offending] images without instructing [the girlfriend] to show them to him."[370] Through the officer's instructions, according to the court, the girlfriend "became an agent of the officer."[371]

Although the court focused on the effect of the officer's direction on Lichtenberger's girlfriend, it is clear that the court also understood that the officer's directing of the second search pulled the officer closer to, if not squarely in, the zone of participation. The court was explicit, for instance, that the officer "was actively directing [the search], not merely passively viewing."[372] The court remarked further that the officer's directives to the girlfriend to open and reboot the laptop, were "no different than if she had been told to open dresser drawers, a closet, or a physical file cabinet. Both activities were at the direction and subject to the control of the officer."[373]

Lichtenberger shows that while providing direction is arguably encouraging and inciting a private search, there is significant value in a separate examination into whether the encouragement takes the form of direction.[374] The value stems from understanding that encouragement in the form of direction blurs the line between participant and witness in a way that encouragement absent direction does not.[375]

F. Did the Private Searcher Receive, or Expect to Receive, Any Benefit for Conducting the Search or Providing Search Material to Law Enforcement?

To reiterate, a primary goal of this proposed standard is to expand the number of factors that focus on the private searcher's intent, role, and expectation. This factor is in line with that goal. It is

368. *Id.*
369. *See id.*
370. *Id.* at 758–59.
371. *Id.*at 759.
372. *Id.*
373. *Id.* at 759.
374. *See id.*
375. *See, e.g.*, United State v. Hardin, 539 F.3d 404, 417–20 (6th Cir. 2008) (finding an apartment manager acted as a government agent when police officers told him about the defendant's criminal record and suggested that the manager use a water-leak ruse to enter and search the defendant's apartment).

a benefit-focused factor that is the flip side of the regularly accepted factor of whether the government encouraged or enticed a private search. This flip side is needed because an expectation of benefit can exist without government persuasion to conduct a private search—that a private searcher can expect a benefit even though the government did not suggest a benefit was forthcoming. In the absence of this factor, the government persuasion factor simply does not capture a motivation that goes to the heart of the public-versus-private search issue. The Ninth Circuit recognized this as much in *United States v. Walther*, when it affirmed the trial court's finding that an airline employee's search of the defendant's luggage constituted a government search.[376] The finding was made, in large part, because the employee had conducted the search "with the expectation of probable reward from the [Drug Enforcement Agency]."[377] In comparison, when the Seventh Circuit faced a similar circumstance, it found that an airline's employee had not acted as a government agent because the employee opened the defendant's luggage for the business purpose of finding contact information for the defendant (in order to return lost luggage), and not in expectation of a reward for assisting law enforcement.[378]

Allowing this factor to reach a private searcher who expects a benefit even without the promise or suggestion of a reward from the government, would still allow courts to distinguish private searches where a benefit was not even contemplated. This proposed factor would have had no determinable impact, for instance, in *United States v. Bulgier*, where it was held that an airline's employee had not acted as a government agent because the employee searched the defendant's luggage for the business purpose of finding contact information in order to return the lost luggage.[379] Indeed, this proposed factor likely would have provided additional grounds to support the court's conclusion.

---

376. *See* 652 F.2d 788, 792–93 (9th Cir. 1981).

377. *See id.* at 792 (providing the other basis for the Ninth Circuit's finding that the employee was acting as agent of the government was the employees "extensive contact" with the DEA in the past as a paid informant).

378. *See* United States v. Bulgier, 618 F.2d 472, 473, 477 (7th Cir. 1980) (holding that an airline's employee had not acted as a government agent because the employee opened the defendant's luggage for the business purpose of finding contact information (in order to return lost luggage), and not in expectation of a reward for assisting law enforcement).

379. *See id.* at 473, 477.

G. Has the Private Searcher Previously Provided Search Material to the Government?

Even though it not explicitly included in the various standards used by courts, this is another factor that some courts understand is important when weighing whether a private searcher acted as an agent or instrument of the government.[380] One such case is *United States v. Walther*, where the Ninth Circuit affirmed the lower court's finding that an airline employee acted as a government agent in searching the defendant's luggage because, in large part, of the extensive history of the airline employee searching customers' luggage to assist law enforcement.[381] What the circuit court understood was that with a shared history comes familiarity and expectations.[382] When a private searcher has previously been applauded, rewarded, or simply not punished for trespassing or intruding on another's property, she becomes comfortable and emboldened to do so again.[383] The history becomes an incentive, rather than a disincentive or deterrent, for such acts.[384]

The particular facts of a case may cause this factor to overlap with the benefit factor (i.e., whether the private searcher expected to, or did receive a benefit from the government).[385] As in *Walther*, where there is a history of extensive contact there likely will be a corresponding history of benefits received.[386] However, it is important that this factor stands alone because there are circumstances that do not conform to this expectation—that is, private searchers who have previously provided the fruits of their private search to the government without reward or the expectation of one.[387]

380. *See Walther*, 652 F.2d at 792.

381. *See id.* at 790, 793 (noting that the airline employee had been a confidential informant for the DEA for four years, during which provided the DEA with information eleven times in return for $800 total).

382. *See id.* at 792–93.

383. *See generally id.*

384. *See id.* at 793.

385. *See supra* Section V.F.

386. *See Walther*, 652 F.2d at 793 (discussing the extensive contact between the airline employee and the government, the court noted that the employee "had been rewarded for providing drug-related information in the past").

387. *See, e.g.*, United States v. Keith, 980 F. Supp. 2d 33, 41 (D. Mass. 2013) (explaining how the National Center for Missing and Exploited Children has a "partnership" with the government where it provides the results of its private searches to serve the public interest).

H. Was Assisting Law Enforcement a Primary Motivation of the Private Searcher?

Whether assisting the government motivated a private search is widely recognized as a key factor when determining whether a private searcher is a government agent for Fourth Amendment purposes.[388] In *Knoll Associates, Inc. v. Federal Trade Commission*, for example, the Seventh Circuit affirmed a finding that a disgruntled employee's stealing of company documents and providing them to the FTC to aid the agency's prosecution of the company constituted a government search reached by the Fourth Amendment.[389]

The proposed standard takes this accepted factor and adjusts it slightly so that the factor is no longer unduly narrow. Instead of measuring whether the goal of assisting the government is *the* primary motivation, this proposed factor measures whether assisting the government is *a* primary motivation.[390] The slight adjustment has significant implications, namely it broadens the scope of this motivation factor. The broadening recognizes that motivations are rarely easily segregated and more often are intertwined and convoluted.[391] Rare is the case where a private searcher's sole motivation is to assist the government.[392] This is particularly true when the private searcher is a company or corporation, who by its nature

388. *See* discussion *supra* Section IV.C; *see also* United States v. Silva, 554 F.3d 13, 18 (1st Cir. 2009) ("[T]he extent to which the private party aims primarily to help the government."); United States v. Souza, 223 F.3d 1197, 1201 (10th Cir. 2000) ("[W]hether the party performing the search intended to assist law enforcement efforts or to further his own ends."); United States v. Krell, 388 F. Supp. 1372, 1375 (D. Alaska 1975) (holding that an airline employee acted as a government agent in searching the defendant's property because, in large part, "the only purpose of the search was to further a government investigation").

389. 397 F.2d 530 (7th Cir. 1968).

390. *Cf. id.* at 533–34 (reasoning the private searcher "stole the documents for the purpose of assisting" the government agency).

391. *See* United States v. Leffall, 82 F.3d 343, 347 (10th Cir. 1996) ("Almost always a private individual making a search will be pursuing his own ends—even if only to satisfy curiosity—although he may have a strong intent to aid law enforcement.").

392. *See, e.g.*, Corngold v. United States, 367 F.2d 1, 5–6 (9th Cir. 1966) (finding that search was a "joint endeavor" reached by the Fourth Amendment because the private searcher's sole purpose was to assist law enforcement); United States v. Keith, 980 F. Supp. 2d 33, 40–41 (D. Mass. 2013) (same).

have profit and self-protection (i.e., protecting itself from being used to facilitate criminal activity) as perennial primary motivations.[393]

Even when a key motivation is assisting law enforcement, it can come from a personal place—such as moral conviction—that courts can seize upon to hold that the factor weighs against finding that the private searcher acted as a government agent.[394] This is what the Seventh Circuit did when it held that a mall security guard was not acting as a government agent when he searched the defendant, who was suspected of theft, and recovered a firearm.[395] According to the circuit court, that mall security and the local police shared the goal of preventing crime was a "happy coincidence" that did not transform the mall security officer who conducted the search into an arm of the government.[396]

The Seventh Circuit's approach underscores why this proposed factor (and the change it reflects) is surely needed.[397] As the Ninth Circuit recognizes, "if crime prevention could be an independent private motive, searches by private parties would never trigger Fourth Amendment protection."[398]

The commonality of concurrent and comingling motivations is recognized by well-accepted agency principles.[399] As the Tenth Circuit has noted, "[n]either has the common law [concerning agency relationships] traditionally required that the agent be an altruist, acting without any intent of advancing some personal interest along the way (like monetary gain).").[400] In other words, a private searcher's personal interest, especially if it is financial gain, does not alone defeat a finding of an agency relationship.[401]

The transformation of this factor to *a* primary motivation from *the* primary motivation is necessary to reach a particular brand of private searcher: the extremist. For the extremist, the motivation to assist law enforcement will always be subordinate to that motivation that drives the person to be an extremist. For the white supremacist

393. *See* United States v. Smith, 383 F.3d 700, 705 (8th Cir. 2004) (noting that when commercial carriers such as Federal Express inspect suspicious packages for contraband they are motivated by their own desire and responsibility to not transport contraband as well as a desire to help law enforcement).

394. *See* United States v. Shahid, 117 F.3d 322, 326 (7th Cir. 1997).

395. *See id.* at 326–28

396. *Id.* at 327.

397. *See id.*

398. United States v. Reed, 15 F.3d 928, 932 (9th Cir. 1994).

399. *See* United States v. Ackerman, 831 F.3d 1292, 1301 (10th Cir. 2016).

400. *Id.*

401. *See id.*

extremist, for instance, it is his racial animus toward people of color and his desire to hurt them; assisting law enforcement will always be a secondary motivation for him.

The expansion advocated here, however, is not limitless and without boundaries.[402] By requiring that assisting the government be *a primary motivation*, the proposed standard protects against a finding of government action based on a tenuous, distant, or nonexistent desire to assist law enforcement.[403]

I. Did the Government Know the Private Searcher Was Going to Conduct a Search or Seizure?

Courts have long recognized whether the government had prior knowledge of the private search is a key factor for determining if a private actor acted as a government agent triggering Fourth Amendment protections.[404] The Supreme Court relied on this factor when it decided *Walter* and then *Jacobsen*, two seminal cases concerning the private-versus-government search question.[405]

That said, some courts have taken the position that knowledge by the government holds no weight in converting a private search into a government search absent encouragement by the government.[406] The

---

402. *See, e.g.*, United States v. Stevenson, 727 F.3d 826, 830–31 (8th Cir. 2013) (holding that an agency relationship did not exist when a phone company's primary motivation was business related).

403. *See, e.g.*, *id.* at 830–31 (holding that internet service provider's scanning of emails for child pornography was motivated by the company's "business reasons: to detect files that threaten the operation of [the company's] network" far more than to assist law enforcement); United States v. Auler, 539 F.2d 642, 647–48 (7th Cir. 1976) (finding telephone company's interceptions of defendant's phone activity was not an illegal government search because it was done to determine if the defendant was bypassing the company's billing system and to protect the company's equipment).

404. *See, e.g.*, United States v. Jarrett, 338 F.3d 339, 344 (4th Cir. 2003) ("(1) whether the Government knew of and acquiesced in the private search"); United States v. Livesay, 983 F.2d 135, 136 (8th Cir. 1993) ("[A] search by a private party with no government knowledge or participation does not violate the [F]ourth [A]mendment").

405. *See* Walter v. United States, 447 U.S. 649, 662 (1980) (stating that the Fourth Amendment does not reach private searchers who are "not acting as an agent of the Government or with the participation or knowledge of any government official."); *see also* United States v. Jacobsen, 466 U.S. 109, 113 (1984) (holding that the Fourth Amendment does not extend to searches or seizures conducted by private individuals without the government's knowledge or participation).

406. *See* United States v. Souza, 223 F.3d 1197, 1201–02 (10th Cir. 2000); *see also* Jarrett, 338 F.3d at 345 ("In seeking to give content to this [government

Tenth Circuit is one such court having said that "knowledge and acquiescence . . . *encompass* the requirement that the government agent must also affirmatively encourage, initiate or instigate the private action."[407] To the Tenth Circuit and like-minded courts, more than just knowledge is needed because the government is "under no duty to discourage private citizens from conducting searches of their own volition."[408]

Such a sentiment would be unremarkable and benign if it was limited to searches that do not violate the law (e.g., trespass) or invade the privacy of another in a way that would be illegal if done by the government. Absent such a caveat, the sentiment encourages the very lawlessness, vigilantism, and devaluing of the judiciary that courts sought to avoid by abandoning the silver-platter doctrine that allowed the admission into federal trials evidence unlawfully obtained by state agents.[409] As discussed at various points earlier, private searches often constitute an illegal trespass involving another's property.[410] If law enforcement has prior knowledge of a crime, it has a duty to discourage or prevent the crime from occurring.[411] Purposely disregarding this duty in order to profit from the illegal trespass undermines the integrity of law enforcement, equally undermines trust in law enforcement, and puts the community at risk.[412] It is simple and plain—when the government does not discourage unlawful and privacy intrusive conduct, it incentivizes and encourages such conduct.[413]

---

knowledge] factor, we have required evidence of more than mere knowledge and passive acquiescence by the Government before finding an agency relationship.").

407. United States v. Smythe, 84 F.3d 1240, 1243 (10th Cir. 1996) (emphasis added).

408. *Souza*, 223 F.3d at 1202.

409. *See* Elkins v. United States, 364 U.S. 206, 223 (1960) ("Crime is contagious. If the government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy."); *see also* Burkoff, *supra* note 31, at 643 ("Eliminating this distinction [between private and government searches] would not only deter the violation of individual rights, but would eliminate the sordid specter of the State seeking criminal convictions based in whole or in part upon evidence seized by illegal—even criminal—acts.").

410. *See, e.g.*, United States v. Sweeney, 821 F.3d 893, 899–900 (7th Cir. 2016).

411. *See* Burkoff, *supra* note 31, at 670.

412. *See id.*

413. *See generally id.* (arguing that private actors will make unlawful searches or seizures if this conduct is not discouraged by government); United States v. Koenig, 856 F.2d 843, 850 (7th Cir. 1988) ("[I]t is every citizen's civic duty to do what he can to aid in the control and prevention of criminal activity, and 'it is no part of the policy

J. Did the Private Searcher Transfer Information or Data to Assist Law Enforcement?

Clearly this factor is targeted at the big tech surveillance intermediaries who have become law enforcement's favorite outsourced supplier of surveillance information and data.[414] Professor Brennan-Marquez is the source for it.[415] As the professor notes, guided by the agency framework, courts have historically focused on whether the private search was done to assist law enforcement.[416] For the traditional (no or low tech) private searcher this is understandable and reasonable (which is why it remains a factor in this proposed standard).[417] But for the big tech surveillance intermediaries this approach fails to appreciate that these companies are *constantly* amassing and searching our data for non-law enforcement purposes, e.g., targeted advertisements; and as these companies grow as surveillance intermediaries, user data will increasingly end up in the government's hands.[418] Therefore, for determining when surveillance intermediaries act as a government agent, the "important moment is not data collection[,] it is the transfer of data to law enforcement."[419] This also explains why this factor is needed when the proposed standard already includes as a factor whether a primary motivation of the private searcher was to assist law enforcement.[420] This factor, in other words, focuses on the private searcher's motivation at the time of the transfer of information to law enforcement.[421] If the private searcher relays another's information to the government "*for the explicit purpose of assisting police*, that should be a tick in [the] column of state action."[422]

---

underlying the Fourth and Fourteenth Amendments to discourage citizens from aiding to the utmost of their ability in the apprehension of criminals.'" (quoting Coolidge v. New Hampshire, 403 U.S. 443, 488 (1971))).

414. *See* Brennan-Marquez, *supra* note 22, at 516.

415. *See id.* at 517 (identifying "whether the data-transfer was aimed to assist law enforcement" as an element in determining "whether law enforcement infrastructure has been extended" for Fourth Amendment purposes).

416. *See id.* at 516.

417. *See id.* at 486–89, 517.

418. *See* United States v. Jacobsen, 466 U.S. 109, 119 (1984).

419. Brennan-Marquez, *supra* note 22, at 516–17.

420. *See id.* at 516–17.

421. *See id.*

422. *Id.* at 517.

K. Criticism of Proposed Standard

The first expected criticism of the proposed expanded deputization standard is that it contains too many factors, which makes it complicated and burdensome to apply. The response to this critique is not to argue that the standard is not complicated or not a long list of factors. Instead, the response is that an extensive list of factors is needed because the question itself—when does a private search constitute government action reached by the Fourth Amendment—is complicated, intricate, and holds significant consequences and implications.[423] In short, complexity is needed to address such a complicated and sophisticated issue.

We are seeing the problems with courts taking shortcuts to address the issue.[424] The performance history of the currently employed standards, which consist of a small number of factors (at most three factors), highlights the need for a new and more extensive approach.[425] As discussed earlier, the current standards and tests have failed to establish and maintain a consistent and uniform approach to the issue.[426] They have created a circumstance where the outcome—whether a private search will be deemed government action—largely depends on where (in which court) a challenge is heard.[427] Such a patchwork of outcomes is something that should be avoided when it comes to this important subject: the relationship between individual privacy interests and the government.[428]

Acceptance of the complexity of the proposed standard should not spell its doom. Courts have the experience and capability to employ this new standard and its extensive list of factors.[429] Indeed, there is a long history of courts applying equally complex and extensive standards.[430] The *Daubert* standard for determining the admissibility of expert witness testimony is a particularly prominent example.[431] The *Daubert* multi-factor test replaced a simple, one factor

423. *See id.* at 487–88, 498.

424. *See id.* at 503 (illustrating some of the different approaches taken by circuit courts).

425. *See id.*

426. *See id.* at 488–89.

427. *See id.* at 503.

428. *See id.* at 487–88, 490, 504, 510, 519.

429. *See* Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 597–98 (1993).

430. *See id.* at 597–98.

431. *See generally* Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 579–98 (1993) (establishing the standard and factors); Kumho Tire Co. v. Carmichael, 526

test (i.e., whether an expert's method is generally accepted in the scientific community), and ushered in a "far more complex and daunting task in a post-*Daubert* world than before."[432] While "complex and daunting"[433] the multi-factored *Daubert* test is now understood and accepted as an important tool for trial courts to exercise their gatekeeping duty to ensure the reliability and relevancy of expert testimony, which "can be both powerful and quite misleading."[434] As simply put by the Eleventh Circuit, "[t]he importance of *Daubert*'s gatekeeping requirement cannot be overstated."[435]

Criminal cases are not excluded from the long history of courts applying complex multi-factored tests and standards.[436] A notable example is federal sentencing, where 18 U.S.C. § 3553(a) requires sentencing judges to weigh and analyze seven different factors, including one ("the need for the sentence imposed") that has an additional four separate factors for the court to consider.[437] Many of § 3553(a)'s sentencing factors are complicated individually, and require a sentencing judge to explore abstract concepts such as "adequate deterrence" and the "seriousness" of an offense.[438] It is a challenge that trial courts meet every day.[439] Just look at the 76,565 sentencings that occurred in fiscal year 2019, which translates to nearly 210 sentencings each day of that fiscal year.[440]

Federal sentencings provide another illustrative example: United States Sentencing Guideline § 3B1.2 and its multi-factored standard federal judges use when determining whether a defendant is entitled to a mitigating role reduction provided by the provision.[441] A key application note to the guideline provision instructs a sentencing judge to conduct a fact-based "totality of circumstances" analysis guided by

---

U.S. 137, 141 (1999) (holding that the *Daubert* standard applies to all expert testimony and is not limited to scientific expert testimony).

432. *See* Daubert v. Merrell Dow Pharms., Inc., 43 F.3d 1311, 1315 (9th Cir. 1995).

433. *Id.*

434. *Daubert*, 509 U.S. at 595; *see also* United States v. Frazier, 387 F.3d 1244, 1260 (11th Cir. 2004) (discussing the importance of *Daubert*'s gatekeeping function).

435. *See Frazier*, 387 F.3d at 1260.

436. *See* 18 U.S.C. § 3553(a)(2) (2018).

437. *See id.* (listing the four "needs" a defendant's sentence must fulfill).

438. *Id.* at § 3553(a)(2)(A)–(a)(2)(B).

439. *See* GLENN R. SCHMITT & AMANDA RUSSELL, U.S. SENT'G COMM'N, FISCAL YEAR 2019 OVERVIEW OF FEDERAL CRIMINAL CASES 1 (Apr. 2020).

440. *Id.*

441. *See* U.S. SENT'G COMM'N, GUIDELINES MANUAL § 3B1.2 (2018).

five enumerated factors.[442] In fact, the history of § 3B1.2's factors is particularly instructive for the purposes here.[443] An amendment passed by the United States Sentencing Commission in 2015 added the five-factor list to § 3B1.2.[444] The amendment was motivated by a Commission study of cases involving low-level offenders and the application of the guideline provision.[445] The study found that "[o]verall . . . that mitigating role is applied inconsistently and more sparingly than the Commission intended."[446] Drug and fraud cases in particular, the study revealed, experienced wide inconsistencies in application.[447] The study persuaded the Commission to amend § 3B1.2 with the five-factor list because "providing a list of factors will give the courts a common framework for determining whether to apply a mitigating role adjustment (and, if so the amount of the adjustment) and will help promote consistency."[448] The expanded deputization standard would achieve the same goals: provide a common framework and promote consistency.[449] As discussed earlier, both are needed when it comes to Fourth Amendment challenges to private searches.[450]

The second expected criticism is really more of a question, that is, after the expanded deputization standard is applied, then what happens? The answer is rather straightforward and simple. If a trial court determines that the factors weigh in favor of finding that a private searcher was *not* acting as a government agent or instrument, then the defendant's Fourth Amendment challenge fails (and the motion to suppress is denied).[451]

However, if a court finds the opposite, i.e., the factors weigh in favor of finding the private search was government action, then the challenge proceeds along the same path as any other Fourth Amendment-based challenge.[452] The next immediate next step,

442. *See id.* at § 3B1.2 cmt. 3(C); *see also* United States v. Quintero-Leyva, 823 F.3d 519, 523–24 (9th Cir. 2016) (reversing and remanding because it was unclear if the sentencing judge considered all the factors listed in § 3B1.2).

443. *See generally Amendment 794*, U.S. SENT'G COMM'N, https://www.ussc.gov/guidelines/amendment/794 [https://perma.cc/6QPL-VURQ] (last visited Oct. 25, 2021).

444. *See id.*; *see also Quintero-Leyva*, 823 F.3d 519, 522 (9th Cir. 2016).

445. *See* U.S. SENT'G COMM'N, *supra* note 443.

446. *Id.*

447. *See id.*

448. *Id.*

449. *See supra* Section IV.C.

450. *See* discussion *supra* Section IV.C.

451. *See supra* Part III.

452. *See supra* Part III.

therefore, is the first step in Fourth Amendment challenges lacking the private searcher issue: a *Katz* inquiry to determine whether the private searcher's intrusion (while acting as a government instrument or agent) violated the defendant's expectation of privacy, and therefore constituted a search subject to the Fourth Amendment's reasonableness requirement.[453]

If the challenge survives *Katz* scrutiny, then the next step in the regular course is for the reviewing court to weigh whether the private search (constituting government action) was "reasonable" under the Fourth Amendment.[454] If the search is deemed reasonable, then there is no Fourth Amendment problem since the amendment protects only against unreasonable searches and seizures.[455] The reasonableness of a search "is determined by assessing on one hand, the degree to which [the search] intrudes upon an individual's privacy and, on the other, the degree to which [the search] is needed for the promotion of legitimate government interests."[456] It involves a court weighing "all of the circumstances surrounding the search or seizure and the nature of the search or seizure itself."[457] The general rule is that a search is unreasonable unless accompanied by a warrant that is supported by probable cause, or in the cases of warrantless searches, a recognized exception applies.[458] It is the exception zone where most, if not all, private searches that survived the framework proposed here would be litigated.[459]

---

453. *See* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (establishing two-prong *Katz* test: (1) did the defendant exhibit a subjective expectation of privacy in the item/area searched; and (2) is that expectation one that society is prepared to recognize as reasonable); *see also* United States v. Ishmael, 48 F.3d 850, 853 (5th Cir. 1995) ("As in any Fourth Amendment surveillance case, our analysis begins with *Katz*."); Widgren v. Maple Grove Twp., 429 F.3d 575, 578 (6th Cir. 2005) ("A search is defined in terms of a person's 'reasonable expectation of privacy' and is analyzed under a two-part test first penned in *Katz*.").

454. *See* United States v. Sczubelek, 402 F.3d 175, 182 (3d Cir. 2005) (citing *Skinner v.Railway Labor Executives' Ass'n*, 489 U.S. 602, 619 (1989).

455. *See id.*

456. United States v. Knights, 534 U.S. 112, 112–13 (2001) (citing Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

457. *See* Skinner v. Railway Labor Execs.' Assoc., 489 U.S. 602, 619 (1989) (citing United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985); *see also* United States v. Reid, 929 F.2d 990, 992 (4th Cir. 1991).

458. *See Skinner*, 489 U.S. at 619.

459. *See Reid*, 929 F.2d at 992 (explaining how the Supreme Court recognizes an exception zone for warrantless searches).

L. Applying the Expanded Deputization Standard

Having explained the expanded deputization standard and explored how it would apply in the course of Fourth Amendment challenges, the next natural question is can it make a difference? The case of *United States v. Smith* shows that it can.[460]

Smith started with a California police officer participating in a parcel (drug) interdiction operation at a Federal Express facility.[461] The officer removed a "suspicious looking package" from the conveyor belt, then handed it to a detective on sight who had a canine sniff performed on the package.[462] The police dog alerted to the package, indicating that it likely contained illegal drugs.[463] The detective then took the package to the Federal Express facility manager and told her that he suspected the package contained drugs.[464] When the manager asked if the detective wanted her to open the package to observe its contents, the detective responded, "if she wanted to open it[,] that would be fine."[465] Hearing that, the manager opened the package and, after searching its contents, found a smaller package of a suspected cocaine base (crack).[466] After the package and its contents were examined and photographed by the police, it was resealed and delivered to Smith, its intended recipient, who was subsequently charged with possession with the intent to distribute more than fifty grams of crack cocaine.[467]

Smith moved to suppress the cocaine evidence, partly on the grounds that his Fourth Amendment rights were violated because the Federal Express facility manager acted as a government agent when she opened and searched the package without a warrant.[468] The district

460. *See* 383 F.3d 700, 705–06 (8th Cir. 2004) (applying the normal deputization standard to hold that a private individual was not acting as an agent of the government).

461. *See id.* at 703 (stating that California police officer participated in "parcel interdiction" operation at FedEx).

462. *Id.*

463. *See id.* (indicating that the canine alerted that the package contained illegal drugs).

464. *See id.* (discussing how another officer took the package to a manager and shared that the package may contain drugs).

465. *Id.*

466. *See id.* (recounting how the manager opened the package to find a "white substance" that turned out to be a cocaine base).

467. *See id.* (detailing how the contents of the package were photographed at the police station and then delivered).

468. *See id.* at 705 (presenting Smith's argument that FedEx manager acted as government agent).

court denied his motion, and Smith was eventually sentenced to 120 months' imprisonment.[469]

The Eight Circuit affirmed the district court's denial of Smith's motion.[470] The circuit court first noted its standard consisted of three factors: (1) "whether the government had knowledge of and acquiesced in the intrusive conduct"; (2) "whether the citizen intended to assist law enforcement agents or instead acted to further his own purposes"; and (3) "whether the citizen acted at the government's request."[471] In applying the factors, the court found that the first factor (knowledge and acquiescence) weighed in favor of finding that the facility manager acted as a government agent.[472] The other two factors, the circuit court found, weighed the other way and against Smith's claim.[473] As to the second factor (intent), the court believed that the motivation to assist law enforcement was far too subordinate to the facility manager's motivation to protect Federal Express from carrying contraband.[474] The third factor (government's request) went against Smith's claim, according to the circuit court, because the detective "made it clear that he was not asking or ordering" the manager to open the package.[475]

If the standard proposed here had been applied at the time, the outcome of the question of whether the Federal Express facility manager was a government agent when she opened and searched Smith's package, likely would have been different.[476] Each of the factors are applied next.

1. *Trespass or Intrusion*

There was undoubtedly an intrusion into a constitutionally-protected area.[477] "Sealed packages," such as Smith's package, "are of course, entitled to Fourth Amendment protection against warrantless

469. *See id.* at 703 (recounting that district court denied Smith's motion to suppress and sentenced him to 120 months of prison).

470. *See id.* at 705–06 (affirming the district court's decision to deny the motion to suppress).

471. *Id.* at 705.

472. *See id.* ("[T]he government certainly knew of, and acquiesced in, the opening of the package.").

473. *See id.* (holding that the manager did not act as a government agent).

474. *See id.* at 705–06 (holding that the facility manager primarily intended to make sure FedEx was not shipping contraband).

475. *Id.* at 705.

476. *See generally id.*

477. *See id.* at 703.

searches and seizures, just as any other private area."[478] So this factor would have weighed in favor of finding that the Federal Express facility manager acted as an agent of the government.[479]

2. *Instigate, Incite, or Encourage*

The Eighth Circuit seemingly addressed this factor when it measured its standard's factor of whether the government requested the search and stated that it was "clear that [the detective] was not asking or ordering [the facility's manager] to open the package."[480] This author takes exception to this finding. Clearly the Eighth Circuit took the view that a "request" in this context must be affirmative, explicit, and verbal.[481] Such a narrow view ignores that that person-to-person communication, including requests, can take many forms. Indeed, communications between people regularly are nonverbal, or done through indirect assertions, and even passive.[482] Such is the case in *Smith* when the facility manager asked the detective if *he (the detective)* wanted her to open the Smith's package, and the detective responded, "if you want to open it that would be fine."[483] A persuasive case can be made that the detective's response was a passive request for the manager to open the package, especially considering the context—a drug interdiction program involving police officers stationed within the Federal Express facility to identify suspicious packages for examination.[484] Equally persuasive is the fact that the detective brought the package to the manager *so it could be opened* to confirm his suspicions about it.[485] The exchange between the manager and the detective is analogous to an officer handing a package to another person, and that person saying, "I am going to open this package, unless you tell me to stop," and the officer responding with silence. The silence is a request to open the package considering the

478. United States v. Givens, 733 F.2d 339, 341 (4th Cir. 1984).
479. *See Smith*, 383 F.3d at 703.
480. *Id.* at 705.
481. *See id.*
482. *See How Much of Communication is Really Nonverbal?*, UNIV. OF TEXAS PERMIAN BASIN, https://online.utpb.edu/about-us/articles/communication/how-much-of-communication-is-nonverbal/ [https://perma.cc/L4BA-XSKB] (last visited Oct. 25, 2021).
483. *See Smith*, 383 F.3d at 703.
484. *See id.*
485. *See id.*

circumstances preceding the officer's silence. The same is true of the manager–detective exchange that happened in *Smith*.[486]

Regardless, there is a less cumbersome and arguable path to finding this factor was met. The detective's response of "if she wanted to open it that would be fine" authorized the manager to open the package.[487] Providing authorization is a form of encouragement. Given the context was a drug interdiction effort and that the detective personally handed the package to the facility manager, it is easy to see how the detective's response encouraged the manager to open the package without fear of repercussion.[488]

3. *Means of Communication*

This factor would have also weighed in favor of granting Smith's suppression motion. Federal Express, and its facility manager in particular, had a line of communication that was not available to the general public: police officers and detectives stationed within the facility for the purpose of participating in a drug interdiction program.[489] The officers and detectives were essentially acting as "in-house" law enforcement officers for Federal Express.[490] This relationship and close proximity gave Federal Express and its employees the means and opportunity to communicate with law enforcement in a manner not available to the general public.[491]

4. *Presence*

The detective's presence during the manager's opening and searching of Smith's package would have pushed this factor in Smith's favor. This is especially so because not only was the detective present for the search, he also (as discussed earlier) authorized the search by telling the facility manager that it would be "fine" if she opened the package.[492]

---

486. *See id.*
487. *Id.*
488. *See id.*
489. *See id.*
490. *See id.*
491. *See id.*
492. *See id.*

5. *Direction*

This factor would have been a toss-up. On one hand, there was no evidence that the detective directed the facility manager in how to open or search the package. However, on the other hand, it could be argued that the detective's response that it was "fine" for the manager to open and search the package was direction about opening the package (i.e., that the manager was legally permitted to open the package).[493] Admittedly, the latter argument is the weaker of the two, and therefore, this factor likely would have gone against Smith and his Fourth Amendment challenge.

6. *Benefit*

There is no indication that Federal Express or the facility manager received a benefit, or expected to receive a benefit, for assisting law enforcement by opening Smith's package. This factor would have weighed in favor of the government's position.

7. *Prior History*

The *Smith* opinion does not discuss whether Federal Express previously provided search material to the government for law enforcement. However, Smith could have won this factor by pointing to the numerous cases that preceded his, where defendants made Fourth Amendment challenges based on the searches conducted by Federal Express.[494]

8. *Motivation*

This factor would have been another toss-up. The Eighth Circuit found an "absence of evidence that [the Federal Express facility manager] was motivated solely or even primarily by the intent to aid" law enforcement, and the Eight Circuit also affirmed the trial court's finding that the manager "opened the package out of her desire to ensure that her company was not being used as a vehicle in the drug

493. *See id.*

494. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 115 (1984); United States v. Matthews, Nos. 93-5708, 93-5747, 1994 WL 228226 at *3 (6th Cir. May 24, 1994); United States v. Boyer, 914 F.2d 144, 145–46 (8th Cir. 1990); United States v. Barry, 673 F.2d 912, 914–16 (6th Cir. 1982).

trade."[495] I do not agree with that assessment. As discussed earlier, rare is it that a private searcher has a singular primary motivation that is not intertwined with other motivations.[496] This is particularly true when the private searcher is a private company, such as Federal Express, that always has self-preservation and profit as continual primary motivations.[497] But for the sake of this exercise, it is presumed that the district and circuit courts' view would have prevailed and pushed this factor to the government's side of the ledger.

9. *Prior Knowledge*

That this factor would have favored Smith is straightforward and beyond debate. The detective certainly knew the facility manager was going to open and search Smith's package because he gave her permission to do so (by telling her that it was "fine" to open the package).[498]

10. *Intent in Transferring*

Smith did not involve a transfer of information because the search was conducted in the presence of law enforcement.[499] The witnessing detective learned of the information, i.e., the contents of Smith's package, at the same time the facility manager learned the same.[500] This factor then would have ended up on the government's side of the ledger.

The final tally in this mock reimagining of *Smith* using the expanded deputization standard is six factors (trespass, encouragement, communication, presence, prior history, prior knowledge) favoring Smith's claim compared to four factors (direction, benefit, motivation, intent in transferring) favoring the government and an opposite finding. The totality of the circumstances

495. *Smith*, 383 F.3d at 705–06.

496. *See* United States v. Leffall, 82 F.3d 343, 347 (10th Cir. 1996) ("Almost always a private individual making a search will be pursuing his own ends—even if only to satisfy curiosity—although he may have a strong intent to aid law enforcement.").

497. *See Smith*, 383 F.3d at 705 (noting that when commercial carriers such as Federal Express inspect suspicious packages for contraband they are motivated by their own desire and responsibility to not transport contraband as well as a desire to help law enforcement).

498. *See id.* at 703.

499. *See id.*

500. *See id.*

reflected by this ledger would greatly lean toward a court finding that the Federal Express facility manager acted as a government agent when she opened the package destined for Smith.

That would not be the end of the analysis or fully resolve Smith's Fourth Amendment challenge. Smith and his challenge would then need to survive the subsequent *Katz* inquiry, which would involve complex and difficult questions concerning Smith's expectation of privacy in a package containing contraband.[501] Assuming Smith's challenge survived this step, he would still need to show how the manager's search was unreasonable and not subject to a warrant exception. The key point here is that when it comes to the question of whether the Federal Express facility manager acted as an agent of the government, it is highly likely that the court would have reached a different conclusion had it applied the expanded deputization standard proposed by this Article.[502]

CONCLUSION

There is a pressing and growing need to reimagine and adjust how courts determine whether private searches constitute government action reached by the Fourth Amendment.[503] This need is fueled by the nearly unchecked growth (in size, reach, and power) of technology companies, who as surveillance intermediaries, are amassing troves of data about our lives and regularly sharing that data with the government.[504] Adding to the need are the private security guards who remain unreached by the Fourth Amendment even though they increasingly look and act like police officers, as well as the emergence of private companies, such as Persistent Surveillance System, who seek to profit by serving as outsourced surveillance providers unencumbered by the Fourth Amendment.[505] There is also the growing threat of vigilantism from extremist groups and militias who assume

501. *Compare* United States v. Young, 350 F.3d 1302, 1306–07 (6th Cir. 2003) ("[T]he Federal Express packages were 'effects' in the context of the Fourth Amendment, and therefore defendants presumptively possessed a legitimate expectation of privacy in their contents."), *with* United States v. Boyer, 914 F.2d 144, 146 (8th Cir. 1990) (discussing how Federal Express employee's opening of container extinguished any of the defendant's expectation of privacy in the container).

502. *See Smith*, 383 F.3d at 705–06 (holding that the district court did not err in its decision to deny the motion to suppress).

503. *See supra* Part I.

504. *See* discussion *supra* Part I.

505. *See* Reel, *supra* note 1.

police search and seizure powers to pursue their harmful ends and agendas.[506]

The current deputization framework is not able to meet or address this need. It is anchored to a time when "big tech" surveillance intermediaries and private surveillance companies did not exist or were nascent.[507] And it offers no protection or deterrence against the government profiting from vigilantes and extremists violating the rights and safety of others.[508] The time is now for reform and change, or else surveillance outsourcing will reach a point where the Fourth Amendment has little use or meaning, and no one will be secure in their "persons, houses, papers, or effects."[509]

506. *See* Salcedo, *supra* note 136.
507. *See* Brennan-Marquez, *supra* note 22, at 499–502.
508. *See id.*
509. U.S. CONST. amend IV.