Brooklyn Law Review

Volume 80 | Issue 4 Article 2

2015

A Cyber Age Privacy Doctrine: More Coherent, Less Subjective, and Operational

Amitai Etzioni

A Cyber Age Privacy Doctrine

MORE COHERENT, LESS SUBJECTIVE, AND OPERATIONAL

Amitai Etzioni†

In a previous paper, I outlined a privacy doctrine—a cyber age privacy doctrine, or a CAPD—that seeks to account for important differences between the paper age and the digital one.[1] In the paper age, the main issue was whether or not the government should be allowed to collect personal information without first gaining a court's approval. Many court cases sought to determine whether a particular collection of information by the government—using a wiretap, or a dog, or a speed camera—searching one's trash, or mail—was constitutional. In the cyber age, secondary usages of legally-collected information have become so common that a very major concern has become the circumstances under which such usages should be banned to preserve privacy. So much legally-collected personal information is available in the hands (or in the cloud) of third parties that their secondary usages determine to a large extent how much privacy we still have. For example, although corporations legally collect information about their customers, may they sell it to others? To the government? The CAPD suggests the criteria that should serve as a foundation for a doctrine governing such secondary usages.

This article attempts to show that the CAPD provides a coherent normative doctrine that can be employed by the courts and legislatures and that is more systematic, less subjective, and at least as operational as the prevailing privacy doctrines. It deals with the right to privacy vis-à-vis the United States government rather than as a protection from intrusions by private actors such as corporations. Part I of this article summarizes and develops the previously-published doctrine. Part II compares the coherence

† I am indebted to Peter Swire, Joris van Hoboken, and Daniel Pesciotta for profound comments on a previous draft, to Erin Syring for research assistance, and to Thomas Rory Donnelly for editorial comments on a previous draft.

[1] Amitai Etzioni, *A Cyber Age Privacy Doctrine: A Liberal Communitarian Approach*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 641 (2014).

and objectivity of the CAPD to those of other doctrines and indicates the ways the CAPD can be operationalized.

I. THE CYBER AGE PRIVACY DOCTRINE REVISITED

The advent of the cyber age—also referred to as the digital revolution—requires a new privacy doctrine. The main, although not only, reason for this requirement is that the proportion of privacy violations that result from secondary usages of personal information compared to those that result from primary collection has radically changed. Most privacy violations in the paper age resulted from primary collection; most violations in the cyber age result from secondary usages of information that has been legally collected. If a collection was deemed legal in the paper age, there were still very sharp limits, at least in practice, on the additional uses to which this information could be put.[2] Thus, the danger that it would be abused was relatively limited. In the cyber age, information can be collated much more readily with other items of information, analyzed, and distributed; these processes together comprise "cybernation."[3]

The difference in the extent of secondary usages between the paper age and the cyber age is of such a magnitude that one is hard put to find a measurement or analogy to express it. The difference is much greater than the difference between the impact of a hand grenade and that of a nuclear bomb. Indeed, most secondary analyses conducted these days by using a laptop within a very short period of time—not to mention what is carried out in the "cloud"—could not be carried out at all in the paper age. Because this point is crucial to all that follows, and because people have become so accustomed to the cyber age's information facilities, a simple example follows to illustrate the transformation's scope. Interpol's database of lost and stolen travel documents includes more than 39 million entries reported by 166 countries.[4] When travelers pass through airport security, authorities can determine in a split second whether the passports they carry are on the Interpol list.[5] Such an operation would have been unimaginable a

---

[2] For example, in the paper age, arrest records were kept by local police departments; if an individual wanted to see if a given person had ever been arrested, they would have to review many different police departments' files. *See id.* at 668.

[3] *Id.* at 642-43.

[4] Elisha Fieldstadt & Becky Bratu, *Missing Passport Databases Not Routinely Checked: Interpol*, NBC NEWS (Mar. 9, 2014, 10:09 AM), http://www.nbcnews.com/storyline/missing-jet/missing-passport-databases-not-routinely-checked-interpol-n48261.

[5] Josephine Wolff, *Papers, Please: How to Make Every Country Check Passports to Make Sure They Aren't Stolen*, SLATE (Mar. 11, 2014, 4:42 PM),

mere two decades ago. Among others who have pointed to the rising problem posed by secondary usages of personal information—and have suggested the direction in which governments and the private sector may next move—are Peter Cullen, Fred Cate, Viktor Mayer-Schönberger, and Craig Mundie.[6]

However, most relevant court cases in the United States deal mainly with the primary collection of personal information, much of which falls into the category of "spot collection."[7] These cases concern whether the collection of information through drug testing, wiretaps, screening gates at airports, DNA sampling, breathalyzers, and so forth constitutes a search in Fourth Amendment terms; that is, they concern whether collection should be freely allowed or should require authorization by a distinct institution following given procedures. Notable cases include, among others, *Katz v. United States*,[8] *Terry v. Ohio*,[9] *United States v. White*,[10] *United States v. Knotts*,[11] *United States v. Karo*,[12] *Kyllo v. United States*,[13] *United States v. Jones*,[14] and *Florida v. Jardines*.[15] The courts, in these and other such cases, pay little mind to the privacy violations that occur when personal information that is legally collected is later stored, combined with other information, and analyzed. They, consequently, do not address the fact that information that has been legally collected may be used later to harm the privacy of the individuals involved, harm of such an order that the courts would have prevented it, had it been caused by collection. A privacy doctrine suitable for the cyber age must address both primary collection and subsequent secondary usages of information. Details follow, but as a general principle the government can allow some kinds of personal information to be freely collected and used

---

www.slate.com/articles/technology/future_tense/2014/03/mh_370_stolen_passports_why_don_t_most_countries_check_interpol_s_sltd_database.html.

[6] Craig Mundie, *Privacy Pragmatism: Focus on Data Use, Not Data Collection*, FOREIGN AFFAIRS (Mar./Apr. 2014), http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism; *Reinventing Privacy Principles for the Big Data Age*, OXFORD INTERNET INST. (Dec. 6, 2013), http://www.oii.ox.ac.uk/news/?id=1013.

[7] This article uses the term "spot collection" to mean the collection of a very small amount of information, about one limited facet of the person's conduct, that is neither stored nor cybernated in any other ways—for instance, the information collected by those tollbooths that immediately erase data once the computer has established that the proper toll has been paid.

[8] Katz v. United States, 389 U.S. 347, 353 (1967).

[9] Terry v. Ohio, 392 U.S. 1, 27 (1968).

[10] United States v. White, 401 U.S. 745, 753 (1971).

[11] United States v. Knotts, 460 U.S. 276, 285 (1983).

[12] United States v. Karo, 468 U.S. 705, 713 (1984).

[13] Kyllo v. United States, 533 U.S. 27, 34 (2001).

[14] United States v. Jones, 132 S. Ct. 945, 954 (2012).

[15] Florida v. Jardines, 133 S. Ct. 1409, 1417-18 (2013).

without causing undue risks to privacy. Some other kinds of information might be considered private and therefore should not be collected or used unless a specific authority, following specific procedures, grants an agent a license to do so. In other cases, collection of some information should be allowed, but the government should, from the onset, be limited or banned from carrying out secondary usages of the information. To express this notion in terms of the expectation of privacy, an individual suspected of a crime should expect to be questioned by the police but should also be able to expect that their answers will be locked away if they are found innocent.

Several overarching legal doctrines do address the issues raised by secondary usages and cybernation. This article addresses two of these. First, the third party doctrine holds that once a person has knowingly relayed information to a third party, the sharing of this information with law enforcement officials by the intermediate party does not constitute a Fourth Amendment search and therefore requires no warrant. The Supreme Court ruled in *United States v. Miller*[16] and *Smith v. Maryland*[17] that business records such as financial documents and records of phone numbers dialed are not protected from warrantless collection by law enforcement agencies under certain circumstances.[18] The Court also held that law enforcement's collection of the content of conversations between suspects and third party informants is not presumptively unconstitutional, because those third parties could pass along the information to the police, even without technological assistance.[19] Richard A. Epstein summarizes the third party doctrine as follows: "The received judicial wisdom is that any person who chooses to reveal information to a third person necessarily forfeits whatever protection the Fourth Amendment provides him."[20]

---

[16] United States v. Miller, 425 U.S. 435, 441-43 (1976).

[17] Smith v. Maryland, 442 U.S. 735, 736, 742 (1979).

[18] Stephen E. Henderson, *After* United States v. Jones, *After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431, 434 (2013). "According to Justice Blackmun, writing for the majority, '[t]he switching equipment that processed those numbers [was] merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber.'" Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 570 (2008).

[19] Hoffa v. United States, 385 U.S. 293 (1966); Lewis v. United States, 385 U.S. 206 (1966); Lopez v. United States, 373 U.S. 427 (1963); On Lee v. United States, 343 U.S. 747 (1952). For details, *see* RICHARD M. THOMPSON II, CONG. RESEARCH SERV. R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE (June 5, 2014), *available at* http://www.fas.org/sgp/crs/misc/R43586.pdf.

[20] Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199, 1200 (2009).

The third party doctrine is particularly problematic in an age of cybernation. Given that more and more information about people is in the hands of third parties due to the extensive number and scope of transactions and communications carried out in cyberspace and stored in the cloud,[21] if the third party doctrine is allowed to stand, precious little personal information will remain protected from government incursion. Furthermore, because third parties can share information with others and combine it with still more information, the government and corporations can create detailed and intimate dossiers of innocent people unsuspected of crimes. Individuals constantly leave behind a trail of data with every click of a mouse, "data exhaust" akin to the vapors left behind a car.[22] Will Thomas DeVries points out that one of the key characteristics of the "digital revolution" for privacy is that:

> Every transaction with the Internet, every credit card transaction, every bank withdrawal, every magazine subscription is recorded digitally and linked to specific individuals . . . . [T]he impact of the digital age is so deep and pervasive that expansion of a single area of privacy law is unlikely to adequately address the problems . . . . Since the digital age affects every aspect of privacy, it requires an evolution not just in the existing framework, but in the very conceptual and legal status of privacy.[23]

Many other scholars have criticized the third party doctrine.[24]

Another doctrine that speaks to the cybernation challenge, in effect, takes the opposite tack.[25] It assumes that

---

[21] "[T]he Taneja Group estimated the total cloud storage hardware market in 2010 was $3.2 billion, growing 31 percent per year to $9.4 billion by 2014." Patrick Scully, *Cloud Storage*, BROADCAST ENGINEERING (Nov. 1, 2012), http://www.highbeam.com/doc/1G1-341095101.html.

[22] Mundie, *supra* note 6; *see also* Thomas H. Davenport, *Who Owns Your Data Exhaust?*, WALL ST. J. (Nov. 20, 2013, 2:15 PM), http://blogs.wsj.com/cio/2013/11/20/who-owns-your-data-exhaust/.

[23] Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 291-93 (2003).

[24] Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1315 (1981); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 215 (2006); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (2007); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L.J. 549, 564-66 (1990); Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, UCLA J.L. & TECH., Spring 2007, at 1, 3; Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1231 (1983); Andrew J. DeFilippis, Note, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1093 (2006).

[25] Some refer to this doctrine as the fundamental rights approach; others refer to it as the information as property approach. Eric Pfanner, *Guarding a 'Fundamental Right' of Privacy in Europe*, N.Y. TIMES (Nov. 20, 2012),

personal information belongs to the person to whom it applies, that the individual has a right to keep this information private that extends beyond primary collection, and that only the person can agree to secondary usages of the information—even when they have already consented to primary collection.[26] Europeans often cite this doctrine, which is at the foundation of the European Data Protection Directive and the European General Data Protection Regulation;[27] for this reason, this article will refer to it as the European approach.

At first blush, it may seem that the European approach governs a wholly different area of privacy than the CAPD, which, to reiterate, deals with the right to privacy *vis-à-vis* the government rather than *vis-a-vis* private actors such as marketers and data brokers. The European model is nonetheless relevant because it turns out that, to generalize, governments regularly use personal information collected by private actors. Thus, the limitations imposed on private actors affect the scope of government intrusions. To illustrate: it is difficult to imagine the conditions, short of an extreme national emergency, under which the United States government could require all American citizens to turn over to law enforcement records of their purchases on the Internet, their emails, and their other transactions. However, because the same American citizens "disclose" this information to private corporations, and these corporations aggregate this information, the government in effect can use the resulting databases without seeking permission for these secondary usages.[28]

Many common goods—including public safety, commerce, and research—could suffer greatly if the European Union were

---

http://www.nytimes.com/2012/11/21/technology/guarding-a-fundamental-right-of-privacy-in-europe.html?_r=0; *see, e.g.*, Christopher Rees, *Tomorrow's Privacy: Personal Information as Property*, 3 INT'L DATA PRIVACY L. 220 (2013).

[26] "The EU's proposal includes three elements in particular that lend themselves to a property-based conception: consumers are granted clear entitlements to their own data; the data, even after it is transferred, carries a burden that 'runs with' it and binds third parties; and consumers are protected through remedies grounded in 'property rules.'" Jacob M. Victor, Comment, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L.J. 513, 515 (2013).

[27]

> Though the Regulation is framed in the fundamental-human-rights terms typical of European privacy law, this Comment argues that it can also be conceived of in property-rights terms. The Regulation takes the unprecedented step of, in effect, creating a property regime in personal data, under which the property entitlement belongs to the data subject and is partially alienable.

Id.

[28] Amitai Etzioni, *The Privacy Merchants: What Is To Be Done?*, 14 U. PA. J. CONST. L. 929, 950 (2012).

to adhere strictly to its suggested limitations on secondary usages. It is therefore fortunate that the European laws include a policy that certain secondary usages of personal information, such as those for public health or security, do not require consent.[29] Thus, the Data Protection Directive provides exemptions in cases of "(a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection, and prosecution of criminal offences . . . (e) . . . monetary, budgetary, and taxation matters," and a few other cases.[30] "[T]he exceptions have to become the rule," wrote Joris van Hoboken, "which means that the meaning of the fundamental right, even if one would want to more categorically protect certain core interests, is . . . eroded."[31] Moreover, the European approach is riddled with other weaknesses that make it difficult to implement uniformly.[32] In other words, it is hardly a sound approach.

Moreover, privacy statements provided by businesses and other agents that rely on the collection of consumer data are frequently extensive and draw on legal terminology, making them incomprehensible to most users. Consent means little if those who consent cannot possibly understand that to which they are consenting.[33] In short, the European approach seems not to provide a sound foundation for dealing with secondary usages.

---

[29] For example, restrictions on certain kinds of personal data processing do not apply

> where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Council Directive 95/46, art. 8, 1995 O.J. (L 281) 31, 41 (EC), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN. Alternately,

> Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for [by the directive] when such a restriction constitutes a necessary measure to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters . . .

Id. at art. 13, 1995 O.J. (L 281) 42.

[30] *Id.*

[31] Letter from Joris van Hoboken to author (Apr. 25, 2014) (on file with author).

[32] NEIL ROBINSON ET AL., RAND CORP., REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE 26 (2009), *available at* http://www.hideproject.org/downloads/references/review_of_eu_dp_directive.pdf.

[33] Mundie, *supra* note 6.

If the third-party doctrine is truly followed, it leaves little privacy; if the European approach is truly followed, it undermines the common good. It seems clear that a different doctrine dealing with cybernation is needed—one that is neither as permissive as the third party doctrine nor as strict as the European approach. This monumental task, for which I can provide at best a first approximation, is what this article sets out to chart in the following pages.

Moreover, even initial collection, including limited "spot collection," calls for a new doctrine. Since *Katz v. United States* (1967), the courts have relied on the expectation of privacy to determine which types of primary collection are constitutional. For reasons spelled out in my original paper on this topic,[34] the expectation of privacy is an indefensible basis for such judgments. Briefly, the expectation of privacy test is tautological: if a judge rules that a person's expressed claim to an expectation of privacy meshes with the judge's ideas about what a "reasonable" individual might expect, the expectation of privacy exists. If the judge rules otherwise, the person should not have "reasonably" expected to have privacy.[35] Thus, whether or not Mr. Katz, a gambler, expected or did not expect to have privacy when he placed bets in a public phone booth is immaterial; he had a reasonable expectation of privacy if a court divined that he had a reason to have it, and he had no such expectation if a court ruled otherwise.

The societal expectation of privacy is also subjective. The test presumes that the courts can evaluate such expectations, yet judges have no way of knowing what a "reasonable" person would actually expect—and reasonable people differ greatly in their expectations. Judges do not conduct surveys to discover the expectations of privacy held by a community. Even if they were to do so, the results would differ based on the judges' decisions about which is the relevant community and would be much

---

[34] Etzioni, *supra* note 1.

[35] Many scholars criticize the circular reasoning of the "reasonable expectation of privacy" text outlined in *Katz*. *See*, *e.g.*, Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 188 (1979) (it is "circular to say that there is no invasion of privacy unless the individual whose privacy is invaded had a reasonable expectation of privacy; whether he will or will not have such an expectation will depend on what the legal rule is"); *see also* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974); Richard S. Julie, *High-Tech Surveillance Tools and the Fourth Amendment: Reasonable Expectations of Privacy in the Technological Age*, 37 AM. CRIM. L. REV. 127, 132 (2000); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 106 (2008); Richard H. Seamon, Kyllo v. United States *and the Partial Ascendance of Justice Scalia's Fourth Amendment*, 79 WASH. U. L. Q. 1013, 1023-24 (2001). The Court acknowledged this criticism in *Kyllo*. Kyllo v. United States, 533 U.S. 27, 33 (2001).

affected by minor changes to the questions' wordings. The courts point to their own shadows as independent grounds for their rulings. In short, the whole legal edifice based on the expectation of privacy is fundamentally flawed and should be allowed to fade and be replaced by a new, better privacy doctrine.

The need for a new privacy doctrine stands out in particular when one reviews the major court cases that currently provide the basis for deliberations on privacy by the public, law enforcement authorities, policy makers, and courts. Each case seems to rely on a different rationale; some of these rationales are obsolete, and some are surprisingly idiosyncratic (a harsher critic would call them capricious). In one the Court found unconstitutional the planting of a GPS device because it constituted trespassing;[36] another found unconstitutional the use by law enforcement of a thermal imaging device on the grounds that it was not a technology then in common public use;[37] others have referenced the "special needs" exception;[38] yet another held that the presence of a police narcotics dog at the door of a residence was sufficiently dissimilar to the act of a private citizen knocking on the door as to be unconstitutional without a warrant.[39] Whatever limitations the preliminary CAPD outlined below has, it is surely less subjective than judges' intuitions as to what constitutes a reasonable expectation of privacy and is surely more systematic than the curious amalgam of court cases that currently govern the field.

The liberal communitarian philosophy—which holds that individual rights, including privacy, have the same fundamental standing as the common good and that neither *a priori* trumps the other—provides an excellent normative foundation for just such a new doctrine. Each society works out a balance between the two claims, which is often adjusted to take into account changes to the society's international environment, domestic social developments, and changes in technology. For example, if the United States suffers several new terrorist attacks, a crime wave of the kind that swamped American cities in the 1970s, or a pandemic caused by a new kind of flu, society will likely legitimate moving the point of balance closer to the common good—and away from the protection of individual rights such as privacy. If the current state of affairs continues—that is, there are lower crime rates, no significant terrorist attacks, and no pandemics—the balance is likely to shift in the opposite direction. In the wake of the Snowden disclosures,

---

[36] United States v. Jones, 132 S. Ct. 945, 950 n.3 (2012).
[37] *Kyllo*, 533 U.S. at 27.
[38] New Jersey v. T.L.O., 469 U.S. 325, 332 n.2 (1985).
[39] Florida v. Jardines, 133 S. Ct. 1409, 1417-18 (2013).

for example, public figures have called for reversing the shift towards security that followed 9/11.[40]

The Fourth Amendment exemplifies the liberal communitarian approach. It does not categorically state that there shall be no searches and seizures; instead, it bans only *unreasonable* ones. The Fourth Amendment also provides a mechanism for deciding which of the two claims should be accorded priority; courts determine whether or not there is enough evidence that a given person is endangering the public interest to justify their subjection to legal surveillance. Finally, the Fourth Amendment implies that surveillance should be as limited and non-intrusive as possible.[41]

The following analysis focuses exclusively on one of the two elements of liberal communitarianism: individual rights, in particular the right to privacy. It seeks to outline the principles that should guide the courts and legislatures in determining the kinds and scope of intrusions by the government that should be tolerated, banned, or allowed only with prior authorization. The analysis holds constant the level of contribution to the public good accomplished by these intrusions and studies only changes in the level of privacy violation. This "control" is necessary because, as already indicated, if there was to be a significant change in the threats facing the common good—whether an increase or a decrease—the balance between privacy and security (and other common goods) would have to be recalibrated. I have explored this subject elsewhere.[42]

II. OPERATIONALIZATION OF THE KEY PRINCIPLES

Above all, this paper will attempt to show that the CAPD is more coherent and less subjective than the prevailing doctrines.

---

[40] For example, Sen. Patrick J. Leahy (D-VT), co-sponsored a bill that would have limited the NSA's powers to conduct surveillance. *See* Ellen Nakashima & Ed O'Keefe, *Senate Fails to Advance Legislation on NSA Reform*, WASH. POST (Nov. 18, 2014), http://www.washingtonpost.com/world/national-security/senate-fails-to-advance-legislation-on-nsa-reform/2014/11/18/a72eb7fc-6f70-11e4-8808-afaa1e3a33ef_story.html.

[41] *See generally* United States v. Place, 462 U.S. 696, 700-03 (1983); Katz v. United States, 389 U.S. 347, 352-54 (1967).

[42] *See generally* Amitai Etzioni, *A Liberal Communitarian Conception of Privacy*, 29 J. MARSHALL J. COMPUTER & INFO. L. 419 (2012).

A. The Three Dimensions of the Cyber Age Privacy Doctrine "Cube"

The new doctrine draws on three principal criteria: the volume, level of sensitivity, and degree of cybernation of information collected. Together, these dimensions form a cube; this conceptualization contrasts with the idea of information collection as a "mosaic."[43]

1. Volume

Volume concerns the total amount of information collected about a person by one agency and amassed in one database. The measurement refers to one agency and one database because the law should differentiate between that which *one* agent may collect and that which may be collected in total by *multiple* agents. The law may greatly limit, for example, the information a health inspector, an OSHA specialist, or an IRS agent may individually collect about a given restaurant, but the total amount they and others are allowed to collect will obviously be much more extensive.

This dimension of the CAPD is relatively easy to operationalize, and it encompasses two components. The first of these is *quantity*, which simply concerns the amount of information collected, whether this is measured in terms of emails, phone records, text messages, or, better yet, in terms of megabytes of information.[44] The length of time of a wiretap is in effect a crude but useable measurement of quantity. It is crude because there is no strong correlation between the amount of time a tap is in place and the amount of information collected; parties under surveillance may vary a great deal in the extent to which they use a tapped phone. At the same time, the metric is useable because it may not be practical to allow the authorities to collect a specific number of calls or bytes of information. There are many precedents for this approach. For example, at present the courts limit wiretap orders

---

[43] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 329 (2012).

[44] Though, arguably, restrictions or guidelines on the megabytes of information to be collected should vary based on the type of information. This is because the byte is, strictly speaking, a measure of data, not information. One hundred MB of *data*, for example, is enough for thousands of text emails but less than five minutes of high quality video, and the former could provide a much greater amount of private *information* than the latter.

to 30 days and grant additional 30-day extensions in accordance with the Wiretap Act.[45]

In the case of emails and similar data, the Electronic Communications Privacy Act of 1986 dictates that upon receiving a preservation request from law enforcement officials, telecommunications providers shall:

> [T]ake a "snapshot" of available electronic records in the account which is held pending legal process (such as a search warrant, court order, or subpoena). [This information is] held for 90 days until legal process is obtained and submitted to the provider. The 90 day preservation can be extended once more for an additional 90 days.[46]

In short, there is ample precedent for using time as a crude approximation for determining whether a collection of personal information is acceptable or excessive.

Taking volume into account, rather than merely asking whether a single collection constitutes a search, finds support in Justice Alito's concurring opinion in *United States v. Jones.* This case concerned the installation of a GPS tracking device on Jones' car after the State's warrant had expired.[47] The GPS tracking device was activated constantly for 28 days. The majority opinion did not address the lengthiness of the GPS surveillance, but the concurring opinion by Justice Alito stated that the length of the surveillance was a factor in ruling that this tracking constituted a Fourth Amendment search. Alito writes,

> [T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with

---

[45] *Surveillance Self-Defense: Getting a Court Order Authorizing a Wiretap*, ELECTRONIC FRONTIER FOUND., https://web.archive.org/web/20140529054606/https://ssd.eff.org/wire/govt/wiretapping-authorization (last updated May 29, 2014).

[46] Kevin V. Ryan & Mark L. Krotoski, *Caution Advised: Avoid Undermining the Legitimate Needs of Law Enforcement to Solve Crimes Involving the Internet in Amending the Electronic Communications Privacy Act*, 47 U.S.F. L. REV. 291, 321 (2012), *available at* https://www.usfca.edu/uploadedFiles/Destinations/School_of_Law/Academics/Co-Curricular_Programs/(5)SAN47-2RyanandKrotoski.pdf.

[47] "The Government obtained a search warrant permitting it to install a Global-Positioning-System (GPS) tracking device on a vehicle registered to respondent Jones's wife. The warrant authorized installation in the District of Columbia and within 10 days, but agents installed the device on the 11th day and in Maryland." *Jones*, 132 S. Ct. at 946.

> precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.[48]

The opinion elicited a critical comment by Orin Kerr, who asked what standard would determine when a mosaic has been created.[49] Kerr writes:

> In *Jones*, the GPS device was installed for twenty-eight days. Justice Alito stated that this was "surely" long enough to create a mosaic. But he provided no reason why, and he recognized that "other cases may present more difficult questions." If twenty-eight days is too far, how about fourteen days? Or 3.6 days? Where is the line?[50]

In response, one notes that there are numerous such cut-off points in law, such as the number of days suspects may be detained before they must be charged or released, the ages at which voting and driving become legal, the number of jurors a jury must include, and so on. One may say that these cut-off points reflect the ruling of a "reasonable" person. Actually, they reflect that which judges or legislators consider a compromise between a restriction that is clearly excessive and one that is clearly inadequate—a line that has been adjusted often. There is no reason the volume of collection that society is prepared to recognize as "reasonable" should not be similarly governed. Moreover, the criteria here employed are on the face of it less subjective and more measurable than what a person or society expects or what the founding fathers were thinking.

Moreover, for the first approximation purposes here attempted, it is unnecessary to provide specific numbers to limit various information collection operations. This is a task for another article. This article will instead begin by recognizing the most significant difference regarding volume: the difference between "spot collections," the one-time collection of one or very few discrete pieces of information over a very short period of time, such as those carried out by speed cameras at intersections, TSA agents during airport security screenings, and many CCTV cameras, and prolonged collections, including wiretaps or continuous GPS tracking.[51] Those familiar with these issues may

---

[48] *Id.* at 964.

[49] Kerr, *Mosaic*, *supra* note 43, at 329.

[50] *Id.* at 333.

[51] To clarify, speed cameras tell only what speed a vehicle is going at a single moment in time—that is, they collect one discrete data point. The same is true of an airport screening, which detects information about an individual only at one given point in time. A single CCTV camera is limited in its ability to collect information; it cannot collect information about a passing individual except while that person is within range of the camera. By contrast, wiretaps or continuous GPS monitoring collect

protest that certain spot collection programs are relatively comprehensive because they capture all individuals who walk through an area, for example. However, as will be emphasized later, a large quantity of information can be collected without divining meaning from the information through cybernation.

The second concept relevant to the dimension of volume is *informational bandwidth*, a term here used to refer to the collection of different types of information from or about a single subject. Collection of only one type of information, such as the metadata associated with an individual's phone calls, emails, or locations, constitutes narrow bandwidth collection. By contrast, the collection of several kinds of information—say, phone call content *and* voice data *and* text message content *and* email content—constitutes broad bandwidth collection. Bandwidth is important because if it is broad it allows law enforcement to gain a much more comprehensive profile of the person under surveillance than when it is narrow, and diminishes privacy much more.

One might argue that when high quantities of data are collected, even on a narrow bandwidth, as is the case with "big data," a comprehensive picture of the individual's private life is created. However, these concerns do not take into consideration the limits on cybernation proposed by this article, limits that would apply particularly strongly to sensitive information. These limits—including a ban on cybernating non-sensitive information in order to divine sensitive information—would restrict, legally speaking, the ability to create such comprehensive pictures when it would be detrimental to privacy to do so. For the CAPD to be effective, all three dimensions—volume, sensitivity, and cybernation—must be applied simultaneously. Considering high volume collections without simultaneously considering the sensitivity of the information involved and the level of cybernation to which it is subjected produces an incomplete picture of the privacy violations—or lack thereof—caused by a particular collection. Unbounded "big data" may well blur the difference between collection and cybernation; however, "big data" limited by the suggested restrictions would be much less prone to damaging privacy.

Just as the length of time surveillance is conducted or the number of messages collected by a search are crude but useable measures of volume, so is the number of collection methods a crude but useable measure of bandwidth. This is the case

---

many data points about the individual over a long range of time and paint a much more comprehensive picture of the person's movements or associations.

because some surveillance methods are able to gather many more types of information about an individual than others. For instance, taping phone conversations (which captures the complete content of a call, potentially including many kinds of information) is a much broader bandwidth method than the collection of phone records (which capture who called whom, at what time, and from where). For traffic control purposes, it is possible to measure the speed at which a vehicle travels in public places without taking a picture of the person sitting next to the driver in the front seat (incidentally, speed cameras are set lower, at the level of license plates). A more sophisticated measure of bandwidth could take into account these differences.

2. Sensitivity

The concept that some kinds of information are more sensitive than others has been often articulated by privacy scholars and operationalized by lawmakers, albeit using a variety of terms. Additional terms that have been applied include "intimate information" or "revealing information," and some scholars have defined them in terms of the level of risk to one's privacy or the extent of harm to one's privacy.[52] Still others refer to some searches as "highly intrusive."[53]

Two levels of distinction between types of information must take place in order to enable the development of a nuanced understanding of sensitive information. The first level of distinction is very basic; it merely establishes the realm of information to be considered, distinguishing personal information from other forms of information that either do not deal with persons or have been de-identified or anonymized in ways that are presumed to be irreversible.[54] Briefly, all non-personal information is inherently not sensitive. Revealing the amount of rain that falls in Spain, for example, endangers no one's privacy. The issue of sensitivity concerns the second level of distinction, which distinguishes among the various kinds of personal information.

---

[52] *Reinventing Privacy Principles for the Big Data Age*, *supra* note 6.

[53] Daniel T. Pesciotta, *I'm Not Dead Yet:* Katz*,* Jones*, and the Fourth Amendment in the 21st Century*, 63 CASE W. RES. L. REV. 187, 237 (2012).

[54] This is a subject about which much has been written; it is, therefore, not further explored here. Paul M. Schwartz and Daniel J. Solove note, though, that "numerous federal statutes turn on [the distinction between personally-identifiable information and other forms of information]." Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1816 (2011).

Quite a few leading privacy advocates, including ACLU President Susan Herman,[55] rail against the collection of multiple types of personal information by the government. In response to the introduction of airport screening gates to prevent skyjackings, one of ACLU's staff counsels wrote that "the new [general] passenger screening regulations are completely inconsistent with the values safeguarded by the fourth amendment [sic]."[56] The ACLU has also opposed speed cameras at traffic intersections, calling them "extreme,"[57] as well as the use of cookies on federal government websites[58]—without which many Internet activities might well be impossible. (In fact, the ACLU website itself now uses them.[59]) Some strong privacy advocates concede that exceptional conditions exist under which surveillance and other forms of personal information collection might be justified, but they hold that the onus is on the government to prove that such conditions are in place.[60] They, furthermore, set a very high bar that must be cleared before they consider an intrusion to be justified.

Instead, the CAPD holds—following many others—that not all personal information can or should be accorded the same level of protection, and that the more sensitive the information an agent seeks to collect, the more measures to protect privacy should be implemented and the higher the public interest must be before collection of the information is legitimated.

What ought to determine the sensitivity of a piece of information? Measurements of sensitivity should reflect the values of the society in question. Some societies, for example, consider expressions of affection or intimacy, let alone sexual relations, highly sensitive and private matters, while other societies take a less constricted approach. For instance, Americans consider women's breasts to be highly private, while many Europeans consider it acceptable to go bare on the beaches. In

---

[55] *See generally* SUSAN N. HERMAN, TAKING LIBERTIES: THE WAR ON TERROR AND THE EROSION OF AMERICAN DEMOCRACY (2011).

[56] Joel M. Gora, *The Fourth Amendment at the Airport: Arriving, Departing, or Cancelled?*, 18 VILL. L. REV. 1036, 1038 (1973).

[57] Jay Stanley, *Extreme Traffic Enforcement*, ACLU (May 24, 2012, 2:05 PM), https://www.aclu.org/blog/technology-and-liberty-criminal-law-reform/extreme-traffic-enforcement; Press Release, ACLU, ACLU of Iowa Challenges Use of Speed Cameras in Davenport (June 14, 2006), *available at* https://www.aclu.org/technology-and-liberty/aclu-iowa-challenges-use-speed-cameras-davenport.

[58] Press Release, ACLU, Government Proposes Massive Shift in Online Privacy Policy (Aug. 10, 2009), *available at* https://www.aclu.org/free-speech_technology-and-liberty/government-proposes-massive-shift-online-privacy-policy.

[59] *American Civil Liberties Union Privacy Statement*, ACLU (Jan. 18, 2013), https://www.aclu.org/american-civil-liberties-union-privacy-statement.

[60] *See generally* HERMAN, *supra* note 55.

another example, the cultural norms of some groups hold that disputes should be resolved in private, while the Mambila people of Nigeria consider it important to act "within the sight of everyone" because "[o]nly witches act secretly, eating behind closed doors or conducting financial transactions at night,"[61] . . . and "[q]uarrels held in public are seen as dangerous since witches may 'hide' behind them."[62] This is not to say that any particular society's standards of privacy are superior, merely that they are affected by the particular normative culture of the given society and are a major factor in determining what the legal system considers sensitive personal information.

In each society, the legislatures and courts operationalize these differences in the normative standing of different kinds of information. In the United States, this ranking has been mainly brought about by Congress enacting piecemeal a series of specific laws. For example, the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) treats protected health information (PHI)[63]—the identifying information that would

---

[61] David Zeitlyn, *The Talk Goes Outside: Argument, Privacy and Power in Mambila Society Towards a Sociology of Embedded Praxis*, 73 AFRICA: J. INT'L AFRICAN INST. 606, 607 (2003).

[62] *Id.* at 608.

[63] PHI is information, held by health care providers, defined as:

> 1. Name, including current, previous, and mother's maiden name
>
> 2. Postal address and all geographical subdivisions smaller than a State . . . except for the initial three digits of a zip code . . . .
>
> 3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, [and so forth]
>
> 4. Telephone numbers
>
> 5. Facsimile numbers
>
> 6. Electronic mail addresses
>
> 7. Social security numbers
>
> 8. Medical record numbers
>
> 9. Health plan beneficiary numbers
>
> 10. Account numbers
>
> 11. Certificate/license numbers
>
> 12. Vehicle identifiers and serial numbers, including license plate numbers
>
> 13. Device identifiers and serial numbers
>
> 14. Web Universal Resource Locators (URLs)
>
> 15. Internet Protocol (IP) address numbers
>
> 16. Biometric identifiers, including finger and voice prints

associate an individual with records of their medical conditions—as highly sensitive, with restrictions on the disclosure of psychotherapy notes being especially tight.[64] The Department of Health and Human Services' description of HIPAA's Privacy Rule states that HIPAA "creates, for the first time, a floor of national protections for the privacy of [consumers'] *most sensitive* information—health information."[65]

Following the Supreme Court's decision in *United States v. Miller*,[66] Congress passed the Right to Financial Privacy Act, which restricted financial institutions' ability to share "any record . . . pertaining to a customer's relationship with the financial institution."[67] Several other specific kinds of information have been deemed sensitive enough to protect through federal law. Records of video rentals were protected, for example, through the Video Privacy Protection Act of 1988 following the revelation of a list of movies rented by the family of Supreme Court nominee Robert H. Bork.[68] Additional types of information entitled to a higher level of protection include education records (Family Educational Rights and Privacy Act),[69] genetic information (the federal Genetic Information Nondiscrimination Act of 2008[70]), and journalistic sources (Privacy Protection Act of 1980[71]), among others. The FTC has issued guidelines that sensitive data includes five categories of information, namely financial information, health information, Social Security numbers, information collected from children, and geo-location information such as the information

---

17. Full face photographic images and any comparable images

18. Any other unique identifying number, characteristic, or code (other than a unique study ID)

David T. Fetzer & O. Clark West, *The HIPAA Privacy Rule and Protected Health Information: Implications in Research Involving DICOM Image Databases*, 15 ACAD. RADIOLOGY 390, 390-91 fig.1 (2008).

[64] 45 C.F.R. § 164.508(a)(2) (2013).

[65] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,182 (Aug. 14, 2002) (emphasis added), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privrulepd.pdf.

[66] United States v. Miller, 425 U.S. 435 (1976).

[67] 12 U.S.C. § 3401(2) (2012); *id.* §§ 3402-3422.

[68] Harold C. Relyea, *Legislating Personal Privacy Protection: The Federal Response*, 27 J. ACAD. LIBRARIANSHIP 36, 43 (2001).

[69] 20 U.S.C. § 1232g (2013); 34 C.F.R. Part 99 (2014), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2014-title34-vol1/pdf/CFR-2014-title34-vol1-part99.pdf.

[70] Genetic Information Nondiscrimination Act of 2008, Pub.L. 110–233, 122 Stat. 881 (2008).

[71] "The Act prohibits law enforcement officials from searching for or seizing information from people who disseminate information to the public, such as [the media]. Where it applies, the Act requires law enforcement officials to instead rely on compliance with a subpoena." Elizabeth B. Uzelac, Note, *Reviving the Privacy Protection Act of 1980*, 107 NW. U. L. REV. 1437, 1437 (2013).

gleaned from cell phone tracking.[72] Legislation has been advanced—but not yet passed—to grant this status to information about race and ethnicity, religious and political beliefs, sexual orientation, and "unique biometric data."[73] In all these cases, the kinds of information considered sensitive were denoted rather than defined. That is, lists of examples rather than defining attributes defined each category. To illustrate with a more concrete example, listing the names of all qualifying cities would constitute denotation, whereas stating that any population center with more than 100,000 people qualifies would constitute definition.

When Congress seeks to classify particular classes of personal information as more sensitive than others, it often relies on the rationale that privacy law should prevent economic or physical harm; that is, sensitive information is defined as information the unauthorized disclosure of which could cause tangible harm.[74]

Sensitivity has also been operationalized through enumeration of the specific kinds of information that are or are not sensitive rather than through the articulation of a defining attribute. HIPAA, for example, defines protected health information as that which "is maintained or transmitted in any form . . . and relates to the past, present, or future physical or mental condition of an individual; provision of health care to an individual, or payment for that health care; and identifies or could be used to identify the individual."[75] The Fair Credit Reporting Act of 1970 likewise regulates the disclosure of "consumer reports," which encompass any information "that bears on a consumer's credit worthiness or personal characteristics when used to establish the consumer's eligibility for credit, insurance, or for a limited set of other purposes."[76]

The courts have also contributed to the categorization of sensitive information. In *United States v. Jones*, Justice Sotomayor joined the majority opinion and issued her own concurring opinion, in which she articulated that even short-term GPS monitoring impinges on privacy rights because it "reflects a wealth of detail

---

[72] Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 AM. BUS. L.J. 413, 424-31 (2013).

[73] *Id.* at 430.

[74] *Id.* at 431.

[75] PHI is further elaborated in the law, with 16 specific data fields named as patient information that must be deleted from health care research manuscripts and other publications. Elizabeth Madsen et al., *HIPAA Possumus*, 10 J. AM. MED. INFORMATICS ASS'N 294, 294 (2003).

[76] Schwartz & Solove, *supra* note 54, at 1821.

about [one's] familial, political, professional, religious, and sexual associations."[77] The courts have also limited government's power to obtain information on individuals' book purchasing histories beginning with *United States v. Rumely* and famously in the case of *In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc.*, in which the government unsuccessfully attempted to subpoena Monica Lewinksy's purchase records.[78]

Critics have pointed out that because various kinds of information have been considered sensitive while others have not—at different points in time and based on different rationales—the result is a "crazy" patchwork "quilt."[79] There is indeed a need for Congress to review these myriad laws and more systematically and consistently categorize the types of personal information that should be better protected than others. However, for the purpose of a first approximation, there is little question that sensitivity can be operationalized, and most sensitive types of personal information have been extensively categorized.

3. Cybernation

Cybernation is the most novel component of the CAPD. Sensitivity was a full-blown factor in the paper age; volume was also an issue in the paper age, although it was one of much less pressing importance due to practical limitations. However, the kinds of processing and secondary usages of personal information engendered by cybernation, as well as their effects on privacy, were inconceivable in the paper age. Cybernation is also the most consequential factor of the three dimensions because it is the one directly tied to the grand shift from focusing on primary collection to prevent privacy violations to focusing on the privacy violations caused by secondary uses. Cybernation includes storing, collating (including building dossiers), analyzing, accessing, and distributing discrete items of information in concert with each other.

Privacy is much better protected if the information collected is not *stored*. If a tollbooth payment system immediately erases the information that a given car was at the booth at a certain point in time once the computer has verified payment of the toll, the risk that the information will be abused to violate

---

[77] United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

[78] United States v. Rumely, 345 U.S. 41 (1953); *In re* Grand Jury Subpoena to Kramerbooks & Afterwords, Inc., 26 Media L. Rep. (BNA) 1599 (D.D.C. 1998); Andrew A. Proia, *A New Approach to Digital Reader Privacy: State Regulations and Their Protection of Digital Book Data*, 88 IND. L.J. 1593, 1608 (2013).

[79] Lawless, *supra* note 24.

privacy is very limited compared to a situation in which the same information is stored. The same is true for speed cameras that erase the car's identifying information once it has been established that the car traveled below the speed limit. By contrast, all data banks, which keep records about even a single particular personal item, such as which magazines the person reads and which bars the person frequents, pose a higher risk to privacy than non-storing mechanisms. This element of cybernation can be operationalized, as a first order of approximation, by determining whether or not the information is stored or instantly erased. As a second order of approximation, if information is stored, the degree of cybernation can be approximated by determining the length of time the information is kept.

With regard to the collation of information about the same person, especially when *building dossiers* is involved, the risk to privacy increases when information collected and stored by one agent is combined with or linked with information collected and stored by other agents. For example, some state rights advocates may prefer state or even regional databases to federal ones. However, one must take into account that these local databases are often *linked* to each other and thus in effect act like one central database. Although the volume of information in each state or local database may well be lower than the amount stored in a national database, that the state and local databases are linked to each other means that those who have access to them have access to the same amount of information that would be gathered in a national database. Many civil rights advocates would also be greatly concerned if the FBI amassed information on most Americans, including those who neither have been charged with any crime nor are under any suspicion—but they pay less mind to data brokers who keep such information and sell access to the FBI.[80] The law must adapt to these technological developments, treat all linked databases as if they were one, and impose limits on collection accordingly.

The risk to privacy is also lower when personal information is merely stored and collated than it is when the same information is *analyzed* to ferret out other information and draw conclusions

---

[80] Etzioni, *supra* note 28; Martin H. Bosworth, *FBI Uses Data Brokers, "Risk Scores" To Hunt Terrorists*, CONSUMER AFF. (July 11, 2007), http://www.consumeraffairs.com/news04/2007/07/fbi_risk_scores.html; Ted Bridis, *FBI: Data Brokers Probably Act Illegally*, WASH. POST (June 22, 2006, 5:50 PM), www.washingtonpost.com/wp-dyn/content/article/2006/06/22/AR2006062200932.html

about the person not revealed by the raw data.[81] For first approximation purposes, this dimension can be operationalized by considering whether such analysis is carried out at all; that is, analysis is contrasted with the mere use of raw information. Additional measurements are needed to establish how much and what kinds of new information are gained through analyses. In particular, it is essential that when the collection and use of sensitive information is banned, so too should analysis that is used to divine the same information from non-sensitive information be banned. It seems that no such bans are yet in place. They are clearly needed because without them, limits on collecting and cybernating sensitive information face the grave danger of being eroded.

Finally, risks to privacy are lower when information collected by one party, such as a hospital or the IRS, is *inaccessible* to other parties or is only made available to other parties under highly special circumstances. The Federal Privacy Act of 1974, for instance, limits the conditions and the degree to which information collected, stored, and analyzed by a given federal agent may be shared with other federal agents or other parties.[82] Distribution and access are two facets of the same process; sharing information captures both forms of cybernation. Here, the relevant measures are, first, the scope of limits set by laws and by regulations; second, the volume of information that is shared; and third, the number of agents with whom the information is shared. For instance, social security numbers were initially meant to be used only by the Social Security Administration and were not meant to be shared with other federal agents—let alone other parties.[83] However, by now they are used very widely. This sharing makes it easier to collate personal information from different sources and draw a much more comprehensive, and therefore, privacy-violating picture of an individual.

To complete the analysis, it is essential to add a variable that at first blush seems rather different; one might well hold that it should be treated as a fourth dimension that would turn a cube composed of volume, sensitivity, and cybernation into a four-dimensional tesseract. For first approximation purposes, this additional variable is treated as negative cybernation and is

---

[81] Otherwise known as divining sensitive information from non-sensitive information.

[82] Privacy Act of 1974, Pub. L. 93–579, 88 Stat. 1896 (1974) (codified at 5 U.S.C. § 552a).

[83] Carolyn Puckett, *The Story of the Social Security Number*, 69 SOC. SEC. BULL. 55, 55 (2009), *available at* http://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.

referred to as *accountability*. All the various "places" at which personal information is collected, stored, and analyzed have at least some barriers to use by unauthorized parties. These include simple devices such as passwords and locks on computers as well as more powerful ones such as firewalls and encryption. Although all of these have a technological element, human factors are also involved. Audit trails, for example, are useless if no one reviews the records detailing who accessed the data and determines if that information has been inappropriately employed.

All accountability measures limit one element of cybernation or another. Some limit sharing by preventing most agents from gaining access to Medicare data; others limit storage by ensuring that data that has been stored more than a given number of days or years is erased; others limit analysis, such as by de-identifying the information. The more extensive and effective accountability measures are, the less cybernation occurs and the better privacy is protected. It follows that the stronger the accountability measures associated with a given database, both in terms of the number of layers and instruments of accountability involved and in terms of the quality of each of these—the fewer privacy violations will occur even if the volume of information is high, the information's sensitivity is considerable, and a significant degree of collation and analysis takes place. Conversely, if accountability is deficient, more violations of privacy will occur even if volume is relatively low, information is relatively non-sensitive, and collation and analysis are not particularly extensive. This demonstrates once again that collection is less important in the cyber age than is the scope of—or limits on—secondary usages, a ratio that is expected to continue to grow significantly due to improvements in artificial intelligence.[84]

That the level of accountability can be operationalized can be gleaned from various debates about whether it is sufficient. For instance, it has been widely argued that the Foreign Intelligence Surveillance Court (FISC) is much too lenient because it has reportedly declined a mere 0.03% of the government's requests for court orders authorizing intentional electronic surveillance of United States persons.[85] Defenders of the Foreign Intelligence Surveillance Act that governs such courts argue that the number

---

[84] *See generally* ERIK BRYNJOLFSSON & ANDREW MCAFEE, THE SECOND MACHINE AGE: WORK, PROGRESS, AND PROSPERITY IN A TIME OF BRILLIANT TECHNOLOGIES (2014).

[85] Evan Perez, *Secret Court's Oversight Gets Scrutiny*, WALL ST. J. (June 9, 2013, 7:11 PM), http://online.wsj.com/news/articles/SB10001424127887324904004578535670310514616?mg=reno64-wsj.

is so low because FBI agents, fearing damage to their careers if their requests are rejected, file only well-justified requests, and because FISC often returns requests for reassessment rather than rejecting them outright.[86] This debate suggests that the data used to assess FISC's strictness need to be further fine-tuned while also showing that accountability can be operationalized.

In June 2013, Gen. Keith Alexander, director of the National Security Agency, testified to the House Intelligence Committee that the surveillance programs revealed by Edward Snowden had contributed to averting "'potential terrorist events' more than 50 times since the September 11, 2001 attacks."[87] However, an investigative report by the New America Foundation found that in the 225 cases of "individuals recruited by al-Qaeda or a like-minded group or inspired by al-Qaeda's ideology, and charged in the United States with an act of terrorism since 9/11," the NSA's collection of phone metadata belonging to United States persons was of minimal help.[88] More specifically, the phone metadata collection program "appears to have played an identifiable role in initiating, at most, 1.8 percent of these cases," while surveillance of non-U.S. persons was helpful to 4.4 percent of the cases, and "NSA surveillance under an unidentified authority" was helpful to 1.3 percent.[89] At *most*, therefore, NSA bulk

---

[86]

> Michael Mukasey, who was attorney general under President George W. Bush, said in an interview that the lack of rejections by the FISA court doesn't mean the court is a rubber stamp. He notes the court sometimes modifies orders and that the Justice Department's national-security division is careful about the applications it presents to the court.

Id.

[87] Sean Sullivan, *NSA Head: Surveillance Helped Thwart More than 50 Terror Plots*, WASH. POST (June 18, 2013, 2:21 PM), http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/18/nsa-head-surveillance-helped-thwart-more-than-50-terror-attempts/.

[88] PETER BERGEN ET AL., NEW AM. FOUND., DO NSA'S BULK SURVEILLANCE PROGRAMS STOP TERRORISTS? 17 (2014), *available at* http://www.newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1_0.pdf.

[89] *Id.* at 1-2. It should be noted that in a full 28% of the cases, the study was *unable to determine* what method initiated the investigation because public records and court records do not reveal this information. The authors *assume* that an undercover informant, a family member, etc. tipped off the police, but the possibility of bulk surveillance playing a role that is not publicly claimed cannot be entirely ruled out. Ellen Nakashima, *NSA Phone Record Collection Does Little to Prevent Terrorist Attacks, Group Says*, WASH. POST (Jan. 12, 2014), http://www.washingtonpost.com/world/national-security/nsa-phone-record-collection-does-little-to-prevent-terrorist-attacks-group-says/2014/01/12/8aa860aa-77dd-11e3-8963-b4b654bcc9b2_story.html. "Regular FISA warrants not issued in connection with Section 215 or Section 702, which are the traditional means for investigating foreign persons, were issued in at least 48 (21 percent) of the cases we looked at." BERGEN ET AL., *supra* note 88, at 2.

surveillance programs may have substantially contributed to 7.5 percent of these investigations—or 16 cases in 12 years.[90]

A report released by the Justice Department in 2004 held that 179 convictions or guilty pleas stemming from 310 investigations of terrorism were materially helped by the Patriot Act.[91] However, a later investigation by *The Washington Post* found that despite President Bush's claims that "federal terrorism investigations have resulted in charges against more than 400 suspects, and more than half of those charged have been convicted," by June 2005, only 39 individuals were actually convicted of terrorism or other crimes against national security.[92] Of the 1755 delayed-notice search warrants authorized by the Patriot Act from 2006 to 2009, only 15 (or 0.8%) were related to terrorism investigations.[93] More than 1,600 warrants were related to drug investigations.[94]

To see the utility of these kinds of data for the operationalization of accountability, one only has to imagine that the figures ran the opposite way and demonstrated that the collections prevented a considerable number of significant terrorist attacks. That is, if the evidence instead showed that the various acts by United States authorities that entailed privacy intrusions served to abort many major terrorist attacks, most Americans would see them as much more justified. In any case, the data clearly allow citizens and their elected officials to assess threat levels, the value of countermeasures, and the effectiveness of accountability.

B. Combined Considerations

The next step is to combine and apply the three key considerations. One may argue that such an application of the CAPD reveals that this is a much more complex doctrine than the

---

[90] Author's personal calculations based on figures from BERGEN ET AL., *supra* note 88, at 4-5.

[91] Dan Eggen, *U.S. Report Divulges Details of Patriot Act's Effectiveness*, CHI. TRIB. (July 14, 2004), http://articles.chicagotribune.com/2004-07-14/news/0407140330_1_library-and-bookstore-records-usa-patriot-act-gen-john-ashcroft.

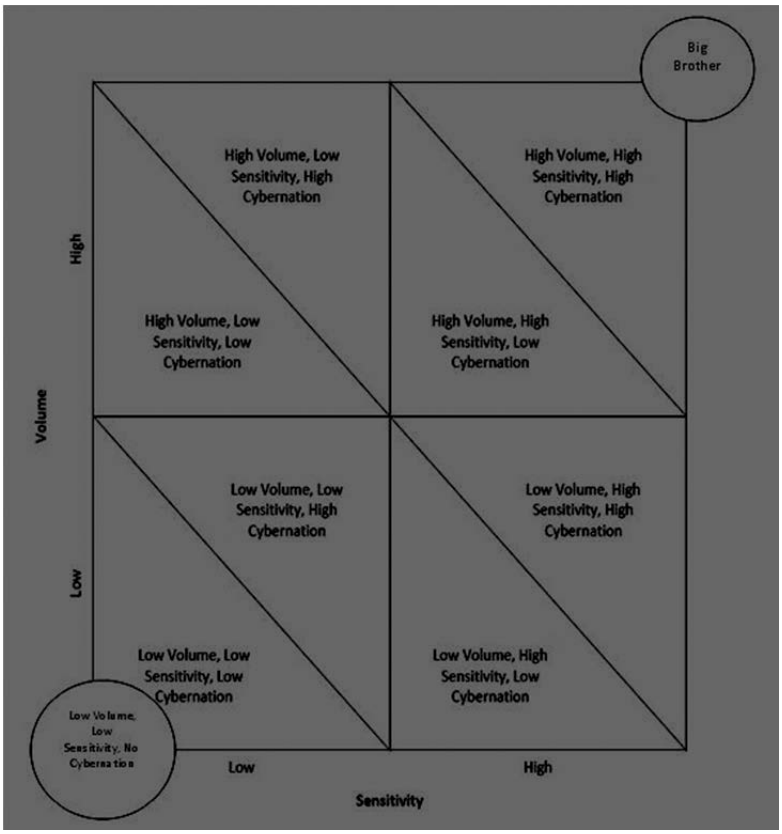
[92] Dan Eggen & Julie Tate, *U.S. Campaign Produces Few Convictions on Terrorism Charges*, WASH. POST (June 12, 2005), http://www.washingtonpost.com/wp-dyn/content/article/2005/06/11/AR2005061100381.html.

[93] Steven C. Bennett et al., *Storm Clouds Gathering for Cross-Border Security and Data Privacy: Cloud Computing Meets the U.S.A. Patriot Act*, 13 SEDONA CONF. J. 235, 245 (2012).

[94] Benjamin Wallace-Wells, *Patriot Act: The Kitchen-sink Approach to National Security*, N.Y. MAG. (Aug. 27, 2011), http://nymag.com/news/9-11/10th-anniversary/patriot-act/.

expectation of privacy rule. This is indeed a valid observation. However, given the explosive growth of the role of information in our private and public lives, its complexity, and the continued expansion of cybernation, a doctrine of privacy of commensurate complexity seems unavoidable. Not all possible permutations are here reviewed, as this article is merely a first attempt to operationalize the CAPD; however, the main ones are considered on a first approximation basis. Moreover, while one day it may well be possible to numerically score each of the elements of the cube, for the preliminary purposes at hand it will suffice to evaluate each in terms of "zones," referring to each variable as "low" or "high." In the process it shall be seen that while the CAPD often leads to rulings and legislation similar to those currently in place, in some cases it calls for reversing the prevailing law. Further, in all cases the CAPD provides a rationale for court rulings and legislation concerning privacy that is much less subjective and much more systematic than the rationales now in place. This is an audacious claim; however, it is one that is surprisingly easy to document, as shall be seen below.

THE CYBER AGE PRIVACY DOCTRINE "CUBE"



1. Low Volume, Low Sensitivity, No Cybernation: Tollbooths.

2. High Volume, Low Sensitivity, Low Cybernation: Collection of phone records.

3. Low Volume, Low Sensitivity, High Cybernation: Household purchases of specific, routine consumer goods.

4. Low Volume, High Sensitivity, Low Cybernation: Airport screening devices that reveal the body.

5. High Volume, Low Sensitivity, High Cybernation: Select cloud storage.

6. High Volume, High Sensitivity, Low Cybernation: Health records.

7. Low Volume, High Sensitivity, High Cybernation: Leaks of the names of CIA agents.

8. High Volume, High Sensitivity, High Cybernation: The sale of data brokers' "dossiers" to the government.

Select sub-cubes are next examined, to illustrate that application of the approach.

1. Low Volume, Low Sensitivity, No Cybernation

The CAPD holds that low volume, low sensitivity, non-cybernated personal information collection should be tolerated at the current level of common good because the risks to privacy are low, and the contributions to the common good engendered by such collection are very often middling to high. (By "tolerated," I mean that the law should allow such collection of information unless there are specific reasons to object to it; the default should be an *a priori* permission to proceed. In colloquial terms, one might say that "you do not have to love it to allow it.") Courts should allow the collection of such personal information, and Congress should pass laws along the same lines. Examples include tollbooths,[95] license plate readers,[96] police body cameras,[97]

---

[95] *See* Jay Stanley, *Christie Use of Tollbooth Data and Why Location Privacy Must Be Protected*, ACLU (Jan. 16, 2015), https://www.aclu.org/blog/technology-and-liberty-national-security/christie-use-tollbooth-data-and-why-location-privacy-m.

[96] *See* Michael Martinez, *ACLU Raises Privacy Concerns About Police Technology Tracking Drivers*, CNN (July 18, 2013, 9:10 AM), http://www.cnn.com/2013/07/17/us/aclu-license-plates-readers/.

[97] *See* Martin Austermuhle, *D.C. Police to Test Body Cameras, but Civil Libertarians Raise Concerns*, WAMU (Sept. 24, 2014), http://wamu.org/news/14/09/24/dc_police_officers_to_test_body_cameras.

airport screening gates,[98] breathalyzers,[99] general traffic stops,[100] random mandatory drug testing,[101] health and safety inspections, and many others. (Components of all these have been contested by civil libertarians.)

In many of these situations, as a rule, no cybernation takes place due to informal practices, the technological limitations of collection mechanisms, or lack of a motive for cybernation—not necessarily because cybernation is banned unless authorized by a judge. This at least used to be the case for many operators of tollbooths and speed cameras, who had no reason to keep the information, let alone combine it with other information or analyze it. However, typically the court rulings stemming from the prevailing privacy doctrine contain nothing to prevent secondary usages of such information.[102] That as a rule no cybernation takes place is either driven by custom or economic motives that are easily reversed if data brokers, the press, or even divorce lawyers seek access to the information. The CAPD points to the need to explicitly rule that points of collection should be required to erase information immediately after primary use or after a given period of time and should be banned from sharing it. An exception should be included for situations in which public authorities declare a state of emergency, such as after a terrorist attack, during the commission of a crime, or after a child has been kidnapped. Even during such a period of exception, sharing

---

[98] *See* Susan Stellin, *Airport Screening Concerns Civil Liberties Groups*, N.Y. TIMES (Mar. 11, 2013), http://www.nytimes.com/2013/03/12/business/passenger-screening-system-based-on-personal-data-raises-privacy-issues.html?pagewanted=all&_r=0.

[99] *See* Lauren C. Williams, *The Next Civil Liberties Fight Could Be over Breathalyzers*, THINKPROGRESS (Nov. 12, 2014, 11:43 AM), http://thinkprogress.org/justice/2014/11/12/3590539/breathalyzers/.

[100] For example, the ACLU has contended that traffic stops show a pattern of racial bias. *See* CPD TRAFFIC STOPS AND RESULTING SEARCHES IN 2013, ACLU OF ILL., (2014), *available at* http://www.aclu-il.org/wp-content/uploads/2014/12/Report-re-CPD-traffic-stops-in-2013.pdf.

[101] *See Workplace Drug Testing*, ACLU (Mar. 12, 2002), https://www.aclu.org/racial-justice_womens-rights/workplace-drug-testing.

[102] See for example: Alderman v. United States, 394 U.S. 165 (1969), which addressed electronic surveillance as a collection mechanism but did not comment on the government's right to share that information with others; Berger v. New York, 388 U.S. 41 (1967), which found New York's eavesdropping laws unconstitutional but never called into question the right of the government to share the information among law enforcement officials; Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls, 536 U.S. 822 (2002), which held that the school district's drug testing policy was constitutional, but not on the grounds that banning someone from playing a sport for a positive drug test in effect shares information about that person's drug use with a variety of others; and many more. All of the Fourth Amendment cases read by this author addressed the question whether an unreasonable search or seizure had occurred, and never asked about the appropriate scope of the government's subsequent use of legally-obtained information.

should be limited to the relevant public authorities. To reiterate, this is often already the *de facto* practice; however, for each category of information collection, it should be made law.

Before turning to the examination of a similar category—that of high volume, low sensitivity, and low cybernation collection—that requires distinct treatment, this article shall show that the CAPD provides a much more systematic rationale for cases of information collection than does the odd assortment of prevailing rationales employed by the courts to deal with the very same cases. The courts provide different rationales for different cases, which seem highly similar from the CAPD viewpoint because they all concern low volume, low sensitivity, non-cybernated information—and should therefore be allowed.

In *Schmerber v. California*, the court ruled that blood tests used to evaluate a suspect's blood-alcohol content are not an undue imposition on an individual's privacy per se; although the collection of a blood sample constitutes a Fourth Amendment search, there was justification for the police officer to arrest the defendant and collect a sample, on the grounds that "the test chosen to measure petitioner's blood-alcohol level . . . *involves virtually no risk, trauma or pain* . . . [and] was performed in a reasonable manner . . . by a physician in a hospital."[103] In *Kyllo*, the Court ruled that because the thermal imaging device used to survey the temperature in a private home was not yet in general public use, the use of that device without a warrant under the circumstances constituted an unreasonable search. In the Court's words, "Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a [Fourth Amendment] 'search' and is presumptively unreasonable without a warrant."[104] This represents yet another rationale and includes an undefined term—general public use—as pointed out by Justice Stevens' dissent, who stated:

> [T]he Court's new rule is at once too broad and too narrow, and it is not justified by the Court's explanation for its adoption . . . . [H]ow much use is general public use is not even hinted at by the Court's opinion, which makes the somewhat doubtful assumption that the thermal imager used in this case does not satisfy that criterion.[105]

In the opinion of this author, a great deal depends on the nature of the device. If it is able merely to establish the

---

[103] Schmerber v. California, 384 U.S. 757, 771 (1966) (emphasis added).
[104] Kyllo v. United States, 533 U.S. 27, 40 (2001).
[105] *Id.* at 46-47 (Stevens, J., dissenting).

temperature in select rooms of the house and thus determine whether it is abnormally high—which may indicate the presence of a marijuana "grow room"—the device's bandwidth is very narrow. By contrast, thermal imaging that produces detailed images of the interior of the house based on temperatures—showing where individuals are sitting, whether they are in bed, and so forth—would be considered to have a high bandwidth. The less invasive form of thermal imaging (the former) should be allowed; the more invasive one (the latter) should not.[106] There is no inherent reason to cybernate this information for the purposes of divining additional information about that individual if nothing incriminating is found.

Still another rationale was used by the Supreme Court in their ruling in *Florida v. Riley*,[107] which examined the question whether aerial surveillance from a helicopter constituted a violation of Riley's Fourth Amendment rights. The Court held that, because Riley had no reason to believe that his criminal activity was not visible from the air by a private citizen operating an aerial vehicle from a height of 400 feet, Riley had no reasonable expectation of privacy in this situation.[108] The height of 400 feet was selected because this was the height at which the police helicopter in the case flew over Riley's property; the Court ruled that it was entirely possible that "any member of the public" could have flown at that height over the property. It is at least implied that if a higher flying plane would have been used, Riley might have had a reasonable expectation of privacy.

Moreover, in the cyber age, one can violate privacy just as much or more in public spaces (e.g., by using parabolic microphones to eavesdrop on conversations in a public park) as one can do in the home (e.g., by using a thermal device or narcotics sniffing dogs to measure temperatures or detect the presence of controlled substances in a private residence). Although many sensors are being added daily to the home—such as smart thermostats, computers, security cameras, and smart televisions—the tapping of these sensors by the government becomes excessively intrusive on privacy only when the information collected either is inherently sensitive or is considered jointly, or cybernated. It is only from examining all of these streams of information that the government can

---

[106] Amitai Etzioni, *Eight Nails into* Katz*'s Coffin*, 65 CASE W. RES. L. REV. (forthcoming 2015), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2506312.

[107] Florida v. Riley, 488 U.S. 445 (1989).

[108] *Id.* at 451-52.

piece together a comprehensive picture of the activities of the individuals contained within. For this reason, the CAPD should be applied as if privacy were a bubble that surrounds a person and that is carried with her wherever she goes.[109] This idea is consistent with Justice Stewart's oft-cited assertion from *United States v. Katz* that "the Fourth Amendment protects people, not places."[110]

Moreover, the bubble should be extended to the digital person—that is to dossiers or profiles kept by the government. This deserves some elaboration. An individual in a remote ranch in Montana may be free from most physical surveillance by speed cameras, CCTVs, and other technologies. However, his communications and internet transactions could still be used to form an invasive profile of him. The CAPD therefore holds that the personal bubble, including personal information amassed by the government, should only be legally penetrated if law enforcement follows given procedures and is authorized by specified authorities, in line with the very communitarian Fourth Amendment—or if only low volumes of narrow-bandwidth information, low in sensitivity, are collected and subjected to low or no cybernation. *In other words, the CAPD should extend the right to privacy to the virtual person.*[111] The right to privacy should encompass both parts of the person: the virtual and the offline. (Calling the offline "real" disregards the increasing importance of the virtual part of life for more and more people.)

In *Jones*, the Court drew on two considerations. First, attaching the GPS to a car, considered a private space, amounted to trespassing.[112] CAPD would not accept this consideration for reasons previously indicated. Second, the Court opened the door to the CAPD by suggesting that the surveillance undertaken in *Jones* was too long.[113] However, given the very narrow bandwidth of information collected and its relatively low sensitivity, the CAPD would allow the surveillance at issue in *Jones* if cybernation was properly limited.

---

[109] For additional discussion of this concept, see Etzioni, *supra* note 1.

[110] Katz v. United States, 389 U.S. 347, 351 (1967).

[111] Technically, the term "virtual sub-person" would be more appropriate because the virtual parts of personhood are still part of the person. The agent that acts in cyberspace has one or more names of his or her own, a distinct locality and address, manners, and postures that are on the one hand distinct from those of the offline person but are also linked. Moreover, if the virtual person commits a crime, the whole person is judged and punished. If the virtual agent is exposed, the offline person is as well.

[112] United States v. Jones, 132 S. Ct. 945, 949 (2012).

[113] *Id.* at 964 (Alito, J., concurring).

In *Katz v. United States*, the Court used a still different rationale—by finding that Katz had a reasonable expectation of privacy in a public telephone booth. By contrast, the CAPD would hold that the police should be allowed to install surveillance equipment on telephone booths on the grounds that the amount of information collected is low, the bandwidth of the information collected is limited (and could be further curtailed by using the same minimization techniques used in wiretaps and other methods of intelligence collection), and the information collected is not of a sensitive nature. The CAPD would be more concerned if, even if Katz was found innocent, law enforcement were to keep and share a record that he was a suspect. The CAPD would therefore allow this kind of warrantless tapping only if proper accountability measures were in place to ensure this information is not shared inappropriately.

In *Florida v. Jardines*, the Court ruled that the use of a narcotics-sniffing dog to detect illegal drugs in a suspect's home was a search within the meaning of the Fourth Amendment because the dog was brought into the curtilage of the home—albeit only onto the porch.[114] The Court found that unlike a law enforcement official knocking on the door, the act of introducing a police dog into the area was different from the typical, expected actions of a private citizen and was therefore a search. In the majority opinion, Justice Scalia wrote:

> We have accordingly recognized that "the knocker on the front door is treated as an invitation or license to attempt an entry, justifying ingress by solicitors, hawkers and peddlers of all kinds." This implicit license typically permits the visitor to approach the home by the front path, knock promptly, wait briefly to be received, and then (absent invitation to linger longer) leave. Complying with the terms of that traditional invitation does not require fine-grained legal knowledge; it is generally managed without incident by the Nation's Girl Scouts and trick-or-treaters. Thus, a police officer not armed with a warrant may approach a home and knock, precisely because that is "no more than any private citizen might do."
>
> But introducing a trained police dog to explore the area around the home in the hopes of discovering incriminating evidence is something else. There is no customary invitation to do *that*.[115]

A court following the CAPD would arrive at the opposite conclusion, given that the information collected was of low volume and very narrow bandwidth. Concern with cybernation would be

---

[114] Florida v. Jardines, 133 S. Ct. 1409, 1415-16 (2013).

[115] *Id.* (internal citations omitted) (internal quotation marks omitted).

the same as with *Katz*. Once again it must be emphasized that the CAPD views the home as no more inherently private than the public sphere—or, more precisely, the CAPD seeks to protect information, not places. The premise of the CAPD is that sensitive information derives its status not from where it is revealed, but from the content contained in the revelation. A great many things that occur in the home may be sensitive, but this is not due to their occurrence in the home. Measuring the level of air pollution in a home would entail much less of a privacy violation than reading a person's emails, even if they were sent from a bench in a public park. Of course, the opposite may also take place; much more highly sensitive information could be collected from the home than from speed cameras. The key variables are the volume, the level of sensitivity, and the extent of cybernation—not where the information was first collected. Thus, while the Fourth Amendment refers to "persons, houses, papers, and effects"[116]—in the various cases cited above, and many others, it deals with private space, mainly the home and other spaces that like the home, have walls, such as containers and bags. The CAPD, which focuses strictly on the person, places greater emphasis on protecting what the Fourth Amendment lists.

United States v. White concerns the use of a government informant wearing a hidden microphone to record conversations.[117] The Court ruled that this act does not constitute a Fourth Amendment search, because the suspect has no reasonable expectation that the undercover informant will not pass along the information she receives to law enforcement.[118] A court following the principles of the CAPD would come to the same conclusion as long as the authorities set limits on the length or number of conversations recorded, no other modes of surveillance are used simultaneously, and cybernation of the resulting information is properly limited through accountability measures.

---

[116] U.S. CONST. amend. IV.

[117] United States v. White, 401 U.S. 745 (1971).

[118]

> Hoffa v. United States, 385 U.S. 293, 87 S. Ct. 408, 17 L.Ed.2d 374 (1966), which was left undisturbed by *Katz*, held that however strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected by the Fourth Amendment when it turns out that the colleague is a government agent regularly communicating with the authorities. In these circumstances, "no interest legitimately protected by the Fourth Amendment is involved," for that amendment affords no protection to "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."

Id. at 749 (internal quotation marks omitted).

The CAPD would also recognize a broad category of administrative and safety "searches" that collect a low amount of narrow bandwidth information but furnish critical contributions to a public good. Health inspections at restaurants fit into this category; the information collected by the health inspector is of low volume, with very few searches happening per year and specific types of information sought. The information collected is also of low sensitivity—indeed, most of it is not personal. Finally, there is little need to cybernate the information as long as the restaurant is in compliance with food safety laws; in the case of non-compliance, the information would only be cybernated with other health inspection information from the same restaurant to track progress. If kept for the purposes of public policy analysis, the information's identifying markers would be removed. This rationale seems more coherent, more systematic, and less subjective than the myriad diverse reasons given by the courts for authorizing administrative searches. Indeed, many legal scholars have bemoaned the complexity of administrative search jurisprudence in particular, calling it "incoherent," "abysmal," "devoid of content," a "conceptual and doctrinal embarrassment," and "chaotic at best."[119]

It is therefore clear that the criteria employed by the CAPD can be as readily operationalized as the criteria now used by the courts. It is similarly clear that the CAPD provides a much more systematic and less subjective set of criteria for distinguishing those intrusions that do not constitute a search under the Fourth Amendment.

2. High Volume, Low Sensitivity, Limited Cybernation

The collection of information about a person over longer periods of time and at a high bandwidth should be tolerated as long as the information is of limited sensitivity and cybernation is limited, in particular by strong accountability measures, because violations of privacy will be limited in these cases. This category includes the planting of beepers, tracking the location of cell phones, the long-term use of GPS tracking devices, and similar law enforcement projects. Again, it is useful to consider the similarities and differences between courts instructed by the

---

[119] Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 257 (2011); Russell L. Weaver, *Administrative Searches, Technology and Personal Privacy*, 22 WM. & MARY L. REV. 571, 571 (2013).

prevailing privacy doctrine and a court whose rationale stems from the CAPD.

Consider, for example, the case of *Smith v. Maryland*. In this case, the police, without a warrant, installed a pen register that recorded all of the numbers that connected to the phone of a robbery victim who had begun receiving calls from his attacker.[120] The Court ultimately ruled in this case that the suspect's expectation of privacy had not been violated on the grounds that the numbers he dialed had been passively received by the phone company, a third party.[121] In this case, a court applying the CAPD would reach the same ruling—albeit with a different rationale for doing so. Such a court would find that the information collected was of low sensitivity because it does not include the content of the calls.

Persistent Surveillance Systems sells to police departments in the United States a technology that can combine and analyze multiple public safety data streams instantaneously. It uses helicopters or small planes whose cameras scan large parts of a city continuously and feed the images into a command center.[122] The planes also carry infrared cameras that can track people and cars under foliage and in some buildings.[123] The information is kept and analyzed in the command center maintained by the company. *The Washington Post* reports that "[the company that sells the system] has rules on how long data can be kept, when images can be accessed and by whom. Police are supposed to begin looking at the pictures only after a crime has been reported. Fishing expeditions are prohibited."[124] The amount

---

[120] "[T]he telephone company, at police request, installed a pen register at its central offices to record the numbers dialed from the telephone at petitioner's home." Smith v. Maryland, 442 U.S. 735, 737 (1979). . . . "The activity here took the form of installing and using a pen register. Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner obviously cannot claim that his 'property' was invaded or that police intruded into a 'constitutionally protected area.'" *Id.* at 741.

[121]

> [P]etitioner's argument that its installation and use constituted a "search" necessarily rests upon a claim that he had a "legitimate expectation of privacy" regarding the numbers he dialed on his phone. This claim must be rejected. First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial.

Id. at 742.

[122] Craig Timberg, *New Surveillance Technology Can Track Everyone in an Area for Hours at a Time*, WASH. POST (Feb. 5, 2014), http://www.washingtonpost.com/business/technology/new-surveillance-technology-can-track-everyone-in-an-area-for-several-hours-at-a-time/2014/02/05/82f1556e-876f-11e3-a5bd-844629433ba3_story.html.

[123] *Id.*

[124] *Id.*

of information this technology collects, its bandwidth, and its cybernation are significantly higher than those of tollbooths, speed cameras, and other similar technologies included in the previous category. The information's sensitivity is, generally, relatively low. The main privacy effects of this technology concern the scope and kind of cybernation involved. If the company's self-imposed rules are codified in the law—and the law is effectively enforced—the privacy implications of this and other such technologies would be limited and tolerable. If these conditions are not met, the use of such technologies should be prohibited because their use amounts to subjecting all people all the time to fishing expeditions. The main variable that differentiates that which can be tolerated from that which should be banned is not collection but rather the level of cybernation. (To reiterate, this article focuses on the harms to privacy of various government acts rather than on their contributions to the common good. Both elements must be considered, per liberal communitarianism, but this article holds constant the contributions to the common good accomplished by a particular use of surveillance.)

An even more telling case is that of Microsoft's Domain Awareness System (DAS), a technology that "aggregates and analyzes existing public safety data streams" from cameras, license plate readers, radiation detectors, and law enforcement databases.[125] The technology helps police keep an eye on suspects by providing their arrest records, related 911 calls, and local crime data, as well as by tracking their vehicle's location.[126] DAS also makes it possible to tap into and rewind more than 3,000 CCTV camera feeds.[127] DAS may also be expanded in the future to gain access to many additional CCTV cameras as well as to encompass facial recognition, cell phone tracking technologies, and even social media scanners.[128] The data assembled is cybernated in order to identify particularly suspicious individuals, their contacts, and their *modi operandi*. Data are to be deleted within five years, but material deemed to have "continuing law enforcement or public

---

[125] Press Release, Mayor Bloomberg, Police Commissioner Kelly and Microsoft Unveil New, State-of-the-Art Law Enforcement Technology that Aggregates and Analyzes Existing Public Safety Data in Real Time to Provide a Comprehensive View of Potential Threats and Criminal Activity (Aug. 8, 2012), *available at* http://www.nyc.gov/portal/site/nycgov/menuitem.c0935b9a57bb4ef3daf2f1c701c789a0/index.jsp?pageID=mayor_press_release&catID=1194&doc_name=http%3A%2F%2Fwww.nyc.gov%2Fhtml%2Fom%2Fhtml%2F2012b%2Fpr291-12.html&cc=unused1978&rc=1194&ndi=1.

[126] *Id.*

[127] *Id.*

[128] Martin Kaste, *In 'Domain Awareness,' Detractors See Another NSA*, NPR (Feb. 21, 2014, 4:00 PM), http://www.npr.org/blogs/alltechconsidered/2014/02/21/280749781/in-domain-awareness-detractors-see-another-nsa.

safety value or legal necessity" may be retained indefinitely.[129] The New York Police Department has some accountability measures in place to limit access, with the "type of data each officer can view" being "tailored to their job duties,"[130] but it also shares "data and video with third parties not limited to law enforcement."[131] Oakland, CA, has already operationalized the first phase of a similar system,[132] and Baltimore, MD, and the United Kingdom already use similar technologies.[133]

The CAPD here alludes to the same conclusions drawn from the case of Persistent Surveillance Systems (PSS). The main difference between PSS' technology and DAS is that the amount and bandwidth of information collected by DAS is much higher. The question whether or not accountability measures sufficiently limit cybernation, by guaranteeing no fishing expeditions occur and information is not unduly shared or abused, is the critical variable to consider.

The NSA's collection of phone call metadata raises numerous complex issues that cannot be explored in passing in this article.[134] However, the ways the CAPD would approach the program are illustrative. First of all, much discussion by those who follow the prevailing privacy doctrines has focused on the question of collection and on suggestions that the government should cease to collect this information and instead should rely on phone companies to keep it. The CAPD would focus much more attention on the usages of the information. *If* it is true: that the NSA collects only metadata and refrains from collecting the content of calls; that it collects a large volume of information of very narrow bandwidth and relatively low sensitivity, akin to addresses on envelopes; that the NSA has to gain approval of a FISC judge in order to examine the records associated with any particular individual; and that FISC is indeed strict in granting such permissions only when there is a compelling case; then

---

[129] PUBLIC INTELLIGENCE, PUBLIC SECURITY PRIVACY GUIDELINES 4 (2009), *available at* https://info.publicintelligence.net/NYPD-DomainAwarenessSystem.pdf.

[130] Pervaiz Shallwani, *'Future' of NYPD: Keeping Tab(let)s on Crime Data*, WALL ST. J. (Mar. 4, 2014, 11: 52 PM), http://www.wsj.com/articles/SB10001424052702304815004579419482346315614.

[131] Neal Ungerleider, *NYPD, Microsoft Launch All-Seeing "Domain Awareness System" with Real-Time CCTV, License Plate Monitoring*, FAST COMPANY (Aug. 8, 2012, 12:07 PM), http://www.fastcompany.com/3000272/nypd-microsoft-launch-all-seeing-domain-awareness-system-real-time-cctv-license-plate-monito.

[132] Nadia Kayyali, *EFF Fights Back Against Oakland's Disturbing Domain Awareness Center*, ELECTRONIC FRONTIER FOUND. (Mar. 5, 2014), https://www.eff.org/deeplinks/2014/03/eff-fights-back-against-oaklands-disturbing-domain-awareness-center.

[133] Ungerleider, *supra* note 131.

[134] For more on this subject, see Amitai Etzioni, *NSA: National Security vs. Individual Rights*, 30 INTELLIGENCE & NAT'L SEC. 100 (2015).

cybernation is well-limited and the program seems to pass muster. If one or more of these suppositions are not valid, it becomes much more difficult to justify the program given the United States' current security needs. To reiterate, the goal here is *not* to evaluate the program but rather to call attention to the key variable that should be employed in judging it—the extent of cybernation, which includes an assessment of the level of accountability that is in place.

3. High Volume, Low Sensitivity, High Cybernation

The courts, in accordance with their focus on primary collection rather than on secondary usages, have allowed surprisingly high quantities of wide bandwidth, highly sensitive, highly cybernated personal information to be collected by law enforcement. Once again, the discussion that follows assumes a constant level of threat to the public good and holds constant the benefits of surveillance programs.

The increasing use of drones by public authorities (privacy violations by private actors are beyond the subject of this article[135]) raises still more complex issues. On the one hand, drones are mainly engaged in primary collection. From this viewpoint, if one draws on Justice Alito's concern in *Jones*, the use of drones would constitute a search in Fourth Amendment terms because they collect large quantities of information. The CAPD would add that drones provide information that is of a much broader bandwidth than the information provided by a GPS. At the same time, drones are often used for purposes such as finding lost children or skiers or delivering help to stranded victims of earthquakes and floods—all acts for which one might hold that there is presumed consent by those involved. What about their deployment for routine police surveillance? This issue is now being sorted out by regulatory agencies and the courts.

In one case, in which they ruled wiretaps constitutional, the court neglected to comment on the use of drones.[136] The case concerned a group of far-right extremists known as the Montana Freemen that issued in 1995 a "citizens declaration of war"[137] against the United States government, occupied a 960-acre

---

[135] *See generally* Etzioni, *supra* note 28; *see also* JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE (2014).

[136] *See* United States v. McGuire, 307 F. 3d. 1192, 1197 (9th Cir. 2002).

[137] Ann LoLordo, *'Freemen' Wage War Against Authority in Montana*, BALTIMORE SUN (July 31, 1995), http://articles.baltimoresun.com/1995-07-31/news/1995212003_1_freemen-skurdal-musselshell-county/2.

ranch in Montana following foreclosure, and initiated an armed standoff with law enforcement.[138] The resulting case, *United States v. McGuire*,[139] held in part that federal agents had not violated the Freemen's right to freedom from unreasonable searches and seizures. The Freemen claimed that the government's use of judicially-approved "phone and fax wiretapping on Freemen properties, and . . . a microphone on the premises to record conversations" were in violation of the Fourth Amendment because they allegedly exceeded the limits of authorized government action outlined by the relevant portions of the Omnibus Crime Control and Safe Streets Act of 1968.[140] However, the Supreme Court held that:

> *FBI agents could not have conducted on-site surveillance of the Freemen property because of its remote, rural location and group members' alertness to law enforcement activities, which created grave dangers.* Agents also would have faced risks in executing any search warrant at the compound, because of the group's known violent propensity and undisputed possession of assault weapons. Federal agents would have had difficulty infiltrating the group with FBI informants . . . [and] interviewing witnesses would have helped little.[141]

Because direct surveillance posed a danger to the agents working on the case, and there were no alternative reasonable options available to the agents, the Court ruled a number of search techniques constitutional under the circumstances, namely electronic surveillance. (The agents also used aerial surveillance to monitor the ranch, and the issue was not raised in court.[142]) (The Court also held that the FBI had met the Act's requirement to use reasonable minimization procedures when conducting wiretaps, that it had indeed taken reasonable steps to "eliminate irrelevant information," and that any delays in sealing the information in accordance with federal law had a reasonable explanation.[143] For these reasons, the Court denied the claim that the FBI had acted improperly.) The CAPD would reach the same conclusion, but a court following the CAPD would hold that given the high amount and considerable bandwidth of the

---

[138] Leonard Zeskind, *Montana Freemen Trial May Mark End of an Era*, 90 S. POVERTY L. CENTER INTELLIGENCE REP. 9 (1998), *available at* http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/1998/spring/justice-vs-justus.

[139] *McGuire*, 307 F. 3d. at 1195.

[140] *Id.* at 1195-96.

[141] *Id.* at 1197 (emphasis added).

[142] Tom Kenworthy, *Freemen Surrender Ends 81-Day Siege, All 16 Give Themselves Up Peacefully to FBI*, SPOKESMAN-REV. (June 14, 1996), http://m.spokesman.com/stories/1996/jun/14/freemen-surrender-ends-81-day-siege-all-16-give/.

[143] *McGuire*, 307 F.3d at 1202.

information collected, even of low sensitivity, drones should be allowed only if cybernation is limited.

4. High Volume, High Sensitivity, Must Limit Cybernation

According to the CAPD, highly sensitive information should be collected only if there is a compelling public interest in doing so. Here, too, the main issue is limiting cybernation rather than collection. The Social Security Administration, Medicare, Medicaid, and the IRS all hold considerable amounts of sensitive personal information on the United States' 300 million (mostly) innocent citizens. That their databases have been very rarely abused and the harm caused by violations has been limited, however, shows that a considerable level of collection and cybernation of sensitive information can be tolerated when accountability is very high.[144]

The same cannot be said about the databases kept by the FBI,[145] or state and local government agencies[146] and accessed by

---

[144] *See, e.g.*, G.W. Schulz, *Bureaucrats Can't Resist Celebrity Snooping in Government Databases*, THE CTR. FOR INVESTIGATIVE REPORTING (Oct. 13, 2010), http://cironline.org/blog/post/bureaucrats-cant-resist-celebrity-snooping-government-databases-821; *Chronology of Data Breaches: Security Breaches 2005–Present*, PRIVACY RIGHTS CLEARINGHOUSE (Dec. 31, 2013), http://www.privacyrights.org/data-breach; Michael Cooney, *How to Get the IRS' Attention: Forge Nearly $8 Million in Tax Returns, Steal Identities*, NETWORK WORLD (Feb. 10, 2012, 11:16 AM) http://www.networkworld.com/article/2186572/malware-cybercrime/how-to-get-the-irs--attention--forge-nearly--8-million-in-tax-returns--steal-iden.html; *IRS Employee Charged with Illegally Accessing Celebrity Tax Records*, ACCT. WEB (June 4, 2008), http://www.accountingweb.com/topic/tax/irs-employee-charged-illegally-accessing-celebrity-tax-records; Levi Pulkkinen, *IRS Worker Caught Snooping on Ex, Others*, SEATTLE PI (Apr. 23, 2012, 9:44 PM), http://www.seattlepi.com/local/article/IRS-worker-caught-snooping-on-ex-others-3498550.php; Andrea Coombes, *IRS Employee Sentenced for Snooping*, MARKETWATCH (Aug. 20, 2008, 7:40 PM) http://www.marketwatch.com/story/irs-worker-snooped-on-tax-records-of-almost-200-celebrities; Stephen Barr, *IRS Still Has Tax Snoops: Workers Fired, Disciplined for Peeking at Friends', Celebrities' Records*, SEATTLE TIMES (Apr. 9, 1997, 12:00 AM), http://community.seattletimes.nwsource.com/archive/?date=19970409&slug=2533005; Mark Ballard, *List of Councils Whose Staff Illegally Accessed DWP Data*, COMPUTER WEEKLY (July 21, 2009, 1:00 AM), http://www.computerweekly.com/news/1280090284/List-of-councils-whose-staff-illegally-accessed-DWP-data; Jim Geraghty, *The 'Very Serious' Tradition of the Internal Revenue Service*, NAT'L REV. (June 13, 2013, 4:00 AM) http://www.nationalreview.com/article/350906/very-serious-tradition-internal-revenue-service-jim-geraghty'.

[145] Tom Hays, *NYC Cases Show Crooked Cops' Abuse of FBI Database*, YAHOO FINANCE (July 7, 2013, 12:21 PM), http://finance.yahoo.com/news/nyc-cases-show-crooked-cops-abuse-fbi-database-162152158.html.

[146] Press Release, U.S. Attorney's Office, Private Investigator and Former NYPD Officer Arrested in Bribery Scheme to Obtain Reports from Federal Law Enforcement Databases, (Oct. 22, 2014), *available at* http://www.fbi.gov/newyork/press-releases/2014/private-investigator-and-former-nypd-officer-arrested-in-bribery-scheme-to-obtain-reports-from-federal-law-enforcement-database; Amy Pavuk, *Law-Enforcer Misuse of Driver Database Soars*, ORLANDO SENTINEL (Jan. 22, 2013),

the Department of Homeland Security.[147] These all have been abused, as revealed by the Church and Pike Committees and various leaks to the media. Some consequently argue that these collections should be greatly curtailed, if not abolished entirely. Civil libertarians have often objected to the details (or even the very existence) of such databases, including the Terrorist Screening Database—which includes the "No Fly List"[148]—and the federal DNA profile database, NDIS.[149] Although the rationales for these objections differ, they often reflect—aside from specific concerns, such as the belief that DNA profiles are particularly sensitive information—a sense that the government cannot be trusted. Even if the *current* government is trustworthy, many civil libertarians say, future governments will abuse the databases, and it is therefore best if no collection or storage occurs.

Discussion of the CAPD has so far focused on one of the two core elements of a liberal communitarian approach—rights, in particular the right to privacy—and has held constant the other element: the common good. This is necessary because a society that faces higher demands for the common good in the face of an epidemic or some other threat may well permit greater intrusions on individual liberties than a society that faces lower or declining demands for the common good. However, it must be noted in closing that the analysis is incomplete without accounting for the contributions to the common good called for in a given society at a particular moment in history. To stay with the present example, given that many crimes in the United States remain unsolved and that DNA databases help to close a growing number of such cases, DNA databases should be maintained or expanded with the caveat that accountability measures should be improved. Numerous suggestions to this effect have been made

---

http://articles.orlandosentinel.com/2013-01-22/news/os-law-enforcement-access-databases-20130119_1_law-enforcement-officers-law-enforcers-misuse.

147 "As part of the [Pretrial Diversion] agreement, Camaj admitted to having conducted 314 queries [of the Treasury Enforcement Communication System] while knowing that those queries were unauthorized." Camaj v. Dep't of Homeland Sec., No. 2013-3060, slip op. at 2 (Fed. Cir. Oct. 16, 2013), *available at* https://cases.justia.com/federal/appellate-courts/cafc/13-3060/13-3060-2013-10-16.pdf.

148 *See* ACLU, U.S. GOVERNMENT WATCHLISTING: UNFAIR PROCESS AND DEVASTATING CONSEQUENCES (2014), available at https://www.aclu.org/sites/default/files/assets/watchlist_briefing_paper_v3.pdf. The ACLU's writings on and advocacy against the "No Fly List" are available at https://www.aclu.org/blog/tag/no-fly-list.

149 *See, e.g.*, TANIA SIMONCELLI & SHELDON KRIMSKY, AM. CONST. SOC'Y FOR L. & POL'Y, A NEW ERA OF DNA COLLECTIONS: AT WHAT COST TO CIVIL LIBERTIES? (2007), *available at* http://www.acslaw.org/sites/default/files/Simoncelli__Krimsky_-_DNA_Collection__Civil_Liberties.pdf.

and need not be explored here.[150] (That accountability can be effectively operationalized has already been demonstrated.)

Some have expressed fear that a future government might remove such protective measures and abuse the information held in databases. The greatest threats to democracy, however, have historically arisen not from abuses of databases but from fearful populations that sought stronger authorities because the existing ones did not adequately protect them from violent crime, civil war, and external enemies. Russians suffering from a breakdown of law and order welcomed Putin. In Russia between 1989 and 1993 the total crime rate increased by 73%, or 1,180,000 reports.[151] The homicide and attempted homicide rate rose from 9.2 per 100,000 inhabitants to 19.6 per 100,000 inhabitants in the same timeframe.[152] Indicative of how shredded the social fabric had become, in 63% of major criminal injuries the victims were relatives or friends of the offenders. Russia's suicide rate increased 60% from 1989 to 2000.[153] There were also sharp increases in highway accidents, weapons and currency smuggling, and robberies. In Egypt, the citizens restored a military regime. Post-Mubarak, violent interpersonal attacks increased, as did inter-group violence, and a complete breakdown of civil order occurred as the police in more than one-third of Egyptian provinces walked off the job in 2013.[154] Many Iraqis increasingly yearn for stronger, more authoritarian leadership. New Yorkers and Angelenos, suffering from high rates of violent crime in the 1980s, supported police departments that made short order of individual rights, as well as the commissioners and mayors that adopted such initiatives. In the mid-1990s, the public cited crime as the biggest problem facing the country (19%), with an additional 2% identifying guns as the biggest problem.[155] In 1996, 54% of American adults said drug and alcohol abuse were getting worse, and 53% said the same of "robberies, shootings, and other kinds of

---

[150] *See, e.g.*, Amitai Etzioni, *Give the Spies a Civilian Review Board*, HUFFINGTON POST (May 25, 2011, 11:50 AM), http://www.huffingtonpost.com/amitai-etzioni/give-the-spies-a-civilian_b_14793.html.

[151] Ilya V. Nikiforov, *Russia*, *in* WORLD FACTBOOK OF CRIMINAL JUSTICE SYSTEMS (1993), *available at* http://www.bjs.gov/content/pub/pdf/wfbcjsru.pdf.

[152] COUNCIL OF EUROPE, EUROPE IN A TIME OF CHANGE: CRIME POLICY AND CRIMINAL LAW 97(1999).

[153] *Facts & Stats of the Yeltsin Era*, PBS FRONTLINE, *available at* http://www.pbs.org/wgbh/pages/frontline/shows/yeltsin/etc/facts.html (last visited Mar. 8, 2015).

[154] Patrick Kingsley, *Egyptian Police Go on Strike*, GUARDIAN (Mar. 10, 2013, 3:41 PM), http://www.theguardian.com/world/2013/mar/10/egypt-police-strike.

[155] Richard L. Berke, *Crime Is Becoming Nation's Top Fear*, N.Y. TIMES (Jan. 23, 1994), http://www.nytimes.com/1994/01/23/us/crime-is-becoming-nation-s-top-fear.html.

violent crime."[156] After 9/11, a majority of Americans favored adopting more limited interpretations of the Constitution in order to protect the nation from further attacks.[157]

All this suggests that a doctrine concerned with protecting privacy should allow for sufficient security—and other public goods, such as public health in the face of a pandemic—and should permit the collection and cybernation of the data necessary to do so, so long as the usages of this data are properly supervised and curbed. Prohibiting all collection is not the answer. Concerns about government abuse are best addressed not by ceasing collection and storage, but by building up the foundations of civil society, public education, and voluntary associations, and by ensuring that public goods are provided.

C. Key Considerations

It is necessary to outline a few major considerations that underlie the endeavor. First, during a discussion of the original paper, several colleagues asked whether the suggested doctrine is a proposed means of interpreting the Constitution or a framework for passing legislation and formulating public policy. After all, as these legal scholars pointed out, a world of difference exists between the former, which deals with the courts, existing case law, and the ways in which judges deliberate; and the latter, which involves the democratic processes of the legislature.[158]

While there are indeed significant differences between these two institutions, the CAPD is an articulation of normative principles that apply to and affect both. That changes to normative precepts affect both institutions is highlighted by developments in other arenas. In the wake of changes to the United States' moral culture precipitated by the Civil Rights Movement, the Supreme Court overturned *Plessy v. Ferguson* in the landmark case *Brown v. Board of Education*, and Congress passed the Voting Rights Act of 1965. Recent changes to the moral culture, in which libertarian principles led some to take similar positions to those held by liberals regarding same-gender marriage, have led to court cases, most notably *United States v.*

---

[156] HINDELANG CRIM. JUST. RES. CTR., SOURCEBOOK OF CRIMINAL JUSTICE STATISTICS-1995 130 tbl. 2.5 (1996).

[157] AMITAI ETZIONI, HOW PATRIOTIC IS THE PATRIOT ACT?: FREEDOM VERSUS SECURITY IN THE AGE OF TERRORISM 5 (2004).

[158] Peter P. Swire, Katz *is Dead. Long Live* Katz, 102 MICH. L. REV. 904, 913 (2004).

Windsor,[159] in which the Court ruled that interpreting the words "marriage" and "spouse" to apply only to heterosexual couples violates the Due Process Clause. There have similarly been gains for same-gender-marriage in state legislatures. Furthermore, the same moral shift has led to changes to federal administrative rules regarding the extension of the tax and other benefits of marriage to same-gender couples. A similar sea change must now take place with respect to the normative conceptualizations of privacy and its application by the courts and legislatures. Several preliminary steps in this transformation are outlined below.

Second, this article has assumed the current state of the common good in the United States will continue—that is, there will be declining or relatively low rates of violent crime, no new major terrorist attacks on the United States homeland, no pandemics, and no other significant new challenges to the common good. Otherwise, for reasons already mentioned, the equilibrium between the common good and privacy may have to be established at a different point than indicated below.

Third, an important thesis underlying this article is that as a privacy doctrine is adapted to the grand transformation of information from the paper age to the cyber age, society can become more tolerant of spot collection of personal information if at the same time it becomes more restrictive of secondary usages—that is, if it restricts cybernation of the information collected—without suffering a net increase in privacy violations. This is true of all circumstances except for limited conditions, such as the arrival of a tyrant. There is an inverse relationship between the two elements: the less cybernation, the more primary collection is possible without causing an increase in privacy violations. The more cybernation is allowed, the less collection can be tolerated if the demands of the common good do not call for a net increase in intrusions.[160]

Fourth, the challenge my colleagues posed when asking me to specify the new doctrine is completely justified, indeed essential, if the courts and legislatures are to apply this doctrine. However, the law often functions without taking definitions to the third decimal point and by leaving much interpretation to the discretion of law enforcement authorities, lower courts, and regulators. For example, in cases of drunk driving, the moment a suspect has actually been taken into custody and must be read

---

[159] United States v. Windsor, 133 S. Ct. 2675, 2714 (2013).

[160] For a concept of harm, see *Reinventing Privacy Principles for the Big Data Age*, *supra* note 6.

her Miranda rights seems to remain unclear.[161] The Bill of Rights defines the right of a United States citizen to be tried by an "impartial" jury rather than merely a judge in criminal cases; however, the definition of "impartial" is far from specified.[162] These examples illustrate that the courts function more or less effectively without excessive precision. In short, specification is essential, but the law functions quite well without carrying it to the level demanded by the sciences. This is particularly the case given that, to reiterate, only a first approximation of the new doctrine is here attempted.

CONCLUSION

The prevailing privacy doctrines (of which this article has discussed two) reflect concepts suitable to the paper age, in which the main issue was whether primary collection of information unduly intruded on individuals' privacy. Such intrusions required court authorization in line with the Fourth Amendment. This article argues that since the advent of the cyber age many more risks to privacy emanate from the secondary usages of personal information—regardless of how it is collected. No prevailing privacy doctrine of which I am aware addresses this pressing issue.[163] Moreover, the notions of a "reasonable expectation of privacy" and affording special status to the home are obsolescent.

The CAPD would take into account the risks to privacy posed by the collection of high volumes of information of high sensitivity, paying particular attention to the extent to which the information is cybernated—processed, analyzed, and shared. The CAPD would also consider the degree to which various accountability mechanisms impose limitations on cybernation.

This analysis has focused exclusively on one of the two core elements of a liberal communitarian philosophy—namely, the effects on the right to privacy, holding constant the contributions to the common good. Several illustrations have been provided to

---

[161] Berkemer v. McCarty, 468 U.S. 420 (1984). Although the Supreme Court granted certiorari to a case of drunk driving that sought to clarify this distinction, the Court ruled that until the suspect is actually placed under arrest and into a police vehicle the question of whether she is in custody is a function of the extent to which the circumstances of the stop mimic the restraints and stresses of actual arrest. *Id.*

[162] In common law, "impartial" was understood to mean having a lack of familial ties to or financial interest in the outcome of a case; however, today people often interpret "impartial" to mean that jurors know nothing of the case at hand other than the facts presented at trial. Caren Myers Morrison, *Jury 2.0*, 62 HASTINGS L. J. 1579, 1619 (2011).

[163] The "equilibrium-adjustment theory" proposed by Orin Kerr does, however, provide an interesting perspective. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 478 (2011).

demonstrate that such an analysis can be operationalized and that the CAPD provides a much less subjective and more systematic rationale for the courts and legislatures to consider when creating law than the rationale presently available. Such a doctrine would form part of a long-overdue refinement to the concept of privacy, allowing it to stay relevant in the cyber age.

How should the judicial and legislative branches proceed? Part of what must be done is the job of Congress. In particular, the legislature ought to examine the myriad and diverse laws that define some kinds of personal information as more sensitive than others. It should determine if the rankings pursuant to the CAPD need to be updated, and it should identify and rank types of information that remain undefined; for instance, are records of a person's reading habits sensitive information that should be entitled to special protections? The rest is up to the courts. Here, a lawyer might point to Alito's concurrence in *Jones* as a starting point.

The most difficult challenge facing the courts and Congress concerns cybernation, first because the courts focused for so long on primary collection and not on secondary usages, and second because of the possibility of "split decisions" that would allow the collection of certain kind of information (e.g., phone records) but limit secondary usages of that information. The courts will have to do what it did with decisional privacy and read between the lines of the Constitution to divine a basis for the much-needed CAPD.