2016

Fourth Amendment Time Machines (And What They Might Say About Police Body Cameras)

Stephen E Henderson, *University of Oklahoma College of Law*

FOURTH AMENDMENT TIME MACHINES (AND WHAT THEY MIGHT SAY ABOUT POLICE BODY CAMERAS)

Stephen E. Henderson[*]

ABSTRACT

When it comes to criminal investigation, time travel is increasingly possible. Despite longstanding roots in traditional investigation, science is today providing something fundamentally different in the form of remarkably complete digital records. And those big data records not only store our past, but thanks to data mining they are in many circumstances eerily good at predicting our future. So, now that we stand on the threshold of investigatory time travel, how should the Fourth Amendment and legislation respond? How should we approach bulk government capture, such as by a solar-powered drone employing wide-area persistent stare technology? Is it meaningfully different from civilian equivalents that find their way into government hands, whether it be tomorrow's drone flight, or today's record of all of our internet activity compiled by our internet service provider, or a current record of all of our movements compiled by our mobile phone company? What of targeted time machines such as government over-seizure of digital data in every computer search? This Article considers the benefits and costs of these miraculous time-machine technologies, including as evidenced by several recent court opinions. Considering the very serious privacy implications—from the individual to the relational and societal—we have good reason to be wary of their coming ubiquity. Yet perhaps in very limited spheres we should welcome them, going so far as to entirely abandon front-end acquisition restrictions and rely solely upon ex post access, use, and disclosure limitations to protect the security in our persons, houses, papers, and effects. I suggest that one such sphere might be law enforcement body cameras, an instance in which full capture has great benefits, and via which we can experiment upon the utility of solely ex post restraints.

* Judge Haskell A. Holloman Professor of Law, the University of Oklahoma College of Law; B.S. in Electrical Engineering, University of California at Davis; J.D., Yale Law School. I am grateful to the *University of Pennsylvania Journal of Constitutional Law* for the invitation to participate in the symposium, and to Nathan Hall and Jeffrey Vogt for excellent research assistance. Several years ago, George Asllani and Adrienne Robertson also performed some research which I have finally incorporated. Better late than never. Finally, I am grateful to Kiel Brennan-Marquez, Jules Epstein, Andrew Ferguson, Harold Krent, Christopher Slobogin, and Joseph Thai for providing comments and suggestions on previous drafts.

TABLE OF CONTENTS

INTRODUCTION

Time travel fascinates, whether it is the 1895 science fiction of H.G. Wells,[1] the 1985 humor of *Back to the Future*,[2] or the 2015 Hollywood manifestations in *Terminator Genisys*,[3] *Project Almanac*,[4] and *Tomorrowland*.[5] The reality is quite a bit more pedantic. Astronauts travel into the future via the relativistic effects of time dilation, it is true, but in an amount measured in milliseconds.[6] To do anything more impressive would require greater speeds than are currently possible.[7] Gazing at the stars is seeing events of time past, it is true,[8] but I can do the same by inserting a DVD or opening a book. Travel into the past remains the domain and dispute of theoretical physics and its Einstein-Rosen Bridges, more commonly known as wormholes,

1 H.G. WELLS, THE TIME MACHINE (1895).
2 BACK TO THE FUTURE (Universal City Studios, Inc. 1985).
3 TERMINATOR GENISYS (Paramount Pictures 2015).
4 PROJECT ALMANAC (Paramount Pictures 2015).
5 TOMORROWLAND (Walt Disney Pictures 2015). Time travel has been a feature of hundreds of films. *See* Kenneth Krabat, *All Time Travel Movies from 1896 and on*, KENNETH KRABATS 1000 STEMMER (Oct. 30, 2015), http://krabat.menneske.dk/kkblog/all-time-travel-movies/.
6 *See Time Dilation*, WIKIPEDIA, https://en.wikipedia.org/wiki/Time_dilation (last visited Feb. 13, 2016).
7 *Id.*
8 *How far is a light year?*, EARTHSKY (Nov. 27, 2015), http://earthsky.org/astronomy-essentials/how-far-is-a-light-year.

meaning that, so far as we know, traveling backwards in time might prove forever impossible.[9] So much for science.[10]

Yet when it comes to criminal investigation, time travel seems increasingly possible. It is not actually time travel, of course, and it has longstanding roots in traditional investigation. But science has provided us remarkably complete historical records in the form of digital data.[11] Well over a half century ago, Justice Robert H. Jackson recognized that "it would, no doubt, simplify enforcement of all criminal laws if each citizen were required to keep a diary that would show where he was at all times, with whom he was, and what he was up to."[12] The law requires no such diary. Only in certain sector-specific instances, such as banking, prescription records, or hotel registries, has the law itself created comprehensive records.[13] Nonetheless, we increasingly create a diary like that Justice Jackson envisioned via our smartphones and online technologies, and we even helpfully carry it with us wherever we go. Further, the National Security Agency ("NSA") has demonstrated that data from various third party sources might be gathered, stored, and later queried for evidence of criminality (or, in that case, evidence of threats to national security).[14] In short, we are "living in the golden age of surveillance."[15]

And lest we think criminal investigation can only offer that elusive travel back in time, developments in data mining and machine learn-

---

9 *See Wormhole*, WIKIPEDIA, https://en.wikipedia.org/wiki/Wormhole (last visited Oct. 31, 2015).

10 If my statements are proved dramatically wrong and we do learn to travel into the past, I will look to rewrite this.

11 *See* Stephen E. Henderson, *Our Records Panopticon and the American Bar Association Standards for Criminal Justice*, 66 OKLA. L. REV. 699, 700–06 (2014) (chronicling the massive increase in digital information).

12 Shapiro v. United States, 335 U.S. 1, 71 (1948) (Jackson, J., dissenting) (arguing against creation of the required records exception to the Fifth Amendment privilege against self-incrimination).

13 *See* City of Los Angeles v. Patel, 135 S. Ct. 2443, 2456 (2015) (striking down an ordinance giving police unrestricted and unchallengeable access to mandatory hotel guest registries); Whalen v. Roe, 429 U.S. 589, 598–600, 603–04 (1977) (permitting state prescription registry against constitutional challenge); United States v. Miller, 425 U.S. 435 (1976) (permitting government access to bank records required by Bank Secrecy Act of 1970). The most robust category of ongoing, population-wide acquisition and databasing would seem to be health information, but such acquisition has been little analyzed, perhaps because it is typically acquired for civil purposes. But that of course does not take it outside of the ambit of the Fourth Amendment, and Wendy Mariner has written a critical analysis of this historic "pass." *See generally* Wendy K. Mariner, *Reconsidering Constitutional Protection for Health Information Privacy*, 18 U. PA. J. CONST. L. 935 (2016).

14 *See infra* at 940–43.

15 BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 4 (2015).

ing are demonstrating that significant human behavior is predictable. For example, one study using mobile phone data found that location is 93% predictable,[16] and based only upon Facebook "likes," a computer was able to better predict personality and personal problems, including substance abuse, than real-life friends.[17] So, the more we learn about the past, the better we can predict the future.[18] We have not reached anything like the world of Philip K. Dick's *The Minority Report* with its mutant forward-seeing precogs,[19] or the world of Lewis Padgett's *Private Eye* with its ever-recording surroundings.[20] But, as is so often the case, today's science is creeping towards yesterday's science fiction.

So what happens as technology increasingly permits capture of almost all information? How should we, and our constitutional jurisprudence, approach bulk government capture, such as by a solar-powered drone employing wide-area persistent-stare technology,[21] or by a massive system of interconnected ground cameras?[22] Is it equiva-

16 Chaoming Song et al., *Limits of Predictability in Human Mobility*, 327 SCIENCE 1018, 1021 (2010), http://www.barabasilab.com/pubs/CCNR-ALB_Publications/201002-19_Science-Predictability/201002-19_Science-Predictability.pdf; *see also Dr Seldon, I Presume*, ECONOMIST, Feb. 23, 2013, at 76.

17 *See* Clifton B. Parker, *New Stanford Research Finds Computers Are Better Judges of Personality Than Friends and Family*, STANFORD REP. (Jan. 12, 2015), http://news.stanford.edu/news/2015/january/personality-computer-knows-011215.html; Wu Youyou et al., *Computer-based Personality Judgments Are More Accurate Than Those Made by Humans*, 112 NAT'L ACAD. SCI. 1036, 1036–39 (2015), http://www.pnas.org/content/112/4/1036.full.pdf.

18 Police are increasingly interested in such prediction. *See* Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 369–73 (2015) (explaining predictive policing); Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259, 265–85 (2012) (same).

19 *See The Minority Report*, WIKIPEDIA, https://en.wikipedia.org/wiki/The_Minority_Report (describing the film) (last visited Oct. 7, 2015).

20 Lewis Padgett, *Private Eye*, *in* MIRROR OF INFINITY: A CRITIC'S ANTHOLOGY OF SCIENCE FICTION 99 (Robert Silverberg ed. 1970).

21 *See* Ryan Gallagher, *Could the Pentagon's 1.8 Gigapixel Drone Camera Be Used for Domestic Surveillance?*, SLATE (Feb. 6, 2013, 10:14 AM), http://www.slate.com/blogs/future_tense/2013/02/06/argus_is_could_the_pentagon_s_1_8_gigapixel_drone_camera_be_used_for_domestic.html (describing government drone capability for data collection); Tyler Rogoway, *Drones in Afghanistan Have the Most Advanced Aerial Surveillance Ever*, FOXTROT ALPHA (Apr. 6, 2015, 9:40 AM), http://foxtrotalpha.jalopnik.com/drones-in-afghanistan-have-the-most-advanced-aerial-sur-1695912540 (describing the aptly named Gorgon Stare Increment II, which combines images from 368 integrated cameras); Tyler Rogoway, *How One New Drone Tech Finally Allows All-Seeing Surveillance*, FOXTROT ALPHA (Aug. 18, 2014, 12:45 PM), http://foxtrotalpha.jalopnik.com/how-one-new-drone-tech-finally-allows-all-seeing-survei-1553272901 (explaining several such technologies and both their utilities and their dangers).

22 *See* Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 48–50 (2014) (describing New York's "Domain Awareness System"); Somini

lent to a general warrant that can never be reasonable, or is that too simplistic an analogy?[23] The general warrant permitted indiscriminate *searching*, not merely *storing*. Is such direct gathering meaningfully different from what the government could obtain from a private party gathering such data, either by drone[24] or by a vast network of interconnected cameras?[25] Is it meaningfully different from what is available via an internet service provider that logs all of our online activity? Or from a mobile phone company tracking all of our movements? What about searches of our own devices that spy upon us, like our computers that log information we do not realize or desire? Can the government forever freeze and store that data, creating a mini, targeted time machine? Can it do the same by recording every home that officers enter, perhaps via officer body cameras?

While it may not be immediately obvious what to do about these disparate Fourth Amendment time machines, there is value in considering them for what they are. We should consider how they affect the security in our persons, houses, papers, and effects.[26] And we should consider their benefits to criminal investigation and, perhaps, separately to front-end deterrence. We have always known that limited government norms like that expressed in the Fourth Amendment are anti-accuracy: if police could enter any home at will, or even were quartered there, we would have less crime.[27] But life would be insufferable, and so we accept more crime in return for more lib-

---

Sengupta, *Privacy Fears Grow as Cities Increase Surveillance*, N.Y. TIMES (Oct. 13, 2013), http://www.nytimes.com/2013/10/14/technology/privacy-fears-as-surveillance-grows-in-cities.html (describing systems in several cities).

23 The general warrant in the form of the writs of assistance was a major impetus for the American Revolution and for the Constitution's Fourth Amendment. *See* Boyd v. United States, 116 U.S. 616, 625–27 (1886). For an analysis of the Fourth Amendment law of government drone flight, see Marc Jonathan Blitz, James Grimsley, Stephen E. Henderson & Joseph Thai, *Regulating Drones Under the First and Fourth Amendments*, 57 WM. & MARY L. REV. 49, 65–72 (2015). *See also* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71–72 (2013) (citations omitted) ("In our view, the threshold Fourth Amendment question should be whether a technology has the capacity to facilitate broad and indiscriminate surveillance that intrudes upon reasonable expectations of quantitative privacy by raising the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of law enforcement officers or other government agents.").

24 *See generally* Blitz et al., *supra* note 23, at 70–71 (explaining the First Amendment right to fly recording drones and its connection to the Fourth Amendment).

25 *See, e.g.*, Diane Cardwell, *A Light Bulb Goes On, Over the Mall*, N.Y. TIMES, July 20, 2015, at B1 (describing systems of internet connected cameras placed in lighting).

26 *See* U.S. CONST. amend. IV.

27 *See, e.g.*, United States v. Ganias, 755 F.3d 125, 139 (2d Cir. 2014) ("[T]he Fourth Amendment clearly embodies a judgment that some evidence of criminal activity may be lost for the sake of protecting property and privacy rights.").

erty, while always attempting not only the ideal balance—whatever that might be—but also always seeking pareto superior moves that increase one without lessening the other. As science increasingly permits capture without immediate human observation, does this call for a fundamental rethinking? Should we in certain instances abandon entirely front-end limitations on capture so long as we are guaranteed evenhanded treatment that traditional investigation lacks, and back-end limitations on access, use, and distribution? Can we ever feel secure if there is a government "database of ruin" that could be accessed at any moment?[28] Yet can we turn our backs on the ability to save lives and livelihoods, and in a manner that uniformly distributes the privacy costs?[29]

For some, perhaps the failed East German state and its Stasi is sufficient answer, a view to which I am personally sympathetic.[30] But, of course, access to those secret police files was not strictly circumscribed by fair legal process, and, more importantly, the data in the files were created by and for officers of the state. Should the same rules apply when data are created for other, beneficial purposes, or will never be subject to human analysis except upon demonstrated cause?[31] And if it becomes the case that, either on account of lack of political will, or perhaps on account of very broadly interpreted First Amendment rights, private third parties retain all data,[32] is there a realistic way to keep them out of government hands, or do the more important questions essentially once again amount to access, use, and

---

28 *See* Paul Ohm, *Don't Build a Database of Ruin*, HARV. BUS. REV. (Aug., 23, 2012), https://hbr.org/2012/08/dont-build-a-database-of-ruin (arguing against thoughtless databasing in the private sphere).

29 The details of any such claim to decreasing crime would be difficult, and would typically rely less on preventing crime than on deterrence via raising the likelihood of apprehension and conviction, thereby raising crime's expected cost. Whereas ex ante detection via data mining is extremely difficult and in some contexts currently impossible, ex post sifting through data to find then-evident connections is much easier. *See* SCHNEIER, *supra* note 15, at 136–40. And it is not hard to see that knowing *everything* tends to discourage crime and facilitate its apprehension.

30 *See, e.g.*, GARY BRUCE, THE FIRM: THE INSIDE STORY OF THE STASI (2010); ANNA FUNDER, STASILAND: STORIES FROM BEHIND THE BERLIN WALL (2011); ROBERT H. SLOAN & RICHARD WARNER, THE SELF, THE STASI, THE NSA: PRIVACY, KNOWLEDGE, AND COMPLICITY IN THE SURVEILLANCE STATE (forthcoming 2016) (manuscript at 5), http://ssrn.com/abstract=2577308. For a beautiful film fictionalizing some of the personal costs—and triumphs—of the human spirit in such surveillance conditions, see THE LIVES OF OTHERS (Sony Pictures 2006).

31 *See, e.g.*, *Persistent Stare Through Imagination*, U. ARIZ. SCH. INFO.: SCI., TECH., AND ARTS, http://w3.sista.arizona.edu/minds-eye.html (last visited Nov. 4, 2015) (seeking to build an artificially intelligent surveillance system).

32 *See* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 342–43, 367–71 (2010) (recognizing robust First Amendment rights of corporations).

disclosure? If a store-everything world is so abhorrent—and I personally believe it might be—then why do we keep rushing towards precisely that?[33]

Big questions rarely have small or singular answers, and this Article will hardly provide either. But it can begin the conversation or, more accurately, continue it under different framing. It does so in the following manner. Part I reminds us what the National Security Agency was attempting with its bulk telephone metadata collection, and then looks at two recent court decisions, one by a Second Circuit panel in *United States v. Ganias* (now headed en banc)[34] and one from the United States Supreme Court in *Riley v. California*,[35] each of which articulates a realization that historic digital data are meaningfully different for Fourth Amendment purposes. It then considers the Supreme Court's most recent Fourth Amendment decision, *City of Los Angeles v. Patel*, in which the Court floats the proposition that record-keeping for purposes of deterrence might be a "special need" subject to more lenient Fourth Amendment rules.[36] All three decisions and the NSA metadata program concern what might be considered Fourth Amendment time machines.

Part II canvasses the important principles of information privacy that are at stake. Part III then travels back in time to consider a 1995 proposal by Harold Krent in which he argues the Fourth Amendment should employ use restrictions upon data law enforcement has lawfully acquired.[37] The Second Circuit panel in *Ganias* would have recog-

---

33 Information security expert and frequent commentator Bruce Schneier declared "game over" in 2013:

> So, we're done. Welcome to a world where Google knows exactly what sort of porn you all like, and more about your interests than your spouse does. Welcome to a world where your cell phone company knows exactly where you are all the time. Welcome to the end of private conversations, because increasingly your conversations are conducted by e-mail, text, or social networking sites.
>
> And welcome to a world where all of this, and everything else that you do or is done on a computer, is saved, correlated, studied, passed around from company to company without your knowledge or consent . . . . Welcome to an Internet without privacy, and we've ended up here with hardly a fight.

Bruce Schneier, *The Internet Is a Surveillance State*, CNN, (Mar. 16, 2013, 2:04 PM), http://www.cnn.com/2013/03/16/opinion/schneier-internet-surveillance/index.html. Perhaps, however, at least some of the problem is one of market failure that could be remedied via regulation requiring internalizing of privacy harms. *See* A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. Ill. L. Rev. 1713, 1728–37 (2015).

34 755 F.3d 125 (2d Cir. 2014), *reh'g granted*, 791 F.3d 290 (2d Cir. 2015) (en banc).

35 134 S. Ct. 2473 (2014).

36 135 S. Ct. 2443 (2015).

37 Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49 (1995).

nized such a restriction.[38] It would of course be a significant further move to argue that the Fourth Amendment might be satisfied by such restrictions alone, a move I believe is fraught with great danger in most contexts. But perhaps there are limited contexts in which a move to solely use restrictions is one that legislatures, courts, agencies, and commentators should at least debate, if not begin to experiment with. Particularly when designed by legislatures, perhaps programs of uniform applicability should generally be considered constitutionally reasonable. And if there is any chance we are ever to rely solely upon back-end limitations in the world of Fourth Amendment time machines, it would be best to start learning now, in smaller spheres, whether such means can ever alone guarantee the securities promised by the Fourth Amendment. Thus, perhaps an ideal sphere for experimentation might be officer body cameras. Here the benefits of always recording are sufficiently great, and the domain sufficiently narrow, that it seems reasonable—and perhaps wise—to always record and to rely upon access, use, and disclosure limitations to protect our security interests.

I. THE NSA, HARD DRIVES, CELL PHONES, AND HOTEL REGISTRIES

On June 6, 2013, Glenn Greenwald broke the first story based upon the disclosures of former NSA contractor Edward Snowden.[39] Pursuant to an order from the secret Foreign Intelligence Surveillance Court, Verizon Business was providing the National Security Agency, "on an ongoing daily basis," "all call detail records or 'telephony metadata' created . . . for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."[40] "Telephony metadata" was defined to include "originating and terminating telephone number" and "time and duration of the call."[41] The NSA was creating a database of all telephone calls made on the Verizon Business network. Similar or-

38 *See infra* at 945–46.

39 Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. Many others would follow. *See* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE 90–169 (2014) (discussing the programs Snowden disclosed).

40 Secondary Order, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 13-80, at 1–2 (FISC Apr. 25, 2013), http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

41 *Id.* at 2.

ders were issued to other carriers, such that the NSA was databasing virtually all telephone calls made or received in the United States.[42]

Why? Perhaps no program of surveillance is surprising for an agency that eerily declares its "collection posture" as "Sniff it All—Know it All—Collect it All—Process it All—Exploit it All—Partner [Share] it All."[43] But why in particular did the NSA want to gather these phone records? Because the NSA wanted a time machine.[44] Say on August 1, 2015, the agency obtained reason to believe a particular telephone number, 301-688-6524, was being used by a terrorist. That might lead to a court order requiring the provider to place a pen register and trap and trace device on that line,[45] but of course the line might at this point be abandoned, or at least this would not reveal communications made in the past. So, a court order might require the provider to produce historic records.[46] Only the provider might have retained those records for only a limited duration. Moreover, the NSA wanted guaranteed access not only to the numbers with which 301-688-6524 had communicated (first "hop"), but also the numbers with which those first hop numbers had communicated (second "hop"), and further the numbers with which those second hop persons had communicated (third "hop").[47] The amount of data is growing exponentially, such that if each telephone number communicated with one hundred others, the NSA is looking at one million records. Quite convenient, then, to have everything stored and ready to query in their own servers. Time machines are handy like that.[48]

The NSA claimed statutory authorization to create this "historical repository"[49] was found in Section 215 of the USA PATRIOT Act.[50]

---

42 *See* Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 796–97 (2d Cir. 2015); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 8 (2014), http://fas.org/irp/offdocs/pclob-215.pdf [hereinafter PCLOB REPORT].

43 Greenwald, *supra* note 39, at 97.

44 This particular time machine would also be useful as, over time, the world's largest social network map.

45 *See* 50 U.S.C. § 1842 (2012) (authorizing approved use of pen register or trap and trade device for investigation).

46 *See* 50 U.S.C. § 1861 (2012) (authorizing such orders).

47 *See Clapper*, 785 F.3d at 797; PCLOB REPORT, *supra* note 42, at 9, 28–29.

48 The bulk telephony metadata program was not the NSA's only time machine. *See, e.g.*, Bruce Schneier, *More about the NSA's XKEYSCORE*, SCHNEIER ON SECURITY (July 7, 2015, 6:38 AM), https://www.schneier.com/blog/archives/2015/07/more_about_the_.html (explaining another program by which the NSA pulled massive amounts of internet data from fiber optic backbone cables).

49 *Clapper*, 785 F.3d at 812.

Whether or not it would be ideal to create such time machines, the NSA was certainly wrong in claiming it had been granted here.[51] Thus, the co-author of USA PATRIOT worked to enact legislation that has, for now, shut down this particular program, at least in the sense that the telephone records are no longer being centralized from all providers and held by the government.[52] But this has not been the first such government attempt,[53] and it would be startling if it is the last. There is nothing particularly special about telephone numbers that make them the only useful time machine metadata: the same use could be made of financial, internet, and other data.[54] In rejecting the NSA's contention that its bulk collection satisfied the required relevance threshold, the Second Circuit reasoned as follows:

> If information can be deemed relevant solely because of its necessity to a particular process that the government has chosen to employ, regardless of its subject matter, then so long as "the government develops an effective means of searching through *everything* in order to find *something*, . . . *everything* becomes relevant to its investigations"—and the gov-

50 Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT ACT") Act of 2001 § 215, Pub. L. 107-56, 115 Stat. 272, 287–88 (codified at 50 U.S.C. § 1861 (2012)) [hereinafter USA PATRIOT Act].

51 *See Clapper*, 785 F.3d at 812–21 (holding that Section 215 did not authorize the telephony data collection program); PCLOB REPORT, *supra* note 42, at 10 ("conclud[ing] that Section 215 does not provide an adequate legal basis to support the [telephone records] program"); Stephen E. Henderson, *A Rose By Any Other Name: Regulating Law Enforcement Bulk Metadata Collection*, 94 TEX. L. REV. SEE ALSO 28 (2016) (same).

52 *See* Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 ("USA FREEDOM Act of 2015") §§ 101–10, Pub. L. 114-23, 129 Stat. 268-76 (to be codified at 50 U.S.C. § 1861); Lisa Mascaro, *House Overwhelmingly Approves Bill to Curb NSA Domestic Spying*, L.A. TIMES (May 22, 2014), http://www.latimes.com/nation/politics/la-na-nsa-reforms-20140523-story.html. According to Representative Jim Sensenbrenner, the NSA interpretation was "like scooping up the entire ocean to guarantee you catch a fish." Jennifer Valentino-DeVries & Siobhan Gorman, *Secret Court Ruling Expanded Spy Powers*, WALL ST. J., July 8, 2013, at A4.

53 For years, the DEA collected massive amounts of telephone metadata for international calls under its administrative subpoena authority, an apparent precursor to the NSA bulk collection. *See* Brad Heath, *U.S. Secretly Tracked Billions of Calls for Decades*, USA TODAY (Apr. 8, 2015), http://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/. And there was of course the ill-fated Total Information Awareness program. *See* Joshua Partlow, *Senate Votes to Deny Funding To Computer Surveillance Effort*, WASH. POST, July 19, 2003, https://www.washingtonpost.com/archive/business/2003/07/19/senate-votes-to-deny-funding-to-computer-surveillance-effort/251243f1-8a66-4693-9970-f714130b783f/ (discussing the Senate's denial of funding to the Total Information Awareness initiative, a computer surveillance program that would enable the government to amass and search databases of records for potential terrorist activity).

54 *Clapper*, 785 F.3d at 818.

> ernment's "technological capacity to ingest information and sift through it efficiently" would be the only limit to what is relevant.[55]

This criticism, first made by the Privacy and Civil Liberties Oversight Board, is a fair criticism of the NSA's interpretation of "relevance," in that it is an interpretation inconsistent with legal tradition. But notice the proposition is not illogical: if later searches would prove useful in investigating national security threats (or crime), the existence of the database *is* relevant to a legitimate government role, and the program did include audit, security, and reporting requirements.[56]

But again, in this case it was clear this novel interpretation was not one Congress intended. The Second Circuit was correct that:

> Such expansive development of government repositories of formerly private records would be an unprecedented contraction of the privacy expectations of all Americans. Perhaps such a contraction is required by national security needs in the face of the dangers of contemporary domestic and international terrorism. But we would expect such a momentous decision to be preceded by substantial debate, and expressed in unmistakable language.[57]

Instead, USA PATRIOT and its legislative sponsors intended, and therefore used, the traditional language of legal relevance.[58] But what if the debate occurred and that unmistakable language did come about? Then there would of course be the question of whether it is a method of investigation the Constitution will abide. Although the Second Circuit did not decide this constitutional issue, it recognized the issue as "one of the most difficult issues in Fourth Amendment jurisprudence: the extent to which modern technology alters our traditional expectations of privacy."[59]

Is this an issue of technology? After all, was not the first investigating "time machine" an officer taking notes on what she hears and sees, not to mention the myriad recordkeeping requirements imposed by the modern industrial State? Three recent decisions shed more light on this issue: a panel decision in the Second Circuit (now headed en banc) considering a digital time machine in the form of

---

55 *Id.* at 818 n.10 (quoting PCLOB REPORT, *supra* note 42, at 62).

56 *Id.* at 797–98 (terming them "minimization procedures"); PCLOB REPORT, *supra* note 42, at 33–36. Those requirements did not, however, protect data that had been found responsive to seed queries and thus was placed in the NSA "corporate store." PCLOB REPORT, *supra* note 42, at 30–31. In other words, access to once responsive data was thereafter unrestricted.

57 *Clapper*, 785 F.3d at 818.

58 *Id.* at 811.

59 *Id.* at 822.

government preservation of private computer hard drives,[60] a decision by the United States Supreme Court considering a voluntarily compiled and carried digital time machine in the form of a mobile phone,[61] and another decision by the Supreme Court considering much more old-fashioned recordkeeping in the form of a hotel guest registry.[62]

A. Ganias *and Preservation of Hard Drives*

In November of 2003, federal agents executed a search warrant on the accounting offices of Stavros Ganias.[63] Ganias himself was not the target, but rather the Army was investigating one of his clients with whom the Army contracted.[64] The agents executing the warrant therefore did not remove Ganias's three computers, respecting his as an ongoing business, but instead mirrored the hard drives, making exact duplications thereof.[65] Forensics examiners thereafter copied that data onto two sets of identical DVDs, thereby preserving the government originals from any harm occasioned by access.[66]

That access would not occur for eight months, until July 2004, when Army forensics agents began to review the DVDs pursuant to the search warrant.[67] When they discovered the suspect business might have committed tax fraud, they shared a copy of the data with the IRS,[68] and together the two sets of investigators ultimately identified all responsive material by December of 2004.[69] Nonetheless, the agents did nothing to try and delete or return the non-responsive material. Unlike for seized physical items, these agents never consider deleting or returning non-responsive digital data.[70] "[Y]ou never know what data you may need in the future," testified one.[71]

In July of 2005, some twenty months after the search of Ganias's office and corresponding seizure of his computer data, Army and IRS investigators came to believe that Ganias might have been underre-

60 United States v. Ganias, 755 F.3d 125, 128 (2d Cir. 2014), *reh'g granted*, 791 F.3d 290 (2d Cir. 2015) (en banc).
61 Riley v. California, 134 S. Ct. 2473, 2480 (2014).
62 City of Los Angeles v. Patel, 135 S. Ct. 2443, 2447 (2015).
63 *Ganias*, 755 F.3d at 128.
64 *Id.*
65 *Id.*
66 *Id.* at 129.
67 *Id.*
68 *Id.*
69 *Id.*
70 *Id.*
71 *Id.*

porting income, and therefore expanded their investigation to include him as a suspect.[72] They therefore wanted to have another look at his files, but appropriately did not consider their mere possession of those files to authorize further searches thereof.[73]

To understand why, one must first consider traditional searches and basic Fourth Amendment law. When police search a home pursuant to a warrant, they may look only where sought-after items can be.[74] And they may seize only things the warrant authorizes, or things so located for which authority for seizure is "immediately apparent," such as child pornography or obviously illegal drugs.[75] These things are said to be in "plain view."[76] So, for example, police searching for a large knife should not open a small book at all—it cannot contain the sought-after knife, and therefore is not subject to search. Whereas police searching for a knife *and* any threatening communications could peruse the small book. But upon finding it to contain entirely unrelated material, police of course must leave the book behind *unless* that material is independently subject to seizure, meaning the officer has probable cause to believe it either the fruit of crime (it appears to be a rare book that was reported stolen), an instrumentality of crime (it appears to be the very book used to lure a young victim), contraband (it appears to contain child pornography), or evidence of crime (it appears to contain the planning for a recent bank robbery).[77] In rare instances, large quantities of physical documents might be impossible to sort onsite, but then special rules are to be followed.[78]

With computers, everything is done differently. Because they contain so much disparate data, and in so many formats, police cannot reasonably be expected to bring experts to sufficiently sort through it on site.[79] Thus, courts all permit *over-seizure* of digital evidence in eve-

72 *Id.*

73 *Id.* at 129, 133 n.7.

74 Horton v. California, 496 U.S. 128, 140–41 (1990).

75 *Id.* at 136–37.

76 *Id.*

77 Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 301–02 (1967).

78 *Ganias*, 755 F.3d at 135 (citing United States v. Tamura, 694 F.2d 591, 595–96 (9th Cir. 1982)).

79 *See* OFFICE OF LEGAL EDUC., EXEC. OFFICE OF U.S. ATTORNEYS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 76–79 (2009), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf. For an analysis of the law regulating the forensic search, see Stephen E. Henderson, *What Alex Kozinski and the Investigation of Earl Bradley Teach About Searching and Seizing Computers and the Dangers of Inevitable Discovery*, 19 WIDENER L. REV. 115, 130–36 (2013).

ry instance: the entire hard drive, say, can be seized even though much, most, or even all of its contents—entire libraries of digital materials, let alone files arguably equivalent to that small book found in the hypothetical home search—are in fact entirely innocent.[80]

Investigators have thus obtained a time machine. Following the November 2003 execution of the search warrant, Ganias modified the relevant files.[81] Therefore, had the government not over-seized and then retained digital content that it knew was not relevant to the first investigation, and therefore which was not covered by the original warrant, this evidence would not have existed.[82] Yet because agents did retain not only the exact copies of his hard drive but also the DVDs, the data did exist. And they might retain such data for ten, twenty, or a hundred years.[83] So, pursuant to another warrant obtained in April 2006—some two-and-a-half years after the data's seizure—the government once again searched the data and found incriminating evidence. Time machines are handy like that.

The Second Circuit panel addressed just this time machine functionality, although its opinion is now vacated pending en banc review[84]:

> [W]e consider a [] limited question: whether the Fourth Amendment permits officials executing a warrant for the seizure of particular data on a computer to seize and indefinitely retain every file on that computer for use in future criminal investigations. We hold that is does not.[85]

The over two-year retention of Ganias's unresponsive data, retained a year and a half *after* the government had concluded it was nonresponsive, violated the Fourth Amendment.[86] Or, at the very least, its use in a future criminal investigation did.[87]

---

80 *See Ganias*, 755 F.3d at 135–36 (collecting cases).

81 *Id.* at 130.

82 *Id.* at 130, 138 n.11.

83 For the various FBI retention policies, see *Records Control Schedules*, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, http://www.archives.gov/records-mgmt/rcs/schedules/?dir=/departments/department-of-justice/rg-0065; see also U.S. DEP'T OF JUSTICE, FEDERAL BUREAU OF INVESTIGATIONS, A GUIDE TO CONDUCTING RESEARCH IN FBI RECORDS (2010), https://www.fbi.gov/foia/a-guide-to-conducting-research-in-fbi-records. The harms are of course even greater when law enforcement has seized the originals and not merely image copies. *See, e.g.*, United States v. Gladding, 775 F.3d 1149, 1152 (9th Cir. 2014) (requiring the government to prove it is not feasible to disaggregate, and then return, innocent over-seized data).

84 *Ganias*, 791 F.3d 290.

85 *Ganias*, 755 F.3d at 137. *Cf.* United States v. Johnston, 789 F.3d 934, 941–43 (9th Cir. 2015) (holding, without considering *Ganias*, that a five-year delay in searching a computer pursuant to the original warrant is not constitutionally problematic).

86 *Ganias*, 755 F.3d at 138. In so holding, the court importantly sided with those arguing Fourth Amendment seizure is implicated by any meaningful deprivation in the *exclusive*

I agree, though I differ from the panel's reasoning. The panel believed the government's position would mean that "every warrant to search for particular electronic data would become, in essence, a general warrant."[88] That does not seem quite apt, as a general warrant permitted the executive to search *anyone's* house for information of interest,[89] or at least one person's house for *anything* incriminating,[90] whereas both in 2003 and in 2006 the government obtained a warrant demonstrating particularized suspicion towards Ganias's data, and in each instance agents thereafter only looked for the responsive data. Instead, the government's position would turn every computer warrant into an investigative time machine.

It is a serious invasion if the government can over-seize massive amounts of private information and forever retain it for indefinite later search. One can understand the concern of the government, which is that if the data are not retained in their original form it might be difficult to answer later claims of unreasonable search or challenges to authentication.[91] But, like the panel, I do not see that

---

possession of property. *Id.* at 137 ("The Government's retention of copies of Ganias's personal computer records for two-and-a-half years deprived him of exclusive control over those files for an unreasonable amount of time. . . . This was a meaningful interference with Ganias's possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment."). *See* Paul Ohm, *The Fourth Amendment Right to Delete*, 119 HARV. L. REV. F. 10, 12 (2005) (arguing for such an interpretation).

87 *Ganias*, 755 F.3d at 139 ("[E]ven if we assumed it were necessary to maintain a complete copy of the hard drive solely to authenticate evidence responsive to the original warrant, that does not provide a basis for using the mirror image for any other purpose."). *Id.* at 138 ("[T]he Government clearly violated Ganias's Fourth Amendment rights by retaining the files for a prolonged period of time *and then using them* in a future criminal investigation." (emphasis added)). *Id.* at 139 ("Because the Government has demonstrated no legal basis for retaining the non-responsive documents, its retention *and subsequent search* of those documents were unconstitutional." (emphasis added)); *id.* at 141 ("We conclude that the Government violated Ganias's Fourth Amendment rights by seizing and indefinitely retaining non-responsive computer records, *and then searching them* when it later developed probable cause." (emphasis added)).

88 *Id.* at 139.

89 *See* WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 602–1791, at 233 (2009). Thus, a warrant for stolen sheep in 1749 instructed the local constable to "diligently search every suspected House and Place within your Parish, which you and the . . . [owner of the sheep] shall think convenient to search." *Id.* (citations omitted). A 1661 warrant authorized the executive "to make diligent search . . . throughout the whole town of Milford and the precincts thereof . . . ; and this to be in all dwelling houses, barnes or other buildings whatsoever, and vessels in the harbor." *Id.* at 234–36 (citations omitted).

90 *See, e.g.*, United States v. Stefonek, 179 F.3d 1030, 1032-33 (7th Cir. 1999) (rejecting a warrant permitting seizure of "evidence of crime" as an impermissible general warrant).

91 *See Ganias*, 755 F.3d at 139; Recent Cases, *Fourth Amendment—Search and Seizure and Evidence Retention—Second Circuit Creates a Potential "Right to Deletion" of Imaged Hard Drives.—*

as an impossible hurdle.[92] So, perhaps the panel's answer is broadly the right answer: maybe the Fourth Amendment bans even relatively small digital time machines, no matter how useful, no matter how regulated, and no matter how democratically conceived and applied. The government can retain the data for its original purposes as long as it must, but cannot search the data for any other. Or, perhaps such time machines are only permissible where government need is at its highest, such as for purposes of national security, or where the retention was pursuant to a carefully structured—and fairly inclusive—legislative authorization. I will return to these questions below. The immediate point is merely to highlight that digital evidence has made these questions increasingly pressing.

The Supreme Court came to the same realization when it considered searches of cell phones incident to lawful arrest.

B. Riley *and Searches of Cell Phones*

David Riley was stopped for a minor traffic infraction, his car was searched pursuant to impoundment, and he was arrested for illegally possessing two handguns found therein.[93] As police are permitted to do as a routine incident of any lawful arrest,[94] officers searched Riley's person and found a smartphone in his pocket.[95] A search of that phone onsite and a couple of hours later at the station yielded relevant evidence in the form of incriminating text messages, videos, and images.[96]

The Supreme Court consolidated Riley's case with that of Brima Wurie, who was arrested following an apparent drug sale.[97] At the police station, officers seized two phones from his person, and one of them—a flip phone—continued to receive calls from a number the phone identified as "my house."[98] Officers opened the phone and accessed the call log, thereby obtaining the phone number associated with these calls.[99]

The Court resoundingly rejected both searches:

United States v. Ganias, *755 F.3d 125 (2d Cir. 2014).*, 128 HARV. L. REV. 743, 748–50 (2014).

92 *Ganias*, 755 F.3d at 139.

93 Riley v. California, 134 S. Ct. 2473, 2480 (2014).

94 United States v. Robinson, 414 U.S. 218, 235–36 (1973).

95 *Riley*, 134 S. Ct. at 2480.

96 *Id.* at 2480–81.

97 *Id.* at 2481.

98 *Id.*

99 *Id.*

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life." [quoting Boyd v. United States, 116 U.S. 616, 630 (1886)] The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.[100]

Established doctrine would allow similar searches of non-digital containers immediately associated with an arrestee's person, including any found in the same pocket as Riley's phone.[101] So, why did all nine Justices reject these mobile phone searches? Lacking both precedent and any "precise guidance from the founding era,"[102] the Court had to make its own assessment of what constitutes an "unreasonable" search,[103] and that is done "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[104]

The governmental interests motivating searches incident to arrest—officer safety and evidence preservation[105]—are not particularly relevant to this Article. But, very briefly, what swayed the Court was that the interests are generally less significant in the digital context.[106] As for officer safety, there is no possibility the digital data will harm the arresting officers, unlike, say, a surreptitious knife or razor blade.[107] As for the remote possibility the data would inform officers of indirect harm—for example, that dangerous confederates were en route—the Court properly held this to be a case-specific exigent cir-

---

100 *Id.* at 2494–95; *see also id.* at 2495 (Alito, J., concurring in part and in the judgment but expressing reservations with the majority's limiting theory of search incident to arrest and expressing a willingness to reconsider if legislatures lead the way); United States v. Camou, 773 F.3d 932, 941–43 (9th Cir. 2014) (extending *Riley*'s protection of mobile phones to exempt them from the automobile exception to the warrant requirement).

101 *See Riley*, 134 S. Ct. at 2484 (discussing *United States v. Chadwick*, 433 U.S. 1, 15 (1977), which distinguished between searches of items "immediately associated with the person of the arrestee" and those otherwise within the arrestee's reach (quoting *Chadwick*, 433 U.S. at 15)).

102 *Riley*, 134 S. Ct. at 2484 (recognizing that not only was there no equivalent at the time of the founding, but that even the less sophisticated flip-phones "are based on technology nearly inconceivable just a few decades ago").

103 *Id.* at 2482 ("As the [Fourth Amendment] text makes clear, the ultimate touchstone of the Fourth Amendment is reasonableness." (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006)) (internal quotation marks omitted)).

104 *Id.* at 2484 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

105 *Id.* at 2483 (explaining the genesis of these twin aims).

106 *See id.* at 2485–88 (applying the criteria to mobile phones).

107 *Id.* at 2485.

cumstance sufficiently accounted for by that doctrine.[108] In other words, it will be the exception, not the rule. Similarly, there is little risk of evidence destruction once the officers seize the mobile phone, as even the typically negligible possibility of the device being remotely wiped can be countered with a Faraday bag, the cheap version of which is wrapping the phone in aluminum foil.[109]

More importantly for the purposes of this Article, the privacy interest in digital data is very significant, both in terms of quality and quantity.[110] While the government urged "that a search of all data stored on a cell phone is 'materially indistinguishable' from" searches of wallets and purses, to the Court, "[t]hat is like saying a ride on horseback is materially indistinguishable from a flight to the moon."[111]

As for quality, "[A] cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record."[112] As for quantity, a "phone's capacity allows even just one type of information to convey far more than previously possible."[113] Such is the marvel of digital data and its modern storage.[114] Indeed, "it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[115] It did not come at government behest, as Justice Jackson feared in 1948, but it came nonetheless.[116] Each such person is carrying a time machine, and the Court has now recognized how especially private are the digital data contained therein. As the Court

---

108 *Id.* at 2485–86.

109 *Id.* at 2486–88. The government also raised, for the first time before the Supreme Court, that the officers might be able to immediately access the data before the phone "locks," at which point encryption might render the data unreachable even pursuant to a valid warrant. *Id.* at 2486–87. The Court had two responses. First, officers who encounter an unlocked phone and who have probable cause can perhaps take the minimal steps necessary to turn off the auto-locking feature. *Id.* at 2487–88. Moreover, this situation—like the possibility of dangerous confederates texting of their approach—is sufficiently unlikely that it is otherwise properly handled via exigent circumstances. *Id.* at 2487.

110 *Id.* at 2489.

111 *Id.* at 2488.

112 *Id.* at 2489 (explaining that mobile phones "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers").

113 *Id.*

114 *See* Henderson, *supra* note 11, at 700–03 (chronicling the massive increase in digital storage).

115 *Riley*, 134 S. Ct. at 2490.

116 *See supra* note 12.

recognized, a single mobile phone will often contain more information than an entire home.[117] Time machines are useful like that. In the words of the Court, "In the cell phone context, . . . it is reasonable to expect that incriminating information will be found on a phone regardless of when the crime occurred."[118]

So, while *Riley* perhaps left things unanswered that it could have addressed,[119] it made very clear that when it comes to the Fourth Amendment, digital is different. And while compelled government access therefore required a warrant, this does not necessarily mean the Court is generally averse to the existence of digital time machines. The Court's most recent Fourth Amendment decision, which considered records that could be either analog or digital, contains a facially surprising claim that is a nod to time machines' utility.

C. Patel *and Searches of Hotel Registries*

City of Los Angeles v. Patel is a case about mini, government-mandated time machines in the form of hotel guest registries.[120] A provision of the Los Angeles Municipal Code requires that hotels record and maintain information about their guests, including name and address, vehicle license plate of any car parked on the premises, and method of payment.[121] Under certain circumstances additional identification information must be recorded, such as when a guest pays by cash, rents a room without a reservation, or stays for fewer

---

117 *Riley*, 134 S. Ct. at 2491. The Court had previously rejected the claim that officers could search an entire home incident to arrest. Chimel v. California, 395 U.S. 752, 753, 755, 768 (1969); *see also* 381 Search Warrants Directed to Facebook, Inc. v. New York County Dist. Attorney's Off., 2015 WL 4429025, at *7 (N.Y.S.3d July 21, 2015) ("Our holding today [that there is neither a constitutional nor statutory right to challenge of a search warrant other than a defendant's motion to suppress] does not mean that we do not appreciate Facebook's concerns about the scope of the bulk warrants issued here or about the District Attorney's alleged right to indefinitely retain the seized accounts of the uncharged Facebook users. Facebook users share more intimate personal information through their Facebook accounts than may be revealed through rummaging about one's home. These bulk warrants demanded 'all' communications in 24 broad categories from the 381 targeted accounts. Yet, of the 381 targeted Facebook user accounts only 62 were actually charged with any crime.").

118 *Riley*, 134 S. Ct. at 2492.

119 *See generally* Ric Simmons, *The Missed Opportunities of* Riley v. California, 12 OHIO ST. J. CRIM. L. 253 (2014) (arguing that the *Riley* Court did not "repair the critically flawed search incident to arrest doctrine" or "provide useful guidance for law enforcement officers faced with emerging technologies").

120 135 S. Ct. 2443, 2447–48 (2015).

121 L.A., CAL., MUN. CODE § 41.49(2)(a) (2008), http://clkrep.lacity.org/onlinedocs/2006/06-0125-s1_ord_179533.pdf.

than twelve hours.[122] Registry information must be maintained for a period of ninety days, and must be made available upon officer request.[123] As the recent publicity regarding the hack of cheating or "adultery" website Ashley Madison demonstrates,[124] it is not hard to imagine some of the privacy interests implicated by knowledge of hotel stays.[125]

At the same time, such a recordkeeping requirement is hardly novel, and the hotels did not challenge it.[126] A group of hotel operators did, however, challenge the provision requiring that the registry "shall be made available to any officer of the Los Angeles Police Department for inspection."[127] They contended such unrestrained access violated their Fourth Amendment rights, and a closely divided Supreme Court agreed.[128] According to the five Justice majority, the officer demand requirement is unconstitutional because it offers no opportunity for pre-compliance legal challenge,[129] essentially combining the ease of an administrative subpoena with the effectiveness of a warrant. *Patel* is an important opinion, because it permits meaningful facial challenges under the Fourth Amendment,[130] and because it lim-

122 *Id.* § 41.49(4).

123 *Id.* § 41.49(3)(a).

124 *See, e.g.*, Dino Grandoni, *Ashley Madison, a Dating Website, Says Hackers May Have Data on Millions*, N.Y. TIMES (July 20, 2015), http://www.nytimes.com/2015/07/21/technology/hacker-attack-reported-on-ashley-madison-a-dating-service.html; Emma Johnson, *Ashley Madison Hack Would Mean 'Boon for Divorce Lawyers and Marriage Therapists,'* FORBES (July 20, 2015), http://www.forbes.com/sites/emmajohnson/2015/07/20/ashley-madison-hack-would-mean-boon-for-divorce-lawyers-and-marriage-therapists/.

125 *See, e.g.*, Tina Kelly, *Mayflower Mystery: Room 871, Where Are You?*, N.Y. TIMES (Mar. 20, 2008), http://cityroom.blogs.nytimes.com/2008/03/20/mayflower-mystery-room-871-where-are-you/ (detailing how Governor Eliot Spitzer enjoyed the services of a prostitute in The Mayflower's room 871); Sarah Kershaw & Michael Powell, *Just a Hotel? For Some, It's an Adventure*, N.Y. TIMES, March 20, 2008, at G1 (generally describing prostitution at the Mayflower Hotel).

126 *Patel*, 135 S. Ct. at 2454 ("Respondents have not challenged and nothing in our opinion calls into question those parts of § 41.49 that require hotel operators to maintain guest registries containing certain information.").

127 L.A., CAL. MUN. CODE, *supra* note 121, at § 41.49(3)(a).

128 *Patel*, 135 S. Ct. at 2451.

129 *Id.*

130 *Id.* at 2449 ("We first clarify that facial challenges under the Fourth Amendment are not categorically barred or especially disfavored."). Even with facial challenges theoretically available, they could never be successful if defeated by the possibility that an officer *possessing a valid warrant* could make the records request, that an officer *in an emergency* could make the records request, or that the subject of a request could consent. Fortunately, the Court recognized an unrestricted access statute can be facially unconstitutional regardless of those possibilities, because they are properly understood as independent from the grounds of a statutory access not requiring any of them. *Id.* at 2450–51. *Cf. id.* at 2464–66 (Alito, J., dissenting) (arguing otherwise).

its what has been a nebulous "closely regulated industry exception."[131] But what is of interest for this Article is the Court's dictum regarding deterrence.

The Court assumed, without deciding, that the government purpose for the registry program was a "special need" outside of ordinary crime control, thus lessening the Fourth Amendment burden.[132] Since the ordinance was clearly aimed at solving crime, it is hard to imagine what this special need would be. Although the boundaries have always been unclear, in the automobile context, for example, the Court has differentiated roadblocks aimed at preventing highway fatalities and carnage (a special need), from those aimed at interdicting drugs (ordinary crime control).[133] Officers accessing the historic registry were unlikely to prevent imminent threatened harm akin to that posed by drunk drivers, as opposed to finding the clues necessary to prosecute past offenses. This seems true by definition for a registry dating back three months.

Yet the Court assumed a special need, namely deterring criminality.[134] It seems hard to imagine deterrence of criminality can be a meaningful special need: deterrence is not the reason for legitimate police investigation that constitutes a search or a seizure, but instead is the happy—albeit very important—byproduct of investigating actual crime. In other words, surely police cannot routinely make warrantless entry into homes and claim the "special need" of deterring crimes that might otherwise be committed therein. Instead, when law enforcement officers enter homes pursuant to lawful warrants or exceptions thereto, and people learn of those events including sub-

131 *Id.* at 2454–56. The Court has declared four closely regulated industries, for which it permits systems of routine, suspicionless inspection: liquor distribution, firearms distribution, mining, and automobile junkyards. *Id.* at 2454. Before *Patel*, it was unclear whether a legislature could effectively get around the Fourth Amendment: subject a business to sufficient regulation, such that it is pervasively regulated, and now the Fourth Amendment has little play. The Court majority signaled this would not be possible, finding the exception to apply only when something "inherent in the operation of [the business] poses a clear and significant risk to the public welfare." *Id.* This remains somewhat nebulous, especially given the disparate existing four categories, but at least it is a more limited sort of nebulous.

132 *Id.* at 2452.

133 *See* City of Indianapolis v. Edmond, 531 U.S. 32, 48 (2000) (striking down drug interdiction checkpoints); Michigan Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990) (allowing sobriety checkpoints).

134 *Patel*, 135 S. Ct. at 2452 ("Here, we assume that the searches authorized by § 41.49 serve a 'special need' other than conducting criminal investigations: They ensure compliance with the recordkeeping requirement, which in turn deters criminals from operating on the hotels' premises.").

sequent prosecutions, they are deterred from themselves engaging in such criminality.

So, why the odd assertion of deterrence as a special need? Presumably because of the intuition that the registry requirement, like other and more significant time machines, is an effective—and perhaps smart—way to go after criminal behavior. But even if that might be so, the Court was right to find problematic the complete absence of access restrictions given the privacy interests at stake. Indeed, it is worth stepping back to broadly consider these interests of information privacy before contemplating what they implicate for investigatory time machines.

II. PRIVACY

As integral as privacy is to most of our lives—or at least as integral as I believe it is to mine—there is considerable controversy and confusion as to its definition, including as to whether it is a state of being or a right.[135] In other words, is "perfect" privacy achieved only when nobody has any information about and access to my person (which sounds rather awful), or also when I have complete control over those modes of access but have volitionally granted them in certain amounts (which sounds rather utopian)?[136] Learned philosophical minds have debated these concepts for years and presumably will for as long as there are philosophers to debate. My less philosophically tutored mind finds useful—and for criminal procedure purposes seemingly sufficient—the construct that *information* privacy is the ability of a person to control what information about her is given to others, and for what purposes.[137] Such a control construct was most no-

135 *See, e.g.*, Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 425–28 (1980) (arguing privacy is a "condition of life," not a claim or form of control). *See generally* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY (Ferdinand David Schoeman ed., 1984); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002).

136 *See* Gavison, *supra* note 135, at 428.

137 *See* ABA STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS 49–52, 57–58 (3d ed. 2013); Stephen E. Henderson, *Expectations of Privacy in Social Media*, 31 MISS. C. L. REV. 227, 229–34 (2012). Information privacy can be contrasted with decision privacy, the latter encompassing decisions about bodily autonomy like what medical treatment to receive. *See* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762 (1989) ("As we have pointed out before, '[t]he cases sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.'" (quoting Whalen v. Roe, 429 U.S. 589, 598–600 (1977))).

tably articulated by Alan Westin[138] and Charles Fried,[139] and has been recognized by the Supreme Court.[140]

So understood, privacy can be seen as a constitutive element of human autonomy, or as a key element in the identity formation and mental freedom that is central to a *fully realized* autonomy.[141] In the words of Thomas Nagel, "The boundary between what we reveal and what we do not, and some control over that boundary, are among the most important attributes of our humanity."[142] Without privacy, people will engage in harmful self-censorship not only in what they will say and in what they will do, but even in what they will think as they internalize an awareness that they are always watched.[143] And the abil-

138 *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) ("Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."). "Most definitions of privacy agree on a core concept: that privacy is the claim of an individual to determine what information about himself or herself should be known to others. This also involves when such information will be communicated or obtained and what uses will be made of it by others." ALAN F. WESTIN, HISTORICAL PERSPECTIVES ON PRIVACY: FROM THE HEBREWS AND GREEKS TO THE AMERICAN REPUBLIC 4 (presented and distributed at the 2009 Privacy Law Scholars Conference, and quoted with permission).

139 *See* Charles Fried, *Privacy*, 77 YALE L.J. 475, 493 (1968) ("[P]rivacy [i]s that aspect of social order by which persons control access to information about themselves."). Others like to frame privacy as a right to deprive. *See, e.g.*, Jeffrey Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 27, 32 (1995). Others frame it is a limitation on others' access. *See, e.g.*, Gavison, *supra* note 135, at 423 ("Our interest in privacy, I argue, is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention. This concept of privacy as a concern for limited accessibility enables us to identify when losses of privacy occur.").

140 *See Reporters Comm.*, 489 U.S. at 763 ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."). The Court rejected a more "cramped notion of personal privacy" relying upon secrecy. *Id.*

141 *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 81–82 (2010). Nissenbaum's insightful gathering and characterization of philosophies is highly recommended. *See id.* at 67–78; *see also* Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After* Lawrence, 57 UCLA L. REV. 1, 23–25 (2009) (explaining autonomy through a privacy lens).

142 Thomas Nagel, *Concealment and Exposure*, 27 PHIL. & PUB. AFF. 3, 4 (1998).

143 *See* NISSENBAUM, *supra* note 141, at 75–76; Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 483–93 (2015); Reiman, *supra* note 139, at 41–42. Even merely a reminder of the concept of surveillance affects behavior. *See, e.g.*, Melissa Bateson et al., *Cues of Being Watched Enhance Cooperation in a Real-World Setting*, 2 BIOLOGY LETTERS 412 (2006), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1686213/ (finding that people contributed nearly three times as much for drinks when an image of human eyes was displayed nearby); Terence C. Burnham & Brian Hare, *Engineering Human Cooperation*, 18 HUM. NATURE 88, 99 (2007), http://link.springer.com/article/10.1007%2Fs12110-007-9012-2 (finding an increase in simulated public good behavior when an image of a robot with

ity to think freely and critically is essential to full development of one's moral character.[144] This is not to deny, of course, that social pressures can be beneficial ones,[145] but instead only to recognize that they can also be debilitating in the extreme.[146]

Furthermore, without privacy people are (at best) stunted in their ability to form meaningful and diverse relationships, as those relationships depend upon a volitional, gradual, and granular mutual sharing of information.[147] As Nagel explains, "selective intimacy permits some interpersonal relations to be open to forms of exposure that are needed for the development of a complete life. No one but a maniac will express absolutely everything to anyone, but most of us

---

human eyes was displayed); Max Ernest-Jones et al., *Effects of Eye Images on Everyday Cooperative Behavior: A Field Experiment*, 32 EVOLUTION & HUM. BEHAV. 172, 176 (2011), https://www.staff.ncl.ac.uk/daniel.nettle/ernestjonesnettlebateson.pdf (finding that people littered half as often when an image of human eyes was displayed nearby); *see also* MICHEL FOUCAULT, DISCIPLINE AND PUNISH 195–228 (Alan Sheridan trans., 1977) (recognizing the internal significance of feeling watched); CHRISTOPHER SLOBOGIN, PRIVACY AT RISK 92–95 (2007) (building off Foucault's work and others to describe the impact of losing "public anonymity").

In the words of Edward Bloustein, "[t]he man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual." Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 1003 (1964). Or in the words of Ruth Gavison, if subjected to a world without privacy, "[w]e would probably try hard to suppress our daydreams and fantasies once others had access to them. We would try to erase from our minds everything we would not be willing to publish, and we would try not to do anything that would make us likely to be feared, ridiculed, or harmed. There is a terrible flatness in the person who could succeed in these attempts." Gavison, *supra* note 135, at 443.

144 *See* Jeroen van den Hoven, *Information Technology, Privacy, and the Protection of Personal Data, in* INFORMATION TECHNOLOGY AND MORAL PHILOSOPHY 301, 315–16 (Jeroen van den Hoven & John Weckert eds., 2008); NISSENBAUM, *supra* note 141, at 78.

145 *See* William H. Simon, *Rethinking Privacy*, BOS. REV. (Oct. 20, 2014), http://bostonreview.net/books-ideas/william-simon-rethinking-privacy-surveillance ("The second trope of the paranoid style is the portrayal of virtually all tacit social pressure as insidious.").

146 *See, e.g*, Azar Nafisi, *Surveillance States*, N.Y. TIMES (June 11, 2015), http://www.nytimes.com/2015/06/14/books/review/surveillance-states.html ("It stays with you, that fear. It burrows under the skin. Even after you escape and are thousands of miles or many years away, you will still sometimes feel you are being watched. Something within you has been permanently damaged by the terrible knowledge of the human capability for cruelty and your own weaknesses in the face of it.").

147 *See* NISSENBAUM, *supra* note 141, at 84; JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 89, 209–18 (2000); Fried, *supra* note 139, at 477; Gavison, *supra* note 135, at 450. *See generally* IRWIN ALTMAN & DALMAS A. TAYLOR, SOCIAL PENETRATION: THE DEVELOPMENT OF INTERPERSONAL RELATIONSHIPS (1973).

need someone to whom we can express a good deal that we would not reveal to others."[148] As Ferdinand Shoeman explains, "[i]nformation appropriate in the context of one relationship may not be appropriate in another."[149] Indeed, devoid of intended and appropriate context, information can present a vastly incomplete if not completely inaccurate assessment.[150] A spouse, for example, should have sufficient knowledge of a partner that she can place any new information in nearly its correct context, but a stranger, acquaintance, or even fairly good friend might totally misperceive its relevance. As Andrew Taslitz has noted, not only does other-assessment have practical manifestations (e.g., loss of a job opportunity), but psychologically we hold other-assessment dear.[151]

Without privacy, people thus have less fully developed characters and relationships, which in turn are the constituent elements of a robust marketplace of ideas, associations, and religions.[152] In other words, privacy may be critical to the *individual* in a manner necessary to identity formation and to robust small-scale *personal relationships*, but it is ultimately of *collective* societal importance, especially to a democracy.[153] Thus, it is not surprising that Alan Westin found a correlation between political philosophy and privacy throughout western civilization.[154] And there are other ramifications. Without privacy there is increased identity theft, stalking, and other information-

148 Nagel, *supra* note 142, at 10.

149 Ferdinand Schoeman, *Privacy and Intimate Information*, *in* PHILOSOPHICAL DIMENSIONS, *supra* note 135, at 403, 408.

150 *See* WILLIAM JAMES, THE PRINCIPLES OF PSYCHOLOGY (1890), http://psychclassics.asu.edu/James/Principles/prin10.htm ("Properly speaking, a man has as many social selves as there are individuals who recognize him and carry an image of him in their mind. To wound any one of these his images is to wound him. But as the individuals who carry the images fall naturally into classes, we may practically say that he has as many different social selves as there are distinct groups of persons about whose opinion he cares. He generally shows a different side of himself to each of these different groups." (emphasis omitted)).

151 Andrew E. Taslitz & Stephen E. Henderson, *Reforming the Grand Jury to Protect Privacy in Third Party Records*, 64 AM. U. L. REV. 195, 218–19 (2014).

152 *See* NISSENBAUM, *supra* note 141, at 86; PRISCILLA M. REGAN, LEGISLATING PRIVACY 221 (1995).

153 *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1912–18 (2013) (arguing that diminished privacy shrinks the capacity for democratic self-government); Gavison, *supra* note 135, at 455 ("Privacy is also essential to democratic government because it fosters and encourages the moral autonomy of the citizen, a central requirement of a democracy."); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560–63 (1995).

154 *See* WESTIN, HISTORICAL PERSPECTIVES, *supra* note 138, at 4–5, 9.

based or assisted crimes.[155] And given asymmetries of power, distortions in information privacy tend to run solely in one direction, or at least are not distributed equally, benefiting some at the costs of others.[156]

Of course, to assert that information privacy is about control is not to say that one must exercise absolute control. Most rights, and perhaps all rights, are not absolute, and in this case absolute control is unthinkable. First, nobody would benefit from exercising control to achieve absolute seclusion.[157] And society could not permit absolute control, not only because it would have too great a cost to the social order, but also because once any information about me is known to another person, my right of privacy control runs up against their right of free expression.[158]

Fortunately, people innately understand this and rarely, if ever, expect absolute control. But they do wish to exercise some control, even as they are becoming increasingly disillusioned regarding their ability to do so.[159] As sociologist Christena Nippert-Eng explains based upon her recent studies, "[I]t became clear that what I now think of as the process of 'selective concealment and disclosure' plays an important role in how we try to achieve privacy. This is the daily activity of trying to deny or grant varying amounts of access to our

155 *See* NISSENBAUM, *supra* note 141, at 78; Van den Hoven, *supra* note 144, at 311–12 ("information-based harm").

156 *See* NISSENBAUM, *supra* note 141, at 79; Van den Hoven, *supra* note 144, at 312–13 ("informational inequality").

157 *See* Gavison, *supra* note 135, at 440 ("We start from the obvious fact that both perfect privacy and total loss of privacy are undesirable. Individuals must be in some intermediate state—a balance between privacy and interaction—in order to maintain human relations, develop their capacities and sensibilities, create and grow, and even to survive.").

158 *Cf.* Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 496–97 (1975) (striking down a state statute prohibiting the publication of a rape victim's name).

159 *See* MARY MADDEN ET AL., PEW RESEARCH CENTER, PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA 30 (2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf (finding "91% of [American] adults 'agree' or 'strongly agree' that 'consumers have lost control over how personal information is collected and used by companies.'"); Peter H. Schwartz et al., *Patient Preferences in Controlling Access to Their Electronic Health Records: A Prospective Cohort Study in Primary Care*, 30 J. GEN. INTERNAL MED., S25, S27 (2014) (finding almost half of patients will hide certain health information from their health-care providers if given the choice). The Schwartz study is perhaps especially interesting, because as Amitai Etzioni has pointed out, merely asking a person if she would like more privacy is akin to asking whether she would like more health; better information requires recognizing that more of 'x' might have some other cost. Amitai Etzioni, *The Limits of Privacy*, *in* CONTEMPORARY DEBATES IN APPLIED ETHICS 253, 253 (Andrew I. Cohen & Christopher Heath Wellman eds., 2005).

private matters to specific people in specific ways."[160] Nippert-Eng unsurprisingly found disparate people each trying to achieve their preferred balance.[161]

Thus, while any replacement is far less crisp and easy, I have long been a critic of the Fourth Amendment's third party doctrine, which tries to artificially categorize all information as either totally secret (purely private) or freely available to law enforcement (effectively purely accessible).[162] Attempting to force people to maintain absolute secrecy in order to have any degree of constitutional protection is unrealistic and counter-productive.[163]

But what does a control theory of information privacy have to say about investigatory time machines? Obviously at least as to government created ones, there is a serious tension, and it is a tension that goes to the heart of privacy's motivations. Can we fully develop as human beings, with the necessarily divergent ideas and willingness to express them that a thriving democracy requires, if the government is

---

160 CHRISTENA NIPPERT-ENG, ISLANDS OF PRIVACY 2 (2010). Thus, consistent with a control theory, "The goal is to achieve *selectivity* in both [disclosure and concealment]—to carefully choose exactly what is disclosed and concealed, to whom, and how." *Id.* at 7. When people were individually interviewed and asked the very general question, "What does privacy mean to you?", a large majority in some manner described the control theory. *See id.* (noting that the answers of forty-five of fifty-seven participants could be so classified); *see generally* MARY MADDEN ET AL., PEW RESEARCH CENTER, AMERICANS' ATTITUDES ABOUT PRIVACY, SECURITY AND SURVEILLANCE (2015), http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf (finding that Americans want to control who can access their personal information but doubt they are currently able to do so).

161 NIPPERT-ENG, *supra* note 160, at 8 ("For the people in this study [] 'good' privacy exists when the things they want to be private are as private as they want them to be. It's a wonderfully subjective, relativistic standard . . . . [C]ontrol over the amount and type of disclosure and concealment is what really defines their assessment of the situation." (emphasis omitted)); *see also id.* at 5 (positing "[w]hen we think of privacy [] what we really think of is a condition of relative inaccessibility. Any point on the scale has both a degree of privateness and a degree of publicness associated with it" (emphasis omitted)).

162 *See generally* Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH 431 (2013); Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39 (2011) [hereinafter *Timely Demise*]; Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975 (2007); Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373 (2006); Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507 (2005) [hereinafter *Nothing New*].

163 *See* NIPPERT-ENG, *supra* note 160, at 5 ("[A]cquiring privacy is only part of the problem . . . . The totality of the task is to achieve a balance between the need and desire for both privacy and publicity—for a certain degree of concealment and disclosure, for denying and granting access to others." (emphasis omitted)).

always watching? No. Of course, in even the most totalitarian regimes there have proved to be some persons who exercise unpopular autonomy, but then truly pervasive technology like we have today has never before been available. And, more importantly, as Ruth Gavison explains, "Even if we grant that privacy may not be a necessary condition for autonomy for all, . . . it is enough to justify it as a value that most people may require it. We are not all giants, and societies should enable all, not only the exceptional, to seek moral autonomy."[164] An ideal democracy requires thoughtful participation from far more than just a few.

Thus, there is good reason to be extremely skeptical of any government-mandated time machines, and outside of the particular instances in which they have historically been used (e.g., banking, pharmaceuticals, and hotels), we might do best to forbid them, whether constitutionally or otherwise. Indeed, it might be wise to reconsider even those we have historically permitted; the Supreme Court in *Patel* struck down a 116-year-old reporting ordinance.[165] But at the very least, a drone hovering high overhead that records all public movements seems problematic, as do mammoth databases of digital information that can later be searched. On the other hand, broad-based surveillance does have benefits. More inclusive surveillance benefits from a genuine check in the political process, and can more evenly distribute the costs and provide superior accountability.[166] So, is it possible to have our cake and eat it too? If there are sufficiently robust access, use, and disclosure limitations, can they ever ameliorate the very serious privacy concerns? I first address whether such use restrictions could be found within the Fourth Amendment, and then turn to the wisdom of their adoption in the very limited context of police body cameras.

III. FOURTH AMENDMENT USE RESTRICTIONS AND POLICE BODY CAMERAS

In a prescient article from 1995, Harold Krent argued that—whatever definitions of search and seizure are required to make it happen—the uses to which law enforcement can put lawfully ac-

164 Gavison, *supra* note 135, at 450.

165 *See* City of Los Angeles v. Patel, 135 S. Ct. 2443, 2464 (2015) (Alito, J., dissenting).

166 *See* Simon, *supra* note 145 ("[B]road-reach electronic mechanisms have an advantage in addressing the danger that surveillance will be unfairly concentrated on particular groups; targeting criteria, rather than reflecting rigorous efforts to identify wrongdoers, may reflect cognitive bias or group animus.").

quired information should be governed by the Fourth Amendment's reasonableness requirement.[167] According to Krent, "Rapidly developing technology has thrust the use issue to the forefront: what the government does with information may now threaten privacy more than the collection itself."[168] The *Ganias* Second Circuit panel adopted such a use restriction: even if it was permissible for investigators to retain the nonresponsive computer data for such a long period, it was not permissible to search through that data—to use that data—in a new investigation, even pursuant to a newly obtained search warrant.[169] Although it is not clear that Krent would agree with this particular use limitation,[170] he recognized that generally such limits are conducive to the control theory of information privacy: each different use of the data interferes with a person's ability to control *for what purposes* information about her is utilized.[171]

Neither the *Ganias* panel nor Krent argued that use restrictions should be the *sole* Fourth Amendment restrictions: the original law enforcement acquisition remains subject to traditional restraints. For example, merely agreeing to limit use would of course not itself justify compulsory copying of Ganias' hard drives. But there might be circumstances when it is impossible to get the desired law enforcement safety benefit without completely abandoning front-end acquisition restraints, as with broad scale, panvasive drone surveillance, or with broad scale, panvasive internet surveillance for malware.[172] In

---

167 Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 49–51, 51 n.14 (1995).

168 *Id.* at 51. Krent went on to argue for a more specific rule, namely that the only reasonable uses are ones "disclosed or implicit at the time of the underlying seizure," requiring the state to "precommit to all uses of information and items seized." *Id.* at 53; *see id.* at 85–92 (developing this proposed limitation).

169 *See supra* notes 84–92 and accompanying text; *see also* United States v. Davis, 690 F.3d 226, 246, 250 (4th Cir. 2012) (holding the warrantless DNA testing of lawfully seized items from a non-arrestee to constitute an unreasonable Fourth Amendment search); Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1 (2015) (arguing that limited use restrictions are plausible given the necessary over-seizure in the digital search context); *cf.* Commonwealth v. Arzola, 470 Mass. 809, 820 (Mass. 2015) (holding the DNA testing of lawfully seized items from an arrestee did not constitute a Fourth Amendment search).

170 Krent would permit a later use when "the subsequent use would have itself legitimated the initial search." Krent, *supra* note 167, at 93. That would seem true of the later search warrant in *Ganias*. However, as prescient as Krent's article was in 1995, he did not consider the unique nature of computer searches, which might (or might not) alter his conclusions.

171 *Id.* at 51 nn.14 & 18, 92 n.199.

172 Christopher Slobogin has coined the term "panvasive" "to capture the idea that modern government's efforts at keeping tabs on the citizenry routinely and randomly reach across huge numbers of people, most of whom are innocent of any wrongdoing." Christopher

each instance, assuming complete automation, the key privacy harm seems to occur only upon human viewing, or use. Of course, this does not mean the sole privacy harm occurs upon use. If human-programmed algorithms are making decisions based upon content, that seems a relevant use regardless of the lack of direct human observation.[173] And, as described above, knowing that all of our movements, online or off, will be recorded for potential later perusal can very meaningfully chill those actions. Jeremy Bentham long ago realized that constant observation was not necessary in his Panopticon; merely its potential was sufficient to achieve the same results.[174] Thus, European courts have recently rejected requirements that internet service providers retain information for defined periods of time.[175]

So, we should be extremely cautious in accepting ex-post use and dissemination controls as a substitute for—as opposed to a supplement to—front-end acquisition controls. But as part of this calculus we should recognize the benefits of broad access, including its more uniform distribution and thus greater political accountability. As I argued some ten years ago, whether the issue is DNA databanking or a thermal scan of homes or a millimeter wave scan of persons (as now takes place at airports), advanced notice and broad and uniform applicability trigger the protections of the political process in a way that most contemporary policing does not, and this should factor into Fourth Amendment reasonableness.[176] In this, I was building upon

---

Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721, 1723 (2014).

173 *See* Henderson, *Timely Demise*, *supra* note 162, at 47–48 (responding to argument of Richard Posner); *see also* SCHNEIER, *supra* note 15, at 130 ("Whether or not anyone actually looks at our data, the very facts that (1) they could, and (2) they guide the algorithms that do, make it surveillance.").

174 *See The Panopticon*, UCL BENTHAM PROJECT, https://www.ucl.ac.uk/Bentham-Project/who/panopticon (last visited Feb. 19, 2016). George Orwell used the same concept in his 1984: "There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized." GEORGE ORWELL, 1984, at 4 (1949).

175 *See* Davis v. Sec'y of State for Home Dep't, [2015] QBD 3665, https://www.judiciary.gov.uk/wp-content/uploads/2015/07/davis_watson_order.pdf (invalidating UK data retention law); Case C-293, Dig. Rights Ir. Ltd. v. Minister for Commc'ns, 2014 E.C.R. 845, http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN (invalidating the 2006 Data Retention Directive).

176 *See* Henderson, *Nothing New*, *supra* note 162, at 555–59.

the arguments of William Stuntz[177] and the Supreme Court's school drug testing cases.[178] Christopher Slobogin has recently developed the concept into a more rich theory of representative democracy—relying upon the constitutional scholarship of John Hart Ely—that would provide judicial review even where the government activity does not constitute a Fourth Amendment "search" or "seizure."[179]

But again, whatever the benefits of even a well-functioning political process, there are strong reasons to be cautious. As Justice Sandra Day O'Connor argued in personally rejecting the Court's permissive regime of drug testing for student athletes, we have a strong tradition against general warrants, and "[b]lanket searches, because they can involve thousands or millions of searches, pose a greater threat to liberty than do suspicion-based ones, which affect one person at a time."[180] Nonetheless, it would be just as wrong to ignore the fairness benefit of broad applicability, as it would to think a "misery loves company" conception would be ideal across the board (the latter of which would adopt wholesale the hated general warrants of our founding period).[181]

It seems there might be limited, relatively narrow circumstances in which we should embrace solely use restrictions, and I submit that one of them might be for law enforcement body cameras. Of course, perhaps this is an unfairly easy case, because in order for the camera to capture anything, the law enforcement officer should already be lawfully present, a criterion that brings its own sometimes-significant front-end restrictions. But such recording nonetheless creates time machines, and lots of them: there are almost a million law enforcement officers in the United States.[182] With officers on duty at all

177 *See* William J. Stuntz, *Local Policing After the Terror*, 111 Yale L.J. 2137, 2166 (2002) ("[S]preading the cost of policing through a larger slice of the population . . . reduces the odds of voters demanding harsh and intrusive police tactics secure in the knowledge that those tactics will be applied only to others.").

178 *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 664 (1995) ("In many respects, we think, testing based on 'suspicion' of drug use would not be better, but worse."). In its drug testing cases, the Court has also been swayed by use restrictions, holding searches reasonable in part based upon the limited government use of positive testing. *See* Henderson, *Nothing New*, *supra* note 162, at 560–61.

179 *See* Slobogin, *supra* note 172, at 1724, 1733–37.

180 *Vernonia*, 515 U.S. at 667 (internal quotation marks omitted).

181 *See* Delaware v. Prouse, 440 U.S. 648, 664 (1979) (Rehnquist, J., dissenting) (deriding a "misery loves company" Fourth Amendment jurisprudence).

182 NATIONAL LAW ENFORCEMENT OFFICERS MEMORIAL FUND, LAW ENFORCEMENT FACTS: KEY DATA ABOUT THE PROFESSION, http://www.nleomf.org/facts/enforcement/ (last visited Mar. 3, 2016); *see also By the Numbers: How Many Cops Are There In the USA?*, THE SKEPTICAL LIBRARIAN (Aug. 26, 2014), http://blog.skepticallibertarian.com/2014/08/26/by-the-numbers-how-many-cops-are-there-in-the-usa/.

times, watching over mostly innocent behavior as well as some criminal, if every one records his or her entire shift, that is a staggering amount of data.

Those recordings will psychologically affect the officers, and not only in the sense of promoting good behavior. As discussed above, nobody does well to be under constant surveillance (though, interestingly, to many thousands of Americans working in retail and other industries it is probably already their daily reality—albeit without accompanying audio—and these workers might have little to no promises regarding ex-post use and dissemination). Nor is it the case that these recordings will merely duplicate what officers could themselves personally explain. Instead, high quality cameras would record all sorts of events and details never noticed by the officers, and potentially permanently store them for later high-tech perusal (e.g., zoom in and slow down).[183] Moreover, for things an officer does notice—which will include highly traumatic events—the digital record will remain forever pristine, whereas memories quickly degrade and even fade entirely.[184] Such cameras would record not "only" events taking place in public, but instead would record everywhere officers go, including the interiors of our homes and therefore potentially under every bed and into every drawer. So even if officer presence already has an access (and thus acquisition) limitation, it would not necessarily follow that nothing more should be required for the further intrusion of recording.[185]

However, these panvasive qualities of officer recording also make for some of its benefits. As long as there have been police, we have had to rely not only upon their perceptions of what they observe, but upon their memories of those perceptions. Both perception and

183 Of course, sometimes a camera's preserving things unnoticed is precisely its utility. *See* MARC JONATHAN BLITZ, POLICE BODY-WORN CAMERAS: EVIDENTIARY BENEFITS AND PRIVACY THREATS 5–6 (2015).

184 On the benefits of human forgetting, see Henderson, *supra* note 11, at 708–09. As Bruce Schneier has stated in the online context, "I used to say that Google knows more about what I'm thinking of than my wife does. But that doesn't go far enough. Google knows more about what I'm thinking than I do, because Google remembers all of it perfectly and forever." SCHNEIER, *supra* note 15, at 22. And it gets still more privacy invasive, because via data mining Google can learn correlations and patterns in your thinking of which you have *never* been consciously aware.

185 At the very least such videos should not all become public records, as might be the default in some jurisdictions. *See, e.g.*, Jessica Bruha, *Local Law Enforcement Testing Body Cams*, NORMAN TRANSCRIPT (Sept. 21, 2014), http://www.normantranscript.com/news/local-law-enforcement-testing-body-cams/article_c61e8ff4-4052-11e4-b4eb-eb2c7f02e600.html ("[D]ue to a law going into effect . . . the video becomes public record and the department is obligated to turn over a copy to any member of the public.").

memory are fallible, and recollection thereof subject to falsification. Of course, we have done what we can. Because memory dissipates quickly, it is helpful when police contemporaneously record their perceptions, and hence we value the ubiquitous police report (which also "freezes" the account, making later fabrication more difficult). With the advent of readily mobile photography, police could better preserve those observations deemed sufficiently important, and photography of crime scenes thus became routine.[186] With the advent of tape recording, certain police-citizen interactions were recorded.[187] And with the advent of videotaping, we became accustomed to its benefits in certain contexts, such as video recordings of traffic stops via cameras fixed in police vehicles. But when that videotaping made it to the interior of the home, it caused concern, a concern that reached the Supreme Court in 1999 in the case of *Wilson v. Layne*.[188]

---

186 Yet that photography has sometimes proved controversial when used to fill "gang books" of known and suspected gang members for use in future investigations, when part of a restaged arrest to permit the press a perp walk, or—in its most modern manifestation—when an officer took his own selfie during a perp walk. *See* Lauro v. Charles, 219 F.3d 202, 213 (2d Cir. 2000) (holding unconstitutional a restaged perp walk because it had no legitimate law enforcement purpose); Brown v. Pepe, 42 F. Supp. 3d 310, 316 n.10 (D. Mass. 2014) (holding an officer's "selfie" was at most a de minimis privacy intrusion); Commonwealth v. Cao, 644 N.E.2d 1294, 1296–99 (Mass. 1995) (holding the procedure used to obtain a photograph for a gang book did not constitute a seizure); People v. Rodriguez, 26 Cal. Rptr. 2d 660, 663–64 (Cal. Ct. App. 1993) (holding unconstitutional a stop used to obtain a photograph for a gang book).

187 Tape recording likewise sometimes proved controversial, especially in the undercover context. *See, e.g.*, United States v. White, 401 U.S. 745, 753 (1971); Lopez v. United States, 373 U.S. 427, 439 (1963).

188 526 U.S. 603 (1999); *see also* Oziel v. Superior Court of L.A. Cnty., 223 Cal. App. 3d 1284, 1296, 1302 (Cal. Ct. App. 1990) (not deciding the constitutionality of police videotaping the execution of a search warrant but refusing media access to that footage). Since *Wilson*, media presence has continued to cause potential Fourth Amendment violations. *See, e.g.*, United States v. Hendrixson, 234 F.3d 494, 496 (11th Cir. 2000) (holding that media involvement at the execution of a search warrant in a home was a Fourth Amendment violation, but did not require exclusion of evidence); Smart v. City of Miami, 2015 WL 3409329, at *12–13 (S.D. Fla. May 27, 2015) (finding plaintiff's § 1983 claim sufficient to overcome summary judgment based on the theory that police inviting a crew from "First 48" to film plaintiff's home was a violation of the Fourth Amendment); Carr v. Montgomery Cnty., 59 F. Supp. 3d 787, 798 (S.D. Tex. 2014) (finding a plausible § 1983 claim for bringing a third-party film crew into a home to videotape a warrantless search); Frederick v. Biography Channel, 683 F. Supp. 2d 798, 799–802 (N.D. Ill. 2010) (finding a plausible § 1983 claim against a media company where plaintiffs were detained longer than police needed for arrest, just so that a film crew could arrive to cover it); Conradt v. NBC Universal, Inc., 536 F. Supp. 2d 380, 383 (S.D.N.Y. 2008) (finding plausible § 1983 and intentional-infliction-of-emotional-distress claims against media defendant for their show "To Catch a Predator" having an unusually pervasive presence and influence throughout an investigation that led the target to eventually commit suicide); Thompson v. State, 824 N.E.2d 1265, 1266, 1268–69, 1271 (Ind. Ct. App. 2005) (holding that a film crew's pres-

As part of "Operation Gunsmoke," United States Marshals were working with local Maryland police to apprehend dangerous criminals, including one Dominic Wilson.[189] Unfortunately, the address in police files was that of Wilson's parents, so when police entered the home to execute an arrest warrant—accompanied by invited representatives of the media—what they found was Dominic's father roused from bed and dressed only in briefs and Dominic's mother in a nightgown.[190] Before police were made aware of, or at least were convinced of, their mistake, they forcibly subdued the elder Mr. Wilson at gunpoint while a photographer from the Washington Post took photographs.[191] The Court unanimously held that the officers violated the Fourth Amendment by bringing representatives of the media into a home entered pursuant to a warrant.[192] However, the Court acknowledged government interests that could be furthered by law enforcement's own recording: accurately publicizing efforts to combat crime (furthering education and deterrence), deterring and detecting police abuse, protecting the safety of officers, and preserving evidence.[193] Thus, "it might be reasonable for police officers to themselves videotape home entries."[194]

The benefits the Court proffered are real and can be significant. As for evidence preservation, recording can preserve evidence without requiring its physical removal;[195] preserve evidence that would

---

ence during a strip search in the defendant's motel room violated the defendant's Fourth Amendment rights and warranted exclusion of the evidence gained during that search).

189 *Wilson*, 526 U.S. at 606.

190 *Id.* at 607.

191 *Id.*

192 *Id.* at 614. Eight Justices believed, however, that before this decision the law was not clearly established, and therefore that the officers enjoyed qualified immunity. *See id.* at 615; *id.* at 618 (Stevens, J., dissenting in part). On the merits, the Court also distinguished circumstances in which a party is brought in the home to assist the police in their task, as when a citizen is brought along to identify stolen property. *See id.* at 611–12.

193 *See id.* at 612–13.

194 *Id.* at 613.

195 This can serve First Amendment, privacy, law enforcement, and practical values. As for the First Amendment, see, for example, *City of Cincinnati v. Contemporary Arts Center*, 566 N.E.2d 207, 213 (Ohio Mun. 1990) (approving of officers executing a search warrant by videotaping an allegedly obscene art exhibit, which negates otherwise serious concerns of pre-adjudication censorship). As for privacy, in some circumstances it might be difficult for police to distinguish what is subject to seizure, and if probable cause justifies a greater seizure, recording might provide a lesser invasion. For example, in *Commonwealth v. Balicki*, 762 N.E.2d 290, 294–95 (Mass. 2002), defendants were believed to have purchased household items with public funds. In such a case, there might be nothing about tainted items that immediately commands attention, yet there might be probable cause (fair probability) to seize a great portion of them. Similarly, federal agents involved in the 2005 search of Representative William Jefferson's home opted to photograph documents

otherwise be destroyed by investigatory or non-investigatory government actions, or simply by the passage of time;[196] and preserve evidence in its most pristine form, allowing a judge or juror to view it herself.[197] One could imagine recordings being used to routinely decide such contested issues as whether a person consented to an entry or search, and if so, the scope of that consent; whether a reasonable officer would have believed a person to be in need of immediate assistance; whether there was a fair probability that evidence would be imminently destroyed; whether police exceeded the authorization of a warrant; or whether an officer reasonably believed deadly force was justified.[198] To be sure, no single video is "perfect," as the camera

---

for which they alleged probable cause, and thus for which they could have executed a "plain view" warrantless seizure, because the documents were not directly responsive to the warrant's list of seizable items. United States v. Jefferson, 571 F. Supp. 2d 696, 700 (E.D. Va. 2008). As for practicality, there will of course be instances in which physical seizure is impractical or even impossible. *See, e.g.*, People v. Bambino, N.Y. L.J. 25 (Aug. 4, 1992) (Nassau Cnty. Justice Ct. 1992) (photography/videography where defendants were believed to have an apartment in their basement in violation of applicable zoning law); State v. Dickerson, 313 N.W.2d 526, 530 (Iowa 1981) (photography of tire tracks). And as for law enforcement interests, it might be necessary to preserve evidence without tipping off a suspect. *See, e.g.*, United States v. Villegas, 899 F.2d 1324, 1330 (2d Cir. 1990) (authorizing a "sneak and peak" or "covert entry" warrant to search a property for evidence of cocaine manufacturing that would be photographed but not physically seized).

196 This interest arises whenever police entry is predicated upon emergency aid, during which their protective actions will sometimes destroy unseen or in-the-moment unappreciated evidence (or during which a malicious officer could destroy "undesirable" evidence). It also arises when victims' bodies are to be moved. *See, e.g.*, Forbes v. State, 1995 WL 241722, *5–6 (Tex. App. 1995) (permitting photography and videotaping prior to medical examiner and photography by medical examiner); State v. Wright, 558 A.2d 946, 950–51 (R.I. 1989), *abrogated on other ground recognized by* State v. Brennan, 627 A.2d 842, 848 (R.I. 1993) (same); State v. Anderson, 599 P.2d 1225, 1230 (Or. App. 1979) (permitting videotaping prior to removal of victim's body); Patrick v. State, 227 A.2d 486, 488–90 (Del. 1967) (permitting photography prior to removal of victim's body). Or when there is a fire. *See, e.g.*, Michigan v. Clifford, 464 U.S. 287, 289 (1984) (reaffirming and applying these principles); Michigan v. Tyler, 436 U.S. 499, 510–12 (1978) (establishing three tiered structure for searches of fire scenes); Schultz v. State, 593 P.2d 640, 643 (Alaska 1979) (permitting photography during emergency fire search); Dubbs v. State, 157 S.W.2d 643, 645 (Tex. Crim. App. 1942). And sometimes evidence is naturally evanescent, such as a pool of blood not yet dried into a carpet, which might indicate something about the time of an attack or other relevant event. *See, e.g.*, Ortega v. State, 669 P.2d 935, 942 (Wyo. 1983) (permitting photography to preserve evanescent evidence, though in an opinion fraught with scientific error and weak legal reasoning), *overruled in part on other grounds*, Jones v. State, 902 P.2d 686, 692 (Wyo. 1995).

197 *See, e.g.*, Scott v. Harris, 550 U.S. 372 (2007) (relying upon dash camera video to hold officers acted reasonably in using deadly force). The Supreme Court has noted this evidentiary advantage in the context of undercover recordings. *See* United States v. White, 401 U.S. 745, 753 (1971); Lopez v. United States, 373 U.S. 427, 439 (1963).

198 *See, e.g.*, Ohio v. Robinette, 519 U.S. 33, 35 (1996) (noting dash camera video that was presumably used in determining consent to search); United States v. Bah, 794 F.3d 617, 622 n.1 (6th Cir. 2015) (noting use of dash camera video to determine reasonable suspi-

perspective can itself suggest a cognitive frame and thereby affect these myriad determinations.[199] But it is far better than without. In the straightforward words of the Alaska Supreme Court in the context of recording custodial interrogations, "a recording will help trial and appellate courts to ascertain the truth."[200]

Thus, preservation has secondary benefits, including in deterring and detecting police abuse. There are ample recorded examples, from detectives playing Wii Bowling during a home search,[201] to accident investigators "do[ing] a little Walt Disney to protect [a] cop" who rear-ended another vehicle.[202] The most prominent recent ex-

---

cion); Rudlaff v. Gillispie, 791 F.3d 638, 639 (6th Cir. 2015) (using dash camera to determine excessive force); Green v. Throckmorton, 681 F.3d 853, 862 (6th Cir. 2012) (using dash camera to determine whether reasonable suspicion was materially disputed); Lee v. Anderson, 616 F.3d 803, 812 (8th Cir. 2010) (noting jury's use of video in determining whether deadly force was reasonable and relying upon video in denying claim of insufficient evidence); United States v. Nicholson, 17 F.3d 1294, 1296 (10th Cir. 1994) (noting magistrate's use of dash camera video in determining consent); United States v. Abarza, No. 1:14–cr–179–MC, 2015 WL 69556684, at *1–3 (D. Or. Nov. 6, 2015) (noting the usefulness of dash camera footage and using it to negate allegations like "high-crime area" and nervousness); Burnett v. Unified Gov. of Athens-Clarke Cnty., No. 3:08-CV-04 (CDL), 2009 WL 5175296, at *6 (M.D. Ga. Dec. 22, 2009) (noting defendant's refusal to consent in dash camera video); Commonwealth v. Griffin, 116 A.3d 1139, 1143–44 (Pa. Super. Ct. 2015) (using dash camera footage to determine the extent of physical manipulation during a Terry stop); Lampkin v. State, 470 S.W.3d 876, 888–89 (Tex. Ct. App. 2015) (using dash camera footage used to determine whether defendant was intoxicated); Scott v. State, 559 So. 2d 269, 272 (Fla. Dist. Ct. App. 1990) (noting that video of search warrant execution did not conflict with trial court's findings regarding knock and announce); Kimberly Kindy & Julie Tate, *Police Withhold Videos Despite Vows of Transparency*, WASH. POST (Oct. 8, 2015), http://www.washingtonpost.com/sf/national/2015/10/08/police-withhold-videos-despite-vows-of-transparency/ (discussing utility of police body cameras in fatal shootings); Richard Perez-Pena, *Officer Indicted in Shooting Death of Unarmed Man*, N.Y. TIMES, July 29, 2015, at A1 (describing use of officer body camera in murder indictment). This is of course a benefit in the videotaping of interrogation. *See, e.g.*, State v. Hajtic, 724 N.W.2d 449, 454–56 (Iowa 2006) (relying upon and encouraging such recording).

199 *See generally* Kwangbai Park & Jimin Pyo, *An Explanation for Camera Perspective Bias in Voluntariness Judgment for Video-Recorded Confession: Suggestion of Cognitive Frame*, 36 LAW & HUM. BEHAV. 184–85 (2012).

200 Stephan v. State, 711 P.2d 1156, 1161 (Alaska 1985).

201 *See* Steve Andrews, *Polk Sheriff Disciplines Wii-Playing Deputies*, TAMPA TRIB., Nov. 11, 2009, at 4; Steve Andrews, *A Wii Bit Distracted*, TAMPA TRIB., Sept. 22, 2009, at 1.

202 *See* Tonya Alanez, *Ex-Hollywood Officers Accused of Falsifying Crash Report Now Face Federal Lawsuit*, SUN SENTINEL (June 4, 2010), http://articles.sun-sentinel.com/2010-06-04/news/fl-hollywood-cops-federal-lawsuit-20100604_1_andrea-tomassi-officer-dewey-pressley-officer-joel-francisco; Tonya Alanez, *DUI Charge Dropped After Cops Accused of Crash Cover-Up*, SUN SENTINEL (July 30, 2009), http://articles.orlandosentinel.com/2009-07-30/news/hollywood_1_dui-charge-finkelstein-broward-state-attorney; *see also* Jim Dwyer, *Videos Challenge Accounts of Convention Unrest*, N.Y. TIMES, April 12, 2005, at A1, B4 (reporting on videotape contradicting police reports concerning arrests at the 2004 Republican National Convention); Jim Dwyer, *A Switch Is Flipped, and Justice Listens In*, N.Y. TIMES

amples might be the shootings of Walter Scott and Samuel Dubose, each of which resulted in murder charges against the police officer.[203] It seems self-evident that video would deter (and where that fails, detect) abuse, an inference supported by police recording in Rialto, California. In the first year of body camera recording, complaints against officers fell by 88% and use of force by officers fell by almost 60%.[204] Thus, in Judge Shira A. Scheindlin's 2013 order holding unconstitutional the New York Police Department's stop and frisk tactics, she required a trial program of officer body cameras.[205] To be most effective, that video must record all police-citizen interaction—lest officers only turn it on when it serves their purposes[206]—and be

(Dec. 8, 2007), http://www.nytimes.com/2007/12/08/nyregion/08about.html?pagewanted=print&_r=0 (reporting on an officer falsely claiming a recorded interrogation had never taken place); John Eligon, *No Jail for Ex-Officer Over Toppled Bicyclist*, N.Y. TIMES, July 15, 2010, at A26 (reporting on an incident in which a New York City officer body slammed a bicyclist and then, adding insult to injury, charged him with attempted assault and disorderly conduct); Sasha Goldstein, *Police Dash Cam Video Exonerates New Jersey Man, Leads to Indictment of Cops*, N.Y. DAILY NEWS (Feb. 25, 2014), http://www.nydailynews.com/news/crime/police-dash-cam-video-exonerates-nj-man-implicates-cops-article-1.1701763 (reporting on dash camera footage that exonerated a man from evading arrest and proved police had falsified records); David A. Graham, *The Death of Jeremy Mardis and the Honesty of the Police*, ATLANTIC (Nov. 12, 2015), http://www.theatlantic.com/national/archive/2015/11/the-death-of-jeremy-mardis-and-trustworthy-police/415437/ (reporting police lying about an incident that left a 6-year-old boy dead and the body camera footage that proved it); Kim Minugh, *Faked Reports Put Cop in Jail*, SACRAMENTO BEE (Apr. 20, 2013), http://www.sacbee.com/mobile/bees-best/article2577255.html (reporting on an officer who provided false information in a number of police reports); Joe Sharkey, *A Constitutional Case in a Box of Cash*, N.Y. TIMES, Nov. 17, 2009, at B5 (reporting on an illegitimate and abusive detention of an airplane passenger for carrying a significant amount of cash).

203 *See* Alan Blinder & Timothy Williams, *Ex-South Carolina Officer Is Indicted in Shooting Death of Black Man*, N.Y. TIMES, June 9, 2015, at A12; *see also* Perez-Pena, *supra* note 198; Damien Cave & Rochelle Oliver, *The Videos That Are Putting Race and Policing into Sharp Relief*, N.Y. TIMES (updated Oct. 27, 2015), www.nytimes.com/interactive/2015/07/30/us/police-videos-race.html (gathering videos depicting numerous instances of alleged excessive use of force by the police).

204 *See* Ian Lovett, *In California, a Champion for Police Cameras*, N.Y. TIMES (Aug. 21, 2013), http://www.nytimes.com/2013/08/22/us/in-california-a-champion-for-police-cameras.html; *see generally* MICHAEL D. WHITE, POLICE OFFICER BODY-WORN CAMERAS: ASSESSING THE EVIDENCE (2014), https://www.ojpdiagnosticcenter.org/sites/default/files/spotlight/download/Police%20Officer%20Body-Worn%20Cameras.pdf (articulating the strengths and weaknesses of available empirical evidence).

205 Floyd v. City of New York, 959 F. Supp. 2d 540, 563 (S.D.N.Y. 2013).

206 *See* LINDSAY MILLER & JESSICA TOLIVER, POLICE EXECUTIVE RESEARCH FORUM, IMPLEMENTING A BODY-WORN CAMERA PROGRAM: RECOMMENDATIONS AND LESSONS LEARNED 12–14 (2014), http://www.justice.gov/iso/opa/resources/472014912134715246869.pdf (describing ACLU position that would require recording all police-citizen interaction, but also describing counter arguments); *see id.* at 40–42 (making particular recommendations); Ill. S.B. 1304 § 10-20(a)(3) (requiring, with articulated exceptions, that "[c]ameras must be turned on at all times when the officer is in uniform and is re-

tamper-resistant.[207] And when it comes to deterring and detecting abuse, turnabout is fair play. Recording can shield police against false allegations of abuse as well as deter or at least detect poor citizen decisions, perhaps including some that caused those previously unrecorded use of force incidents.

So, given the myriad benefits of tamper-resistant, always-on officer recording—where "always on" includes cameras with a significant, typically-overwritten buffer meant to become permanent when triggered by an officer-citizen interaction—it seems such recording is worth the privacy cost. But this merely means police should record. It remains to be determined—or should remain to be determined—what can be done with those recordings, which of course preserve immense amounts of otherwise ephemeral irrelevant information like the takedown of an innocent man in his bedclothes in *Wilson v. Layne*. The mere preservation of that information is a meaningful harm, if nothing else because the relevant parties know there is always a risk of its further consumption and dissemination.[208] And thus recording can also harm law enforcement interests if it deters citizen cooperation and assistance where persons fear criminal reprisal. Thus, as an administrative matter in police department guidelines, as a legislative matter, and—I would argue—as a matter of Fourth Amendment (and state constitutional analog) reasonableness, there should be use and disclosure limitations on that data. These would include security from unauthorized access, need-to-know limitations, audit logs, and destruction schedules.[209]

For example, viewing the footage of a home search should at least sometimes itself constitute a Fourth Amendment search, just like perusing a seized computer. Reentering the home after completion of the search would of course require a new warrant,[210] and just as a

---

sponding to calls for service or engaged in any law enforcement-related encounter or activity").

207 *See, e.g.*, Dwyer, *supra* note 202 (describing prosecution use of a misleadingly edited police video; the prosecution was dropped when defense attorneys obtained the unedited version); Allesandra Ram, *Sandra Bland's Arrest Footage Shows How Fallible Video Can Be*, WIRED (July 22, 2015, 6:32 PM), http://www.wired.com/2015/07/sandra-blands-arrest-footage-shows-fallible-video-can/ (describing recent instance in which odd edits to a controversial police video seem to be only technical glitches).

208 For a telling example, see *Commonwealth v. Balicki*, 762 N.E.2d 290, 295–96 (Mass. 2002), in which the court describes in detail the many innocent details preserved by the recording of a home search. In today's "reality television" pseudo-celebrity obsessed culture, many might be most interested in the criminally irrelevant portions of a search.

209 *See, e.g.*, STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS §§ 25-6.1, 25-6.2 (3d ed. 2013); *see also* Ill. S.B. 1304 § 10-20(a)(7).

210 WAYNE R. LAFAVE ET AL., 2 CRIM. PROC. § 3.4(j).

search of a seized hard drive yields previously unknown information, viewing of video will yield information not noticed by officers, and—given video enhancement capabilities—information not previously noticeable. Moreover, the resource and legal restraints are far different when any number of officers can view video in their offices than when those officers are on the scene executing a search warrant governed by the constraints of the Fourth Amendment, potentially including a judicial warrant. Thus, just as courts have begun to recognize that "digital is different" in other contexts, courts should here recognize a meaningful difference in kind despite law enforcement officers traditionally being permitted to re-examine physical items in their possession. The over-seizure inherent in the recording merits a different result.

So understood, in the limited context of police body cameras, the benefits of complete recording seem to outweigh the costs, and therefore this is a government time machine that I would permit subject only to meaningful access, use, and dissemination controls. This of course leaves for future work the development of a taxonomy as to when acquisition restrictions are more or less important, and what should be the constitutional and statutory rules and administrative best practices. But it provides a critical perspective as we approach these decisions, seeing them for what they are: Fourth Amendment time machines.

CONCLUSION

We are in the midst of dramatic techno-social change. In the words of Christena Nippert-Eng:

> It's as if a distinct cultural climate change is underway. The ocean has risen, shrinking our islands of privacy and even submerging many of them altogether. Like Atlantis, perhaps, some private spaces and times and matters are fading into the realm of folklore—even legend—their very existence destined to rest one day on the unsubstantiated claims of prior generations.[211]

The ability of technology for the first time to feasibly record and store most all behavior—both online and off—is certainly a tectonic shift. It seriously threatens privacy, and thus all of privacy's myriad individual and societal benefits.

Of course, any such shift can be exaggerated, and in some sense little is ever new. In 1890, with the advent of the portable camera, a newspaper bemoaned that, "This season there is something at the

211 NIPPERT-ENG, *supra* note 160, at 3–4.

seaside worse than sharks. It is the amateur photographer."[212] Yet we somehow made it through, sufficient privacy intact. Laws have long required that certain records be retained, and businesses have long retained far more than what the laws require.

Nonetheless, differences in scope at some point become differences in kind, and I believe there is utility in recognizing today's digital records for what they are—investigative time machines—and openly confronting whether their benefits justify their costs. Where they do, we should utilize access, use, and dissemination restrictions for our privacy. And in those instances in which only a panvasive time machine will do, and in which its benefits still outweigh its costs, we can rely solely upon those ex post restrictions.[213] But these time machines are fraught with great danger to our humanity and to our democracy, and thus should be approached with a healthy, if not vigorous distrust. Thus, in this Article I have taken only a baby step, recommending a use restriction regime for police officer body cameras, recognizing that officer presence builds in acquisition restraints. Legislatures should provide frameworks for these recordings, requiring reasonable guarantees of secure storage and appropriately restricting and disciplining errant access, use, and dissemination.[214] If those restrictions ultimately prove unworkable or insufficient in this

212 *Every Step You Take*, ECONOMIST (Nov. 16, 2013), http://www.economist.com/news/leaders/21589862-cameras-become-ubiquitous-and-able-identify-people-more-safeguards-privacy-will-be.

213 In the context of the NSA bulk telephony metadata surveillance, the Privacy and Civil Liberties Oversight Board recognized that to justify a program solely restricted by use restrictions should require "a strong showing of efficacy." PCLOB REPORT, *supra* note 42, at 13.

214 A growing chorus of voices recognizes the role a legislature should play, and in the relevance of that role to constitutionality. *See, e.g.*, ACLU v. Clapper, 785 F.3d 787, 824–25 (2d Cir. 2015) ("We note first that whether Congress has considered and authorized a program such as this one is not irrelevant to its constitutionality. The endorsement of the Legislative Branch of government provides some degree of comfort in the face of concerns about the reasonableness of the government's assertions of the necessity of the data collection . . . . [T]he legislative process has considerable advantages . . . . A congressional judgment as to what is 'reasonable' under current circumstances would carry weight—at least with us, and, we assume, with the Supreme Court as well—in assessing whether the availability of information to telephone companies, banks, internet service providers, and the like, and the ability of the government to collect and process volumes of such data that would previously have overwhelmed its capacity to make use of the information, render obsolete the third-party records doctrine or, conversely, reduce our expectations of privacy and make more intrusive techniques both expected and necessary to deal with new kinds of threats . . . . Ideally, such issues should be resolved by courts only after [executive and legislative] debate, with due respect for any conclusions reached by the coordinate branches of government.").

limited context, then we will have learned that they certainly cannot alone be trusted in other spheres.