Oklahoma Law Review

Volume 66 | Number 4

2014

Our Records Panopticon and the American Bar Association Standards for Criminal Justice

Stephen E. Henderson
University of Oklahoma College of Law, sehenderson@ou.edu

OUR RECORDS PANOPTICON AND THE AMERICAN BAR ASSOCIATION STANDARDS FOR CRIMINAL JUSTICE

STEPHEN E. HENDERSON*

"Secrets are lies. Sharing is caring. Privacy is theft."[1] *So concludes the main character in Dave Egger's novel,* The Circle*, in which a single company that unites Google, Facebook, and Twitter—and on steroids—has the ambition not only to know, but also to share, all of the world's information. It is telling that a current dystopian novel features not the government in the first instance, but instead a private third party that, through no act of overt coercion, knows so much about us. This is indeed the greatest risk to privacy in our day, both the unprecedented, massive collection and retention by third parties of private information, and then*

* 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 symposium participants for bringing their expertise to Norman, Oklahoma, and to my colleague Joseph Thai for moderating the symposium panels. I am likewise grateful to the members of the *Oklahoma Law Review* for their exceptional planning, for the hospitality provided to our guests, and for their hard work in editing this symposium volume. In particular, I thank Editor-in-Chief Selby Brown, Symposium Editor Charles Knutter, and Assistant Symposium Editor Amanda Lee.

1. DAVE EGGERS, THE CIRCLE 303 (2013). For a fun, albeit distressing, summary of arguments against privacy, see *id.* at 276-304. In a nutshell, if there were no privacy, there would be little to no crime: Why do the crime when you know not only that you will "do the time," serving any set penalty, but that you will also suffer immediate and certain social approbation? *Id.* at 280. Moreover, if all were known, it would prevent people from forming a misleading impression of others based only on knowing a few characteristics or events. *See id.* at 286-87. As for those things we are embarrassed for others to see, one of two things will allegedly happen: either that behavior will be found sufficiently normal that we will no longer be embarrassed, or it will become clear that the behavior actually is deviant and so we should stop. *Id.* at 288. Google CEO Eric Schmidt seems to be a believer: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." Cade Metz, *Google Chief: Only Miscreants Worry About Net Privacy*, REGISTER (Dec. 7, 2009), http://www.theregister.co.uk/2009/12/07/schmidt_on_privacy/ (quoting Eric Schmidt). And why is privacy theft? Because you steal from those who could otherwise have vicariously experienced through you, including those physically, mentally, financially, or otherwise unable to do so on their own. *See* EGGERS, *supra*, at 299-304.

Missing from all of these proffered arguments, of course, is the remarkable richness of varied and unique personal relationships, all the experimenting and growth that those relationships encourage, and all the joy and carefree spontaneity they bring to what could otherwise be a remarkably unfriendly and dreary existence.

secondarily the access to that information by others, including law enforcement. For the past seven years, from 2006 to 2013, I served as the Reporter in drafting the black letter and commentary to what is now the twenty-fifth volume of the American Bar Association Standards for Criminal Justice, this volume relating to law enforcement access to third party records. Considering the talent that served on the Task Force and Standards Committee, and the significant vetting of the ABA process, it would be surprising if the Standards did not get many things right, and hopefully that is evident in the Standards themselves. But inevitably any first-of-its-kind project of this magnitude will be imperfect and incomplete. Continuing to move the conversation forward was my purpose in organizing this Symposium. The articles in this volume are a testament to its success, and here I explain the drafting of the Standards, including a few substantive highlights, and place the Standards in their unique historic context. We have begun to capture, record, and analyze everything within given domains, as opposed to selectively preserving only what is contemporaneously considered relevant or necessary. As we step into this brave new world, the Standards have great value not only to our democratic decision makers, but to all of us, as we seek to reap its benefits without sacrificing our privacy, and with that privacy our individuality and even our personhood.

I. The World in Which We Live

In late 2006, the American Bar Association (ABA) Criminal Justice Standards Committee appointed a Task Force to draft a new set of Criminal Justice Standards, this one relating to Law Enforcement Access to Third Party Records (LEATPR Standards).[2] The new Standards would constitute a new volume in the ABA Standards for Criminal Justice, a massive project that had begun just over forty years earlier, in 1964, when it would have been almost impossible to imagine how much information humanity now stores.[3] In their book *Big Data*, Viktor Mayer-Schönberger & Kenneth Cukier present a telling example from the field of astronomy:

---

2. *See* ABA STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS (2013) [hereinafter LEATPR STANDARDS]. Individual standards will be referred to using the format 'Standard x-x.' The black letter Standards are reproduced in this volume as an Appendix, and the entire Standards volume is available at http://www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/third_party_access.authcheckdam.pdf.

3. *See* Martin Marcus, *The Making of the ABA Criminal Justice Standards: Forty Years of Excellence*, CRIM. JUST., Winter 2009, at 10, 10.

> When the Sloan Digital Sky Survey began in 2000, its telescope in New Mexico collected more data in its first few weeks than had been amassed in the entire history of astronomy. By 2010 the survey's archive teemed with a whopping 140 terabytes of information. But a successor, the Large Synoptic Survey Telescope in Chile, due to come on stream in 2016, will acquire that quantity of data every five days.[4]

One terabyte is 10^{12} bytes (1,000,000,000,000 bytes) and has become a standard size for personal computer hard drives, despite being more computer memory than was available on Earth a mere fifty years ago.[5] To provide some perspective, a single character can be stored as a byte, meaning an article like this one written in a text editor would fill on the order of 70,000 bytes, or .00000007 terabytes.[6] An image file might occupy one megabyte, or .000001 terabytes. The Large Hadron Collider, the world's highest-energy particle accelerator, generates data on an even more impressive scale than our telescopes. When in operation, it generates up to six gigabytes of data every second, meaning one terabyte in under three minutes.[7]

Science has provided similarly impressive techniques to gather information about ourselves. The human genome project required a decade to sequence the three billion base pairs at a cost of $2.7 billion.[8] Today that sequencing can be completed in a day at a cost of $3000.[9] A life logger, meaning one who attempts to self-record all of his experience, generates over a terabyte of data a year.[10] And while they might be far less

---

4. VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 7 (2013).

5. *The People's Panopticon*, ECONOMIST, Nov. 16, 2013, at 27. Of course, digital memory operates in binary, so the same term can also refer to 2^{40} bytes (the number two multiplied by thirty-nine other twos), a slightly different number but of the same order of magnitude. The two conventions are used interchangeably (and sometimes confusingly) for lesser amounts of data, but typically the decimal convention is used for larger amounts.

6. An article written in a program other than a text editor will include data on character formatting (e.g., to account for font size and italics), and thus will be a larger file. One byte is 8 bits, meaning it can contain the numbers 0 to 255, because 2^8=256.

7. *Magnetic Tape to the Rescue*, ECONOMIST, Nov. 30, 2013, at 3 [hereinafter *Magnetic Tape*].

8. MAYER-SCHÖNBERGER & CUKIER, *supra* note 4, at 7; Steve Lohr, *Sizing Up Big Data*, N.Y. TIMES, June 20, 2013, at F1.

9. MAYER-SCHÖNBERGER & CUKIER, *supra* note 4, at 7; Lohr, *supra* note 8, at F1.

10. *The People's Panopticon*, *supra* note 5.

impressive as a matter of hard science,[11] social networking and other online activity amply demonstrate the huge amount of data we collectively generate:

> Google processes more than 24 petabytes [24,000 terabytes] of data per day, a volume that is thousands of times the quantity of all printed material in the U.S. Library of Congress. Facebook, a company that didn't exist a decade ago, gets more than 10 million new photos uploaded every hour. Facebook members click a 'like' button or leave a comment nearly three billion times per day . . . . [T]he 800 million monthly users of Google's YouTube service upload over an hour of video every second. The number of messages on Twitter grows at around 200 percent a year and by 2012 had exceeded 400 million tweets a day.[12]

When it comes to uploading video, YouTube is not even the biggest game in town. Users of Dropcam upload over 1000 hours of video a minute[13] as they use surveillance cameras to "[n]ever miss a moment this year."[14]

The amazing breadth and depth of stored information was very much on our minds as we began drafting the new set of ABA Standards in 2007. Nonetheless, it is remarkable to think on how much more information is stored in 2013, the year I completed drafting the Commentary. While estimating the world's stored information is difficult and uncertain, Martin Hilbert and Priscila López calculate that in 2007 there were approximately 300 exabytes (meaning 300 million terabytes) of stored data.[15] The amount of analog information hardly grows at all, but the amount of digital data

---

11. *See* Jason Pontin, *Why We Can't Solve Big Problems*, MIT TECH. REV., Oct. 24, 2012, *available at* http://www.technologyreview.com/featuredstory/429690/why-we-cant-solve-big-problems/. The cover of this edition intriguingly features a picture of Astronaut Buzz Aldrin with the headline, "You Promised Me Mars Colonies. Instead, I Got Facebook." MIT TECH. REVIEW, Oct. 24, 2012, at front cover, *available at* http://digital.technologyreview.com/?iid=69328#folio=1.

12. MAYER-SCHÖNBERGER & CUKIER, *supra* note 4, at 8.

13. Quentin Hardy, *Today's Webcams See All (Tortoise, We're Watching Your Back)*, N.Y. TIMES, Jan. 7, 2014, at A1.

14. DROPCAM, https://www.dropcam.com/ (last visited Mar. 19, 2014).

15. Martin Hilbert & Priscila López, *The World's Technological Capacity to Store, Communicate, and Compute Information*, SCIENCE, Apr. 1, 2011, at 60, 62. Hilbert and López define storage as "the maintenance of information over a considerable amount of time for explicit later retrieval." *Id.* at 60; *see also* Martin Hilbert & Priscila López, *The World's Technological Capacity to Process Information*, MARTINHILBERT.NET, http://www.martinhilbert.net/WorldInfoCapacity.html (last visited Nov. 30, 2013).

doubles approximately every three years.[16] Thus, in 2013, Hilbert estimates the amount of stored information in the world at around 300 exabytes times 2 times 2, or 1200 exabytes.[17] That is over one billion terabytes. Others estimate the amount of stored data grows even faster, doubling every two years,[18] while the capacity of the fastest way to communicate it, fiber optic cables, doubles every nine months.[19]

To put a less technical face to this, in 2010 Eric Schmidt, CEO of Google, explained that every two days (and by now perhaps every day) we produce more information than was produced over the entire course of civilization up to the year 2003.[20] Thus, every two days of global data production equals or exceeds the amount of information contained in all of the conversations that have ever taken place.[21]

These numbers are mindboggling, and it will require the novel techniques of big data[22] to make sense of information on such massive

---

16. MAYER-SCHÖNBERGER & CUKIER, *supra* note 4, at 9 (describing the work of Hilbert).

17. *Id.*

18. *See* JOHN GANTZ & DAVID REINSEL, THE DIGITAL UNIVERSE IN 2020: BIG DATA, BIGGER DIGITAL SHADOWS, AND BIGGEST GROWTH IN THE FAR EAST 1 (2012), *available at* http://idcdocserv.com/1414 (predicting a doubling every two years); Michiko Kakutani, *Watched by the Web: Surveillance Is Reborn*, N.Y. TIMES, June 11, 2013, at C1; *Magnetic Tape*, *supra* note 7 (referencing such an estimate).

19. ERIC SCHMIDT & JARED COHEN, THE NEW DIGITAL AGE: RESHAPING THE FUTURE OF PEOPLE, NATIONS, AND BUSINESS 5 (2013).

20. MG Siegler, *Eric Schmidt: Every 2 Days We Create as Much Information as We Did Up to 2003*, TECHCRUNCH (Aug. 4, 2010), http://techcrunch.com/2010/08/04/schmidt-data/.

21. *Id.*; *see also* Lohr, *supra* note 8.

22. There is not a single definition of "big data":

> Initially the idea was that the volume of information had grown so large that the quantity being examined no longer fit into the memory that computers use for processing, so engineers needed to revamp the tools they used for analyzing it all. . . . One way to think about the issue today . . . is this: big data refers to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments, and more.

MAYER-SCHÖNBERGER & CUKIER, *supra* note 4, at 6.

> Big Data is a vague term, used loosely, if often, these days. But put simply, the catchall phrase means three things. First, it is a bundle of technologies. Second, it is a potential revolution in measurement. And third, it is a point of view, or philosophy, about how decisions will be – and perhaps should be – made in the future.

Lohr, *supra* note 8, at F1.

scales. But if we step back and think of our everyday experiences, it is easy to see that very significant information about each of us is recorded by third parties that used to be recorded by no one. Whereas I used to pay cash for many purchases, today I buy nearly everything in an identified and recorded manner. And it is not merely what I ultimately purchase that is recorded. Retail store, library, and bookstore browsing are traditionally transient and anonymous, but today I browse online where everything is potentially recorded, from how long I look at a page to where my mouse hovers.[23] Nor will offline, brick-and-mortar store browsing remain anonymous, since high definition store cameras can record a shopper's every move, including using facial recognition to determine ethnicity and identity.[24] And whether we are shopping online or off, soon eye-tracking technology will be able to track and record where our eyes linger as we browse.[25]

Dictionary and encyclopedia browsing are transient and anonymous, but I do these online too. Google knows the words I cannot spell or define as I take advantage of my always-on and always-available connections, from my desktop computer to my iPad to my smartphone.[26] My service providers know and can record everything I do online, and other tracking companies try to learn the same.[27] The broadcast television of my youth

---

23. Lohr, *supra* note 8, at F1; Steve Rosenbush, *Facebook Tests Software to Track Your Cursor on Screen*, WALL ST. J. (Oct. 30, 2013), http://blogs.wsj.com/cio/2013/10/30/facebook-considers-vast-increase-in-data-collection/.

24. Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. TIMES, July 15, 2013, at A1; Stephanie Rosenbloom, *In Bid to Sway Sales, Cameras Track Shoppers*, N.Y. TIMES, Mar. 19, 2010, at A1; *We Snoop to Conquer*, ECONOMIST, Feb. 9, 2013, http://www.economist.com/news/business/21571452-security-cameras-are-watching-honest-shoppers-too-we-snoop-conquer.

25. *See The Eyes Have It*, ECONOMIST, Dec. 1, 2012, http://www.economist.com/news/technology-quarterly/21567195-computer-interfaces-ability-determine-location-persons-gaze; *The All-Telling Eye*, ECONOMIST, Oct. 22, 2011, http://www.economist.com/node/21533362.

26. *Spelling Corrections and Suggestions*, GOOGLE GUIDE, http://www.googleguide.com/spelling_corrections.html (last visited Mar. 19, 2014).

27. For example, we know that when we visit a website, our browser will often differently color those links that we have previously visited. Some data aggregators have sought to take advantage of this by embedding code in sites to which they have access that thereby surreptitiously determines what other sites one has visited. *See* Mathew J. Swartz, *Dataium Settles Browser History Sniffing Charges*, INFORMATIONWEEK (Nov. 26, 2013), http://www.informationweek.com/security/compliance/dataium-settles-browser-history-sniffing-charges/d/d-id/1112817. Other companies use all sorts of other methods to track online activity. *See, e.g.*, Kate Murphy, *How to Muddy Your Tracks on the Internet*, N.Y. TIMES, May 2, 2012, at B7; *Tracking the Trackers: Our Method*, WALL ST. J., July 31, 2010,

was anonymously viewed, but now I consume media from providers who record what I watch and when I watch it.[28] Even the solitary reading of a good book has become a shared spectacle. When I delve into an e-book, the "data exhaust" of such reading is shared and tracked on an incredibly nuanced scale: where I read, when I read, how long I spend on a page, what words I look up in the built-in dictionary, and anything I highlight (and as a consequence, I don't highlight).[29]

How about that weekend drive? Ford Motor Company's top sales executive recently made headlines when he bragged, "We know everyone who breaks the law. We know when you're doing it. We have GPS in your car, so we know what you're doing."[30] And it is not merely your car manufacturer who is watching. The weekend drive is potentially now shared with the insurance company seeking to keep an eye on my driving,[31] the cell phone provider needing to know the location of my phone,[32] and the navigation app helping me on my way.[33] At least portions are shared with others, such as toll-tag operators, license plate readers, stationary cameras, the life-logger driving behind me, and the drone hobbyist flying his new toy.

While I have resisted in a futile attempt at maintaining some control, many have taken advantage of the benefits of remote access and robust backup by moving what used to be stored only on a personal computer into the internet cloud.[34] In short, we share a great deal about our lives with others, and this trend will only accelerate with the impending "internet of

---

http://online.wsj.com/news/articles/SB10001424052748703977004575393121635952084 (discussing three of the fifty most common tracking methods).

28. Neal Ungerleider, *How Big Data Keeps Cable TV Watchers Hooked*, FAST COMPANY (Jan. 14, 2013), http://www.fastcompany.com/3004619/how-big-data-keeps-cable-tv-watchers-hooked.

29. *See* MAYER-SCHÖNBERGER & CUKIER, *supra* note 4, at 113 (explaining the genesis of the term "data exhaust").

30. Jaclyn Trop, *The Next Data Privacy Battle May Be Waged Inside Your Car*, N.Y. TIMES, Jan. 11, 2014, at B1 (quoting Jim Farley).

31. Brad Tuttle, *Big Data Is My Copilot: Auto Insurers Push Devices That Track Driving Habits*, TIME (Aug. 6, 2013), http://business.time.com/2013/08/06/big-data-is-my-copilot-auto-insurers-push-devices-that-track-driving-habits/.

32. Jessica Leber, *How Wireless Carriers Are Monetizing Your Movements*, MIT TECH. REV. (Apr. 12, 2013), http://www.technologyreview.com/news/513016/how-wireless-carriers-are-monetizing-your-movements/.

33. *See id.*

34. Joe Baguley, *How Cloud Computing Is Changing the World . . . Without You Knowing*, GUARDIAN, Sept. 24, 2013, http://www.theguardian.com/media-network/media-network-blog/2013/sep/24/cloud-computing-changing-world-healthcare.

things," in which devices like lights, thermostats, and security cameras are already internet connected, and soon everything from our refrigerators to our running shoes will be as well.[35] Even data that seemingly has no utility is retained in "data tombs," because storage is cheap and the analytics of big data are teaching that new and valuable uses of old data may be just around the corner.[36]

There is certainly an appetite for information.[37] In perhaps what will become the classic story of the dawn of the big data era, Charles Duhigg chronicled how Target's analytics department managed to piece together when a customer is pregnant.[38] Reeling in pregnant shoppers can pay big dividends because such a significant life event shakes up our otherwise routine habits.[39] So when Target's analytics determined that, for example, pregnant women around the beginning of their second trimester purchase increased quantities of unscented lotion, the retailer was able to mine seemingly routine and benign purchase data to predict which customers might be pregnant, scoring them on a "pregnancy prediction" scale and generating a list of tens of thousands of likely pregnant customers.[40] The store's initial blunderbuss targeted advertising raised the ire of the father of a teenager, understandably perturbed that the store would send his daughter personalized advertisements clearly intended for those who were expecting.[41] But when the store manager called to apologize, the father was contrite; it turned out there were things happening in his home of which he was unaware.[42]

---

35. On the internet of things, see, for example, Jesse Emspak, *Smart Shoes Could Help Runners Hit Their Stride*, LIVESCIENCE (Dec. 10, 2013), http://www.livescience.com/41844-smart-running-shoes-improve-runners-gait.html; Brad Spurgeon, *Racing into an Interconnected Future*, N.Y. TIMES, Sept. 21, 2013, http://www.nytimes.com/2013/09/21/sports/autoracing/racing-into-an-interconnected-future.html?pagewanted=all; Bob Sullivan, *The 'Internet of Things' Pits George Jetson vs. George Orwell*, NBC NEWS, June 29, 2013, http://www.nbcnews.com/technology/internet-things-pits-george-jetson-vs-george-orwell-6C.10462818.

36. MAYER-SCHÖNBERGER & CUKIER, *supra* note 4, at 98-104.

37. "[B]ecause Internet companies could collect vast troves of data and had a burning financial incentive to make sense of them, they became the leading users of the latest processing technologies, superseding offline companies that had, in some cases, decades more experience." *Id.* at 6.

38. Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES, Feb. 19, 2002, at MM30.

39. *See id.* ("[N]ew parents are a retailer's holy grail.").

40. *Id.*

41. *Id.*

42. *Id.*

More recently, thanks to Edward Snowden, we have become aware of the massive data surveillance of the National Security Agency, "an electronic omnivore of staggering capabilities."[43] While some portions have been crafty "first person" surveillance, such as the NSA hacking internet security and corrupting cell phones in order to track them even when powered down,[44] many of the revelations relate to the NSA obtaining data from third parties. Some of that third party gathering has been overt, such as gathering all telephone metadata,[45] and some covert, such as gathering cloud storage data as providers transfer it among their own data centers.[46] But either way, this third party surveillance relies upon the breadth of personal information now residing with third parties.[47]

---

43. Scott Shane, *No Morsel Too Miniscule for All-Consuming N.S.A.*, N.Y. TIMES, Nov. 3, 2013, at A1. For more on the connection between big data and the NSA, see James Risen & Nick Wingfield, *Silicon Valley and Spy Agency Bound by Strengthening Web*, N.Y. TIMES, June 20, 2013, at A1. And the revelations keep coming. *See, e.g.*, Geoff White, *Revealed: UK and US Spied on Text Messages of Brits*, CHANNEL 4 NEWS, Jan. 17, 2014, http://www.channel4.com/news/intercept-text-messages-spy-nsa-gchq-british-phone (documenting NSA gathering of 200 million text messages a day).

44. *See* Nicole Perlroth et al., *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES, Sept. 6, 2013, at A1; Shane, *supra* note 43, at A1; Jill Scharr, *NSA Tracks Turned-Off Phones – But Phone Makers Don't Know How*, TOM'SGUIDE (Nov. 12, 2013), http://www.tomsguide.com/us/nsa-track-off-mobiles,news-17851.html.

45. *See* Charlie Savage, *A.C.L.U. Files Lawsuit to Stop the Collection of Domestic Phone Logs*, N.Y. TIMES, June 12, 2013, at A18. For a cogent analysis of the program's legality, see David S. Kris, *On the Bulk Collection of Tangible Things*, LAWFARE RESEARCH PAPER SERIES, Sept. 29, 2013, at 1, http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf. At its core, the NSA argument that Patriot Act section 215 was meant to permit the preservation of *all* third party records on the basis that some miniscule fraction might prove useful at a future time is tenuous. Were Congress to permit such staggeringly broad collection, one would expect—and we should demand—that it then debate the chilling effect this will have, the necessary security precautions for such a database including audit controls and punishments for breaches, the justifications for accessing that database, etc. It is a stretch to think that even our too-often dilatory Congress meant to leave all of those critical matters undecided, implicitly authorizing the secret Foreign Intelligence Surveillance Court to draft all of the critical design elements. This is not to say, however, that such appropriately defined authorization would necessarily be ill-advised. *See, e.g.*, Christopher Slobogin, *Cause to Believe What?: The Importance of Defining a Search's Object—Or, How the ABA Would Analyze the NSA Metadata Surveillance Program*, 66 OKLA. L. REV. 725, 738-39 (2014) (applying ABA LEATPR Standards to NSA collection).

46. *See* Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST, Oct. 30, 2013, http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-

So, what was clear in 2007 as we began drafting the ABA Standards is even clearer today: there is a great need for a coherent, methodical approach to the regulation of law enforcement access to third party information. The LEATPR Standards are the first to articulate such a framework. Before turning to a brief explanation of their drafting process, it is worth spending a moment more on why all of this matters.

The Standards Commentary, including that to Standard 25-3.3, defines and explains the importance of information privacy. That privacy, meaning for each of us the right to control what information about us is conveyed to others and for what purposes, is of course much larger than merely the issue of law enforcement access. It is central to human development and dignity, and should restrict third parties as well. Yet only the government can force disclosure of information unrestrained by market and other pressures, and the ABA Standards for Criminal Justice are inherently limited to considering this subset.

But a subset it is, meaning law enforcement access to third party records is a meaningful component of the larger issue. And in this larger context Viktor Mayer-Schönberger has made important insights, including that "[m]emory impedes change."[48] In his 2009 book, *Delete*, Mayer-Schönberger beautifully empathizes the human experience, an experience that for each of us is often tolerable—and even wonderful—only because we can change. An all-recording and all-remembering digital society could effectively stifle that opportunity:

> I fear the real bottleneck of conflating history and collapsing time is not digital memory, but human comprehension. Even if we were presented with a dossier of facts, neatly sorted by date, in our mind we would still have difficulties putting things in the right temporal perspective, valuing facts properly over time. . . . From the perspective of the person remembering, digital memory

---

d89d714ca4dd_story.html. In retrospect, it is rather remarkable that these cloud providers thought to encrypt data sent to and from the customer, but not when transmitted among their own disparately located servers.

47. Like many, I am critical of much of the NSA surveillance, but I am not as distrustful of the institutional motives. When there are no external restraints, it is logical to gather absolutely everything one can subject only to resource restraints; in the world of intelligence, who knows what will ultimately prove useful? But of course well-intentioned surveillance can be almost equally destructive to social participation and free society, and thus we must figure out how to implement proper restraints without hobbling our intelligence apparatus.

48. VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 125 (2009).

> impedes judgment. From the perspective of the person remembered, . . . it denies development, and refuses to acknowledge that all humans change all the time. By recalling forever each of our errors and transgressions, digital memory rejects our human capacity to learn from them, to grow and to evolve.[49]

In the characteristically deadpan assessment of *The Economist* magazine, "A perfect digital memory would probably be a pain, preserving unhappy events as well as cherished ones."[50] Mayer-Schönberger poignantly asks, "Do we want a future that is forever unforgiving because it is unforgetting?"[51]

On the other hand, as the police and prosecutors involved in the formulation of the Standards were right to often point out, the things some would most like forgotten are the evidences of their victimization of others. In the context of law enforcement access to records, we often must remember and must access to keep us safe from those who would do harm. It is this very difficult balance that the LEATPR Standards aim to enable: permitting law enforcement reasonable access to keep us safe and preventing unnecessary access to keep us secure.

II. Drafting the LEATPR Standards

Perhaps understandably, the American Bar Association conjures different reactions in different people, including among attorneys.[52] So it is worth explaining the rigorous and inclusive drafting process of the LEATPR Standards, which mirrors that of all of the ABA Standards for Criminal Justice. First, in late 2006, a Task Force was appointed to begin the drafting process. The chair was Michael Bender, then a Justice on, and later the Chief Justice of, the Colorado Supreme Court, and I was of course the Reporter. Together we would shepherd the Standards through the six-plus years of drafting. The members of the Task Force were two prosecutors, two practicing attorneys, and three prominent academics, two of whom (Christopher Slobogin and Andrew Taslitz) had very significant

---

49. *Id.*

50. *Every Step You Take*, ECONOMIST, Nov. 16, 2013, at 13.

51. MAYER-SCHÖNBERGER, *supra* note 48, at 4-5.

52. *See, e.g.*, David Segal, *For Law Schools, a Price to Play the A.B.A.'s Way*, N.Y. TIMES, Dec. 18, 2011, at BU1 (discussing controversy over the ABA's law school accreditation role); Adam Liptak, *Legal Group's Neutrality is Challenged*, N.Y. TIMES, Mar. 31, 2009, at A14 (discussing controversy over the ABA's judicial screening role).

standards drafting experience of their own, and the third of whom (Paul Ohm) is a leading scholar on privacy in the information age. The Federal Bureau of Investigation, the National Association of Criminal Defense Lawyers, the National Legal Aid & Defender Association, and the U.S. Department of Justice all appointed liaisons.

Because this was a new set of Standards, we had to start from the very beginning, including reading existing standards and delimiting our scope. Although the title page of the LEATPR Standards denotes them as a "Third Edition," this merely reflects that the ABA is currently in its third iteration of its Criminal Justice Standards project.[53] The LEATPR Standards have no predecessor in the ABA Standards or in those written by other organizations. Over the next three years, the Task Force met in person eight times and corresponded many more times electronically, culminating in a draft that in March of 2010 was sent to the nine-member Criminal Justice Standards Committee. Like the Task Force, the Standards Committee is to have balanced representation, and specifically aims to have three prosecutors, three defense attorneys, and three academics and judges, along with nonvoting liaisons from prosecutorial and defense organizations.[54]

The draft transmitted to the Standards Committee was not unanimous, a matter of significant concern because the ABA prefers to proceed by unanimous, or at least overwhelming, consent whenever possible.[55] The goal of the Standards project has always been to create "balanced and practical" recommendations that "reflect[] a consensus of the views of representatives of all segments of the criminal justice system."[56] Fortunately, the Standards Committee was very ably led by Martin Marcus, a judge on the New York Supreme Court.[57] Judge Marcus and I are both respectably stubborn, and our emails drafting various provisions would go back and forth a substantial number of times (we neared running out of reasonable colors to denote the most recent edits). But thanks to Judge Marcus and the other members of the nine-member Standards Committee (including the person who would become the chair before the drafting process was complete, Judge Marcus' judicial colleague Mark Dwyer), we

53. *See* Marcus, *supra* note 3, at 13 (explaining second and third editions).

54. *Id.* at 14.

55. *See id.* at 15.

56. *Id.* at 14.

57. In an often successful attempt to confuse people, the Supreme Court is New York's trial court of general jurisdiction. *See Structure of the Courts*, NYCOURTS.GOV (Feb. 15, 2012), http://www.nycourts.gov/courts/structure.shtml.

came out of the Standards Committee with a unanimous draft in a little over a year. We were substantially aided by a former prosecutor (Peter Pope of New York) and a current prosecutor (Matthew Redle of Wyoming), who were willing and able to carefully consider what prosecutors require to fulfill their mission.

The next stage was the thirty-four-member ABA Criminal Justice Section Council, where the Standards underwent two "readings," which provided full days to consider and amend their content. As will be no surprise at this point, that Council was broadly representative of the criminal justice system, and prior to the Council's consideration the draft was widely circulated to other interested parties and persons.[58] Again we were fortunate to have good leadership, this time by practitioner Janet Levine, and so, with modification, the Standards were approved for consideration by the ABA House of Delegates. It was during this stage, however, that I believe the two most unfortunate drafting decisions were made, both of which are discussed later in this paper (the expanded grand jury carve-out and the constitutional jurisprudence carve-out).

The draft was once more circulated to interested parties, and the ABA House of Delegates considered and approved the black letter standards on February 6, 2012. I then turned to writing the final commentary, and that commentary was approved by the Standards Committee in March of 2013, thus completing the twenty-fifth volume in the ABA Standards for Criminal Justice, Law Enforcement Access to Third Party Records. Hopefully, in time, this volume will enjoy the wide circulation and use that other volumes have experienced.[59]

III. Introducing the LEATPR Standards

As part of the Standards Commentary I drafted a complete Introduction,[60] and elsewhere I have introduced and applied the LEATPR Standards to the topic of location tracking.[61] I will not seek to replicate that full introduction here, but provide a condensed version for those new to the Standards. For convenient reference, the black letter is included as an Appendix to this volume.

---

58. *See* Marcus, *supra* note 3, at 15.

59. *See id.* at 10-13; 1 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 1.3(f) (3d ed. 2007).

60. LEATPR STANDARDS, *supra* note 2, at 1-16.

61. Stephen E. Henderson, *Real-Time and Historic Location Surveillance After* United States v. Jones*: An Administrable, Mildly Mosaic Approach*, 103 J. CRIM. L. & CRIMINOLOGY 803 (2013).

The LEATPR Standards relate to law enforcement investigatory access to, and storage and disclosure of, records maintained by institutional third parties.[62] In other words, they address government agents seeking to acquire evidence from existing records to be used in the detection, investigation, or prevention of crime. Because different constitutional principles govern, because different interests predominate, and simply as a matter of not tackling more than could responsibly be completed in a single iteration, the Standards do not address access for purposes of national security,[63] civil investigation,[64] or criminal prosecution.[65] The Standards also do not address records access from an individual not acting as a business entity (e.g., police acquiring a letter written to a friend from that friend),[66] and do not address an institutional third party "deciding of its own initiative and volition to provide information to law enforcement."[67] The Standards also do not address acquisition of information contemporaneous with its generation or transmission, because such "wiretapping" is already the province of other Standards.[68] Finally, and more questionably, the

---

62. My text here is adapted from the LEATPR Standards Introduction. *See* LEATPR STANDARDS, *supra* note 2, at 5-11.

63. STANDARD 25-2.1(a).

64. *See* STANDARD 25-2.1(b) commentary.

65. STANDARD 25-2.1(b). For purposes of the Standards, "criminal prosecution" follows the federal Sixth Amendment trigger, meaning the initiation of adversary judicial proceedings. *See id.*

66. STANDARD 25-2.1(d).

67. STANDARD 25-2.1(f)(ii). Not only is this an inherent limitation in Criminal Justice Standards, but the government is unique:

> [A] focus on government activity reflects the reality that only the government exercises the power to compel disclosure of information and to impose civil and criminal penalties for noncompliance. Only the government collects and uses information free from market competition and consumer preferences. When dealing with the government, individuals have no opportunity to express their expectations of privacy by choosing to do business elsewhere or by not engaging in transactions at all. We, like the framers of our Constitution, recognize that in the government context, the law alone provides—or should provide—protection for those expectations.

DEP'T OF DEF. TECH. & PRIVACY ADVISORY COMM., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM 24 (2004), *available at* http://www.fredhcate.com/Publications/TAPAC_Report%20Final.pdf.

68. *See* STANDARD 25-2.1(e); *see also* ABA STANDARDS FOR CRIMINAL JUSTICE, ELECTRONIC SURVEILLANCE SECTION A: ELECTRONIC SURVEILLANCE OF PRIVATE COMMUNICATIONS (3d ed. 2001); ABA STANDARDS FOR CRIMINAL JUSTICE, ELECTRONIC SURVEILLANCE SECTION B: TECHNOLOGICALLY-ASSISTED PHYSICAL SURVEILLANCE (3d ed. 1999).

Standards do not address records access via a grand jury subpoena or a "functionally equivalent prosecutorial subpoena,"[69] a topic I address in the next section of this article.

Part I of the Standards provides definitions, Part II delimits the Standards' scope, and Part III articulates the core governing principles. Parts IV, V, and VI then provide the substantive recommendations, Part IV governing the categorization and protection of information, Part V the access to records, and Part VI record retention, maintenance, and disclosure. Part VII then provides accountability for those substantive recommendations.

In many ways, Part IV is the heart of the Standards. A decision maker, often a legislature but also potentially a court or an administrative agency, first determines the level of privacy for a given category of information.[70] For example, should banking transactions be considered *highly private*, *moderately private*, *minimally private*, or *not private*?[71] The Standards provide four important criteria that should be considered in making this determination, in addition to considering the relevance of present and developing technology.[72] The Standards do not, however, suggest a particular answer, thus respecting local circumstances, changing needs, and the necessarily difficult nature of this inquiry. The four privacy criteria consider, in a nutshell, the reason for and societal importance of the transfer to the third party, the personal nature of the information, whether such information is accessible and accessed by others, and existing law.[73] Once

---

69. STANDARD 25-2.1(c).

70. STANDARD 25-4.1.

71. Why four categories (essentially large, medium, small, or nothing at all) instead of three or five? Obviously there is no magic number; increasing the number of categories increases nuance but sacrifices administrability. For a thoughtful defense of using some sort of categorical system, as opposed to a continuum, see Marc Jonathan Blitz, *Third Party Records Protection on the Model of Heightened Scrutiny*; 66 OKLA. L. REV. 747, 754-61 (2014). *But see generally* Thomas P. Crocker, *Ubiquitous Privacy*, 66 OKLA. L. REV. 791 (2014) (questioning whether a categorical system will ineffectually protect privacy).

72. STANDARD 25-4.1.

73. *Id.* In full, the four criteria are the extent to which

> (a) the initial transfer of such information to an institutional third party is reasonably necessary to participate meaningfully in society or in commerce, or is socially beneficial, including to freedom of speech and association;
>
> (b) such information is personal, including the extent to which it is intimate and likely to cause embarrassment or stigma if disclosed, and whether outside of the initial transfer to an institutional third party it is typically disclosed only within one's close social network, if at all;
>
> (c) such information is accessible to and accessed by non-government

this degree of privacy is determined, it sets a threshold level of protection: highly private records—meaning those that contain highly private information—are *highly protected*, moderately private records are *moderately protected*, etc.[74] Absent consent,[75] emergency aid, or exigent circumstances[76]; consistent with the law of privilege[77]; and absent any greater constitutional protection[78]; the Standards provide that law enforcement should be permitted to access a highly protected record via a warrant supported by probable cause.[79] For moderately protected information, access should require a court order supported by reasonable suspicion or, if the legislature or other decision maker so chooses, a court order supported by relevance or issued pursuant to a prosecutorial certification.[80] Access to minimally protected information should require a prosecutorial or agency determination of relevance.[81] And access to unprotected information should be permissible for any legitimate law enforcement purpose.[82] Although the privacy of a category of information alone sets this threshold, there may be circumstances in which that threshold makes it too difficult to solve otherwise solvable crime. In that case, the legislature or other decision maker may, thinking also of the privacy implications, consider reducing the level of protection accordingly.[83]

The Standards also provide for access to inclusive bodies of de-identified records (that is, records not linkable through reasonable efforts to an identifiable person) when law enforcement has reason to conduct data

---

persons outside the institutional third party; and

(d) existing law, including the law of privilege, restricts or allows access to and dissemination of such information or of comparable information.

Id. For a modified approach drawing insights from constitutional jurisprudence outside of the Fourth Amendment (e.g., considering rational basis, intermediate scrutiny, and strict scrutiny with its narrow tailoring requirement), see generally Blitz, *supra* note 71.

74. STANDARD 25-4.2(a).

75. STANDARD 25-5.1.

76. STANDARD 25-5.4.

77. STANDARD 25-5.3(c).

78. STANDARD 25-2.2.

79. STANDARD 25-5.3(a)(i).

80. STANDARD 25-5.3(a)(ii).

81. STANDARD 25-5.3(a)(iii).

82. STANDARD 25-5.3(d).

83. STANDARD 25-4.2(b). For an argument that there should be an analogous provision that would provide *greater* protection to otherwise minimally protected information in certain privacy-crucial contexts, see Crocker, *supra* note 71, at 810.

mining.[84] Finally, if the record is highly or moderately protected, law enforcement should typically provide notice to the focus of the record, but that notice can be, and often will be, delayed.[85]

The Commentary includes examples applying the Standards to a hypothetical park shooting and then to a bank computer hack.[86] In another article, I apply them to location tracking,[87] and in this volume, Susan Freiwald applies them to cell-site location records.[88] The Standards recognize that a consensus concerning law enforcement access to records is still developing, but also acknowledge the need to appropriately strike a delicate balance between law enforcement's legitimate need for access to records and the privacy interests of the subjects of those records. By setting forth privacy criteria and articulating a framework, the Standards will assist legislatures and other deliberative bodies in carrying out this critical task.

IV. Improving the LEATPR Standards

I will allow the excellent symposium papers to make their own arguments and contributions, other than dropping the occasional footnote where I have been unable to resist noting their insights. I do not want to detract from them, nor at this early stage attempt to contribute to them. Not only will they be valuable to those seeking to implement the Standards, but they are valuable more generally to theorizing and developing this body of law. For example, one of the benefits of the Standards project has been to reveal, or at least to highlight, some critical uncertainties in the core concepts of relevance, reasonable suspicion, and probable cause.[89] Additionally, in several years, with the passage of new events and new law it will come time to update the Standards, and these papers, and future riffs upon them, will be invaluable.

---

84. STANDARD 25-5.6. For an application of these Standards to the National Security Agency's bulk collection of communications metadata, see Slobogin, *supra* note 45, 735-40.

85. STANDARD 25-5.7.

86. LEATPR STANDARDS, *supra* note 2, at 11-16.

87. Henderson, *supra* note 61, at 815-21, 826-31.

88. Susan Freiwald, *Some Light in the Darkness: How LEATPR Standards Guide Legislators in Regulating Law Enforcement Access to Cell Site Location Records*, 66 OKLA. L. REV. 875, 908-17 (2014). Professor Freiwald has not only been a key voice in the academic debate, but has participated in the principal federal litigations.

89. *See generally* Andrew Guthrie Ferguson, *Big Data Distortions: Exploring the Limits of the ABA LEATPR Standards*, 66 OKLA. L. REV. 831, 844-53 (2014); Slobogin, *supra* note 45; Andrew E. Taslitz, *Cybersurveillance Without Restraint? The Meaning and Social Value of the Probable Cause and Reasonable Suspicion Standards in Governmental Access to Third-Party Electronic Records*, 103 J. CRIM. L. & CRIMINOLOGY 839 (2013).

For now, I will content myself with making several points of drafting history.

A. The Investigative Grand Jury

The LEATPR Standards exempt not only the federal grand jury from their scope, and not only similar investigative state grand juries, but more broadly "access to records via a grand jury subpoena, or in jurisdictions where grand juries are typically not used, a functionally equivalent prosecutorial subpoena."[90] This language leaves two questions, one of which is at least partially answered in the Commentary, and one of which is not: What does this mean, and where did it come from?

As for what the exception means, the Commentary first describes the historic, permissive jurisprudence relating to the federal investigative grand jury; describes the reasons to question the continued vitality of that permissive jurisprudence; and then explains as follows:

> There was robust debate on these topics during the drafting of these Standards. Ultimately, however, these Standards are in accordance with the historic treatment, including acknowledging a longstanding alternative in some jurisdictions where grand juries are typically not used. Legislatures, courts, and administrative agencies should be careful, however, to strictly cabin this exception to means for which (1) there is historical practice that has not been discredited and that remains relevantly applicable, and (2) that historical practice includes privacy safeguards equivalent to those of the federal grand jury.[91]

That Commentary is the best indication I can give of *what* a "functionally equivalent prosecutorial subpoena" would be, because the construct is a creation of the ABA Criminal Justice Section Council. My goal in drafting the Commentary language was to remain true to the Council's desire, while also to prevent this exception from being too broadly read, and thereby misread.

Where did this language come from? In other words, why generate this seemingly ill-defined and novel category? Presumably like many others before us, we struggled with what to make of the investigatory grand jury. As a Task Force, we chose to remain true to the reality of grand jury subpoenas in operation and therefore treated a grand jury subpoena as

90. STANDARD 25-2.1(c).
91. STANDARD 25-2.1(c) commentary.

equivalent to any other prosecutorial subpoena, meaning it would suffice to access only minimally protected information. This would certainly work a significant change in the current law, but it is a change that, in my mind, would be beneficial. Blind continuation of a historical anomaly calls to mind Oliver Wendell Holmes' famous assertion:

> It is revolting to have no better reason for a rule of law than that so it was laid down in the time of Henry IV. It is still more revolting if the grounds upon which it was laid down have vanished long since, and the rule simply persists from blind imitation of the past.[92]

Whatever role the grand jury may retain as a bulwark against government oppression, it does not play that role when an assistant U.S. Attorney issues a subpoena.

However, when our Task Force draft reached the Standards Committee, members almost immediately identified our treatment of the grand jury subpoena as a political nonstarter, meaning that any such change to the much-reverenced federal grand jury would not ultimately see the light of day. So, we added the grand jury subpoena as an option to access records containing highly protected information, thus effectively equating the subpoena to a warrant. This might have been too strong, as even current muddled jurisprudence does not equate the two, at least where non-records evidence is at issue and thus courts do not feel hemmed by the third party doctrine.[93] In any event, while the Standards Committee draft permitted a grand jury subpoena to suffice for all records, no matter the level of privacy, we did not include any language permitting a "functional equivalent" to also suffice.

During the first Reading before the Section Council, a council member objected to this favored status on the grounds that a grand jury subpoena is "grand jury" in name only, raising the same objection that had won the day before the Task Force. The resolution was to exempt grand jury subpoenas from the Standards altogether. Grand jury subpoenas would now be exempt from the Standards via Part II (the scope provisions), meaning the Standards simply say nothing about grand jury subpoenas. This was seemingly the only way to both give deference to the historically favored status of this instrument and to recognize that in practice the grand jury

92. Oliver Wendell Holmes, Jr., *The Path of the Law*, 10 HARV. L. REV. 457, 469 (1897).

93. *See, e.g.*, United States v. Thomas, 736 F.3d 54, 60 (1st Cir. 2013) (rejecting a grand jury subpoena for a buccal swab).

subpoena is issued at the discretion of a prosecutor. At least this was the only way that could politically survive. Grand jury subpoenas were *sui generis*—one of a kind—and the Standards therefore did not speak to them.

While that was probably a wise move, at the second Council Reading we added the nebulous "functional equivalent" language without, in my mind, anyone really understanding or appreciating its scope. This was one of the few times in the drafting process where I felt a change was made without due deliberation. Fortunately, I do not expect it to be very significant given the desire to limit it to federal-grand-jury-like proceedings, but nor do I think it was a helpful addition given the confusion it might engender and the potential for misinterpretation.

B. The Court Constitutional Carve-Out

Just like I worry that the nebulous grand jury carve-out might be misinterpreted, I regret another change also made by the Section Council. Indeed, if misunderstood, this change is more likely to have serious deleterious consequences.

As the Standards were drafted in the Task Force and then the Standards Committee, we always had three audiences in mind: courts engaged in constitutional decision making, legislatures enacting law, and agencies promulgating rules. Not only was constitutional adjudication central because the scholarship undergirding the Standards was largely derived from constitutional appellate decisions, but its importance was reinforced by the leadership of our chair, Michael Bender, Chief Justice of the Colorado Supreme Court. It was clear to all of us that courts are very much in need of guidance in making the difficult determinations of precisely what constitutional protection to provide various types of third party information. Of course, statutory and administrative requirements will sometimes differ from the constitutional floor, but all three require a framework for making these decisions and that framework is what the Standards provide.

Unfortunately, when we reached the Section Council, we encountered the view that it was not the province of the ABA Criminal Justice Standards to inform constitutional decision making. Thus, the first of our three intended audiences shrunk to "courts that may act in a supervisory capacity," primarily meaning those state courts empowered to craft common law.[94] Clearly this is not to say that courts engaged in constitutional interpretation will not find much of use in our Standards. Indeed, such a claim is impossible given the genesis of, for example, our

94. STANDARD 25-3.4.

privacy factors in state constitutional law.[95] But the carve-out could well unintentionally discourage courts from using the Standards, which could severely stunt their growth. I can only hope that will not prove to be the case.[96]

C. National Security

The LEATPR Standards do not relate to records access for purposes of national security, meaning an investigation of a foreign power or an agent thereof.[97] Previous sets of Standards have made a similar carve-out,[98] and it makes good sense given the different governing constitutional principles and government needs, and the practicalities of not knowing what national security surveillance takes place given a lack of necessary clearances and the required "need to know."[99]

However, it is worth noting that our preliminary decision as a Task Force was actually to the contrary: we *would* address government access both for purposes of law enforcement and national security, and we looked to educate ourselves about both. As I wrote in an early internal memorandum, "Not only is the line between the two becoming increasingly difficult to draw, but national security surveillance since the attacks of September 11, 2001, makes clear that such acquisition is both important and potentially subject to abuse."[100] Ultimately, however, it would simply have been overwhelming to consider them both together in the first instance, especially given the different governing law.

D. Human Development and Dignity

Even for scholars who, like myself, are largely content with a control theory of information privacy, we ultimately tie its benefits to core notions

---

95. *See* STANDARD 25-3.4 commentary.

96. For a view that any standards will fail absent an even stronger tie to the Constitution, meaning an argument that they require a claim of constitutional necessity, see generally David Gray, *The ABA Standards for Criminal Justice: Law Enforcement Access to Third Party Records: Critical Perspectives from a Technology-Centered Approach to Quantitative Privacy*, 66 OKLA. L. REV. 919 (2014).

97. STANDARD 25-2.1(a).

98. *See* STANDARD 25-2.1(a) commentary at n. 76.

99. Of course, thanks to Edward Snowden we now know much more about NSA surveillance than we did during the drafting process.

100. Memorandum from Stephen E. Henderson, Professor, University of Oklahoma College of Law, to LEATPR Task Force (May 29, 2007) (on file with author).

of personal identity, development, autonomy, and dignity.[101] American law tends to be wary of such language, however, and that played out during the drafting of the Standards. The Task Force draft included as a general principle (what is now Standard 25-3.3) that law enforcement acquisition of records "can infringe the privacy of those whose information is contained in the records, chill information transfers, and thereby diminish human development, dignity, and freedom of speech and association."[102] The Standards Committee eliminated the reference to human development and dignity, but ultimately did add helpful, if less encompassing, language in its place: "Law enforcement acquisition of records maintained by institutional third parties can infringe the privacy of those whose information is contained in the records; chill freedoms of speech, association, and commerce; and deter individuals from seeking medical, emotional, physical or other assistance for themselves or others."[103]

E. Probable Cause of What?—Or, the Object of the Search

As Christopher Slobogin develops in his contribution to this volume, there are significant uncertainties in applying the traditional concepts of relevance, reasonable suspicion, and probable cause.[104] He focuses in particular on uncertainties with respect to how evidential the "object" that the government is seeking must be: must it be contraband, a fruit of crime or an instrumentality or crime, can it be "mere evidence," or can it be anything that might lead to evidence of guilt? Although these vagaries were briefly discussed at various stages of the Standards' drafting, we ultimately made no concerted attempt to resolve them. Thus, for example, for highly protected records the Standards require "a judicial determination that there is probable cause to believe the information in the record contains *or will lead to* evidence of crime."[105] As I describe elsewhere, the italicized language was added during the second reading before the Criminal Justice Section Council for a relatively tangential reason and with little discussion.[106]

---

101. For a discussion of these benefits and their tie to privacy, see Crocker, *supra* note 71, at 794-800.

102. LEATPR Task Force, ABA Standards for Criminal Justice: Government Access to Records: Third Parties and Privacy 19 (Jan. 15, 2010) (on file with author).

103. STANDARD 25-3.3.

104. *See generally* Slobogin, *supra* note 45.

105. STANDARD 25-5.2(a)(i) (emphasis added); *see also* STANDARD 25-5.3(a)(i).

106. *See* Henderson, *supra* note 61, at 821-23.

Slobogin is particularly concerned about justificatory standards that permit access to anything that might aid "an investigation."[107] For example, imagine that access to phone records requires reasonable suspicion, defined as a moderate chance. There is a significant difference between the following: (1) demonstrating a substantial chance that person *'X'* is a meth dealer, and therefore positing a moderate chance that his phone records are relevant to the investigation because he might have contacted known drug offenders; and (2) demonstrating a substantial chance that person *'X'* is a meth dealer, and demonstrating a moderate chance that his phone records contain *evidence of crime* by, say, an informant's explanation that *X* set up his deals via telephone.[108] In other words, when the Standards use "relevant to an investigation," are they merely meaning to lower the required quantum of suspicion, say from forty percent for probable cause to thirty percent for reasonable suspicion to fifteen percent for relevance? Or are they also meaning to change the "object" of that suspicion, requiring only connection to the investigation as opposed to locating evidence of crime? Other than for de-identified records, where different language is used, I believe it was the former, meaning merely a lesser quantum of suspicion. Thus, during the drafting it was pointed out that the Stored Communications Act requires relevance "to an ongoing criminal investigation" as part of its reasonable suspicion standard,[109] and that such language was not thought to work any expansion in theory or practice. And it is possible that when it comes to a quantum of suspicion as low as that of relevance, there is little to no practical difference regardless: if phone records are relevant to some meth investigations, they are ipso facto relevant to this one.

Nonetheless, a jurisdiction opting for one of the lesser LEATPR Standards protections for records containing moderately protected information should take note of the potential breadth of the relevance standard.[110] Indeed, perhaps the most important specific contribution of Slobogin's paper is its critique of the Standards' inclusion of anything less than reasonable suspicion as a default protection for moderately protected records.[111] More generally, as Slobogin, Taslitz, and Ferguson have all

107. *See* Slobogin, *supra* note 45, at 735-40; *see also* STANDARD 25-5.2(a)(iii), (a)(iv), (b), (c).

108. *See* Slobogin, *supra* note 45, at 743.

109. 18 U.S.C. § 2703(d) (2012).

110. *See* STANDARD 25-5.3(a)(ii) (permitting a choice).

111. *See* Slobogin, *supra* note 45, at 743-46.

begun to develop, this will be an area of continuing interest in criminal procedure.

V. Conclusion

Between the emergence of big data and the revelations of Edward Snowden, it is difficult today to avoid talk of access to records. For those of us who have been involved in this area of the law for many years, including in the drafting of the ABA LEATPR Standards, that increased public consciousness is a good thing, and hopefully the Standards will be put to good use and, where found wanting, improved upon. This symposium is certainly a good start for the academic component.

In conclusion, I briefly note two areas I think will be of increasing importance in the coming years. First, as big data teaches what can be learned from existing data gathered for limited purposes, law enforcement will be inclined to combine and mine the vast amounts of information it collects.[112] As merely an isolated but telling example, when a cellphone is reported stolen in New York City, the police routinely acquire the phone's calling information going forward.[113] Regardless of the statutory legality of this acquisition,[114] and regardless of its utility in solving the theft or robbery, there is much less justification for dumping all of the records so obtained into a growing database. Yet that is precisely what police are doing.[115] So, future iterations of the LEATPR Standards might want to spend more time thinking about imposing use restrictions on law enforcement data, an issue that Harold Krent very ably raised years ago but whose time might have finally come for both constitutional and statutory law.[116] Now that we store so much more information to begin with, and that big data analytics make analysis of that data, and analysis of old, pre-existing data, powerful and telling, we need use controls more than ever

112. Andrew Ferguson has correctly pointed out that the concept of mining data for new revelations, including by police, is hardly new. *See* Ferguson, *supra* note 89, at 835-36. But he likewise recognizes and emphasizes the significance of the advances in analytics that we refer to as big data. *See id.* at 839-40.

113. Joseph Goldstein, *City Is Amassing Trove of Cellphone Logs*, N.Y. TIMES, Nov. 27, 2012, at A25.

114. More details would be necessary to ascertain its legality under, for example, the federal Pen/Trap Statute (18 U.S.C. § 3121) or the Stored Communications Act (18 U.S.C. § 2703).

115. *See* Goldstein, *supra* note 113.

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

before. Big data analytics can be incredibly useful to law enforcement, including to officers on the beat,[117] but will be unduly invasive of privacy unless constitutionally or statutorily restricted.

Finally, I continue to become increasingly convinced that we need better dialogue, including law enforcement being more forthcoming regarding what records access it conducts and for what purposes. While I have written about this before,[118] two more recent data points have come to my attention. We did not know until recently that AT&T has for the past twenty-six years maintained an enormous database of phone records tracking every call that passes through its switches.[119] One of the reasons the database remained secret for so long is because when law enforcement uses that database it never admits such access in court or otherwise. Instead, it whitewashes the investigation either by omitting all mention of the phone records, or by re-accessing the same information a second time using a different method.[120] That sort of deception might be thought beneficial to snare unknowing criminals, but it also prevents any discussion about the privacy implications for the innocent.

Another point of records access that some law enforcement would prefer to keep under wraps is obtaining location information from cell phone providers, including the use of "tower dumps" that reveal every phone near a certain cell tower in a given time period.[121] When USA Today recently issued records requests and learned that one quarter of responding law enforcement agencies have obtained information from cell tower dumps, some agencies refused to respond on the ground that "criminals or terrorists could use the information to thwart important crime-fighting and

---

117. *See* Wendy Ruderman, *New Tool for Police Officers: Records at Their Fingertips*, N.Y. TIMES, Apr. 12, 2013, at A17 (describing "the newest tool in the Police Department's crime-fighting arsenal: a smartphone"). According to Ruderman, "The technology offers extraordinary levels of detail about an individual, including whether the person has ever been a passenger in a motor vehicle accident, a victim of a crime or in one instance, a drug suspect who has been known by the police to hide crack cocaine in his left sock." *Id.* (internal punctuation omitted).

118. *See* Henderson, *supra* note 61, at 835-38.

119. Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, N.Y. TIMES, Sept. 1, 2013, at A1.

120. *Id.* (including the law enforcement slides, which are available at *Synopsis of the Hemisphere Project*, N.Y. TIMES, Sept. 1, 2013, http://www.nytimes.com/interactive/2013/09/02/us/hemisphere-project.html).

121. For more on cell tower dumps, including their analysis under the Standards, see Henderson, *supra* note 61, at 803-08, 815-21, 823-31.

surveillance techniques."[122] Agencies have been similarly coy regarding their use of devices that mimic cell phone towers in order to track phone location in real time.[123] Thus, in one recent court opinion it is reported that police "did not want to obtain a search warrant because they did not want to reveal information about the technology they used to track the cell phone signal."[124] According to the prosecutor, the police had a nondisclosure agreement with the company owning the technology.[125] And per the testimony of an investigator, "[W]e prefer that alternate legal methods be used, so that we do not have to rely upon the equipment to establish probable cause, just for not wanting to reveal the nature and methods."[126] Highly weaponized paramilitary police have taken a page from our military, but when they start to articulate the refrains of national security, clearly policing has gone too far. Whatever benefits there are to nondisclosure, in the context of ordinary policing there are at least comparable benefits to robust and honest discussion.

The ABA LEATPR Standards are, at the very least, an important step in the right direction. They are the product of over six years of discussion, dialogue, debate, and compromise, and are the first set of standards to guide legislatures, courts, and agencies in making the difficult decisions of how best to regulate law enforcement access to ubiquitous and varied third party records. It was my privilege to serve as their Reporter and to convene this symposium to continue moving the ball forward.

122. John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY, Dec. 9, 2013, at A1.

123. *See id.*; *see also* Ellen Nakashima, *Little-Known Surveillance Tool Raises Concerns by Judges, Privacy Activists*, WASH. POST, Mar. 28, 2013, at A3.

124. Thomas v. State, 127 So. 3d 658, 660 (Fla. Dist. Ct. App. 2013).

125. *Id.*

126. *Id.*