Preliminary Draft – Please Do Not Cite Without Permission
To be Published in *I/S: A Journal of Law and Policy for the Information Society*
9 ISJLP ___ (2014).
http://www.is-journal.org

A Cyber Age Privacy Doctrine: A Liberal Communitarian Approach[1]

Amitai Etzioni

A privacy doctrine built for the cyber age must address a radical change in the type and scale of violations that the nation—and the world—face, namely that the greatest threats to privacy come not at the point that personal information is collected, but rather from the secondary uses of such information. Often cited court cases, such as *Katz*, *Berger*, *Smith*, *Karo*, *Knotts*, *Kyllo*—and most recently *Jones*—concern whether or not the initial collection of information was legal. They do not address the fact that personal information that was legally obtained may nevertheless be used later to violate privacy. That the ways such information is stored, collated with other pieces of information, analyzed, and distributed or accessed—often entails very significant violations of privacy.[2] While a considerable number of laws and court cases cover these secondary usages of information, they do not come together to make a coherent doctrine of privacy—and most assuredly not one that addresses the unique challenges of the cyber age.[3]

---

[1] I am indebted to Ashley McKinless for extensive research assistance on this article, and to Alex Platt, Steven Bellovin, and Shaun Spencer for comments on a previous draft.

[2] Amitai Etzioni, *The Privacy Merchants: What Is To Be Done?*, 14 PENN. J. CONST. L. 929 (March 2012).

[3] Peter P. Swire, *Katz is Dead. Long Live Katz*, 102 MICH. L. REV. 904, 912 (2002) ("The increasing storage of telephone calls is part of the much broader expansion since 1967 of stored records in the hands of third parties. Although there are no Supreme Court cases on most of these categories of stored records, the Miller and Smith line

True, collected personal information was subject to secondary abuses even when it was largely paperbound (e.g., in police blotters or FBI files). Indeed, when Warren and Brandeis published their groundbreaking 1890 article in the Harvard Law Review, considered the "genesis of the right of privacy," they were not concerned about gossip per se (a first order privacy violation) but about the wider distribution of intimate details through the media (a secondary violation).[4] However, the digitization of information, the widespread use of the Internet and computers, and the introduction of artificial intelligence systems to analyze vast amounts of data have increased the extent, volume, scope, and kinds of secondary usages by so many orders of magnitude that it is difficult to find a proper expression to capture the import of this transformation.[5] The main point is not that information can now be processed at a tiny fraction of the cost and incomparably faster speeds than when it was paper bound, which is certainly the case, but that modes of analysis—which divine new personal information out of personal data previously collected—that are common today were simply inconceivable when most personal information was paper bound.[6] Because this observation is critical

---

of cases make it quite possible that the government can take all of these records without navigating Fourth Amendment protections.").

[4] Samuel D. Warren and Louis D. Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193 (1890).

[5] For an excellent overview of how advances in information and communication technologies have rendered obsolete the privacy laws (and the doctrines on which these laws are based) of the 1980s and 1990s, see Omer Tene, *Privacy: The new generations*, 1 INTERNATIONAL DATA PRIVACY LAW 15 (2011). For a discussion of how these changes have particularly affected the privacy expectations of the 'Facebook generation,' see Mary Graw Leary, *Reasonable Expectations of Privacy for Youth in a Digital Age*, 80 MISS. L. J. 1033 (2011).

[6] This is of course not a terribly new position—legal scholars have been discussing the implications for privacy and the Fourth Amendment of the Internet since its introduction as publically available technology. *See* LAWRENCE

to all that follows, and because the term "secondary usages" (which implies usages less important that the first or primary ones) is a rather weak one, I employ from here on the infelicitous term "cybernated information" (or cybernation) to refer to information that is digitized, stored, processed, and formatted for mass distribution. Cybernated data can be employed in two distinct ways and both represent a serious and growing threat to privacy. A discrete piece of personal information, collected a one point in time ("spot" information) may be used for some purpose other than what it was originally approved for, or spot information may be pieced together with other data to generate new information about the person's most inner and intimate life.

The cyber age privacy doctrine must lay down the foundations on which Congress can develop laws and the courts can accumulate cases that will determine not merely what information the government may legally collect—but what it might do with that data. According to some legal scholars, the D.C. Circuit's decision in *Maynard* and the concurring opinion by the Supreme Court's justices in *Jones* provide the building blocks for this new edifice, sometimes referred to as a mosaic theory of the Fourth Amendment, under which "individual actions of law enforcement that are not searches for Fourth Amendment purposes may become

---

LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 222-23 (1999) and Laurence H. Tribe, The Constitution in Cyberspace, Keynote Address at the First Conference on Computers, Freedom, & Privacy (March 26, 1991) (transcript available at www.sjgames.com/SS/tribe.html).

searches when taken together en masse."[7] This observation is based Justice Alito's argument that the GPS tracking of a vehicle on a public highway constituted a search because of the length of time over which the monitoring took place (28 days). This opens the door to take into account the volume of information collected, and presumes that, while limited amounts collection may be permissible, large amounts could constitute a violation of privacy. *Jones*, however, still only deals with collection. Hence, most of the work of laying down the foundations for the protection of privacy from cybernated information remains to be carried out.

The article first suggests that we cannot rely on the privacy expectations of individuals or society—principles introduced in *Katz*—in developing a new privacy doctrine for the cyber age (Part I, a). The article then briefly indicates that a return to the home as the major focus of privacy will not serve either, and we are to consider privacy as a protective sphere that follows the individual regardless of place (Part I, b). The article then introduces a "social policy model" of the Fourth Amendment to move us forward.[8] Within this model, we shall see that defining what is minimally intrusive becomes a key issue; instead of treating intrusiveness

---

[7] Erin Smith Dennis, *A Mosaic Shield: Maynard, the Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737 (2012). *See also* Orin Kerr, *The Mosaic Theory of the Fourth Amendment,* 111 MICH. L. REV. 311, 320 (2012) ("Under mosaic theory, searches can be defined collectively as a sequence of discrete steps rather than as individualized steps. Identifying Fourth Amendment search requires analyzing police actions over time as a collective 'mosaic' of surveillance."); Madelaine Virgina Ford, *Mosaic Theory and the Fourth Amendment: How Jones Can Save Privacy in the Face of Evolving Technology*, 19 AM. U. J. GENDER SOC. POL'Y & L. 1351 (2011); Bethany L. Dickman, *Untying Knotts: The Application of Mosaic Theory to GPS Surveillance in United States v. Maryland* 60 AM. U. L. REV. 731 (2011).

[8] Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 519 (2007).

as a discreet variable, however, we find it must be treated as a continuous one. That is, the intrusiveness of an act may be considered higher or lower, rather than either minimal or not (Part I, c).

Once it has cleared the way through these deliberations, the article will outline the three dimensions of a cyber age privacy cube: volume, sensitivity, and cybernation (Part II). The last section of paper deals with the issue of defining when the collection and cybernation of information along these dimensions violates privacy (Section III).

Part I. Assumptions

a. Moving Beyond *Katz*

Since 1967, the U.S. legal system has drawn on the twin concepts of personal and societal expectations of privacy to determine whether a Fourth Amendment 'search' has taken place. This article assumes that relying on the expectation of privacy (personal and societal), as articulated by Justin Harlan in his concurring opinion in *Katz*, is indefensible and that it should be allowed to fade from legal practice. Indeed, Justice Harlan himself adopted rather quickly a critical view of his two-pronged test. Four years after *Katz*, in his dissent for *U.S. v. White*, Harlan wrote that "While these formulations represent an advance over the unsophisticated trespass analysis of the common law, they too have their

limitations and can, ultimately, lead to the substitution of words for analysis. The analysis must, in my view, transcend the search for subjective expectations."[9]

The reasonable expectation of privacy standard has since faced a range of strong criticism.[10] In his widely-cited article on the Fourth Amendment, Anthony G. Amsterdam writes,

> "An actual, subjective expectation of privacy obviously has no place in a statement of what Katz held or in a theory of what the fourth amendment protects. It can neither add to, nor can its absence detract from, an individual's claim to fourth amendment protection. If it could, the government could diminish each person's subjective expectations of privacy merely by announcing half-hourly on television that 1984 was being advanced by a decade and that we were all forthwith being placed under comprehensive electronic surveillance…Fortunately, neither Katz nor the fourth amendment asks what we expect of government. They tell us what we should demand of government."[11]

One leading scholar of the Fourth Amendment and privacy, Orin Kerr, concedes "What counts as a 'reasonable expectation of privacy' is very much up for grabs,"[12] while Charles Whitebread and Christopher Slobogin charge that the Supreme Court has sent "mixed signals" on how to apply this standard.[13]

---

[9] U.S. v. White, 401 U.S. 745 (1971)

[10] Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843 (2002); Jim Harper, *Reforming the Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 5 (2008); Haley Plourde-Cole, *Back to Katz: Reasonable Expectation of Privacy in the Facebook Age,* FORDHAM URB. L. J. (2010); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at Understandings Recognized and Permitted by Society*, 42 DUKE L.J. 727 (1993); Richard G. Wilkins, *Defining The 'Reasonable Expectation Of Privacy': An Emerging Tripartite Analysis*, 40 Vand. L. Rev. 1077, 1108 (1987); Sherry F. Colb, *What Is A Search? Two Conceptual Flaws In Fourth Amendment Doctrine And Some Hints Of A Remedy*, 55 Stan. L. Rev. 119, 122 (2002); Silas Wasserstom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 Geo. L.J. 19 (1988).

[11] Anthony G. Amsterdam, Perspectives on the Fourth Amendment, 58 MINN. L. REV. 349, 383 (1974).

[12] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 808 (2004).

[13] Charles H. Whitebread & Christopher Slobogin, Criminal Procedure: An Analysis of Cases and Concepts,

The absurdity of *Katz* is revealed by contemplating the following example: Assume a municipal government announces that, for public health reasons, anyone who relieves themselves in a public pool would be charged with a misdemeanor. This government would then insert a dye (which unfortunately only exists in Hollywood's fertile imagination) that would form a dark blue cloud around anyone who violates the ordinance, but would not announce the introduction of this dye. By *Katz*, surely a person could argue that his expectation of privacy has been grossly violated, as he did not expect to be detected peeing in the pool. Would it be reasonable, therefore, to dismiss the charges against him and to rule the ordinance unconstitutional? And once the introduction of the dye is made public—how many people would have to know about it before it is no longer reasonable to expect privacy in the matter? And as determined by whom and how? Would one announcement about the new dye suffice, or must it be regularly advertised?

Or, take those who speak in a sizeable political meeting. They may well have no expectation of privacy. However, surely they should be protected from government surveillance in such a setting under most circumstances, to protect their privacy (among other reasons).[14] And do new technologies change what is

---

§ 4.03(f) at 116 (3d ed.1993).

[14] Further, what is considered a reasonable expectation is in constant flux due to technological changes. Thus, as the use of the Internet for personal communications grew, the Electronic Communications Privacy Act of 1986 failed protect stored private emails because it was passed in a time when most emails were related to business records, which are expected to be afforded a lesser degree of privacy. *See* Deirdre L. Mulligan Deirdre L. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004).

expected, with, say, Facebook lowering the standards of privacy because so many people post so much private information? ECPA only protects emails for 90 days, during which time a warrant is needed for the government to read them. After that, a subpoena from any prosecutor will do, without judicial oversight, because in 1986 the thought of keeping emails around that long was ridiculous because the cost of storing them was so high.

As to the societal expectation of privacy, a sociologist is keen to know which, if any, communities will be polled to establish what this expectation is. The community of which the defendant is a member? Say Spanish Harlem? Or the city of New York? The American community? Or—the judge's country club? The fact that judges are free to assume they can rely on their sociological instincts as to what the community expects seems a strange foundation to rely on to determine when a search violates the Constitution.[15]

Finally, sociologists would be quick to agree that the whole notion is circular. Mr. Katz—and all others—either has or does not have an expectation of privacy *depending on what the court rules*. Jim Harper put it well when he wrote:

[15] ROBERT M. BLOOM, SEARCHES, SEIZURES, AND WARRANTS 46 (2003) ("Because there is no straightforward answer to this question, 'reasonable' has largely come to mean what a majority of the Supreme Court Justices say is reasonable.")

"Societal expectations are guided by judicial rulings, which are supposedly guided by societal expectations, which in turn are guided by judicial rulings, and so on."[16]

Four years after the Supreme Court ruled that the police had violated Katz's Fourth Amendment rights by bugging a public pay phone without a warrant, the Court held in *United States v. White* that no warrant was needed to record a conversation in a private home![17] A sociologist would expect that Mr. White has a higher expectation of privacy in his home than Mr. Katz has in a public phone booth. Nor is there any reason to believe that 'society' found the government's surveillance to be more reasonable in White's home.

Particularly relevant to what follows is that various court cases that draw on *Katz* seem not to recognize a 'split condition'—that is, situations in which the government collects information in a way that would be considered legal because it was "expected," but then uses and distributes it in "unexpected" ways, which would, thus, be illegal. There are, of course, many such split situations, and these situations should be covered by any comprehensive theory of privacy.

In short, it is difficult for a reasonable person to make sense out of *Katz*. Court rulings on whether a collection of personal information is a 'search' by

---

[16] Jim Harper, Reforming Fourth Amendment Privacy Doctrines, 57 AM. U. L. REV.138. *See also* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 60 (2001) ("Harlan's test was applauded as a victory for privacy, but it soon became clear that it was entirely circular."); Michael Abramowics, *Constitutional Cicularity*, 49 UCLA L. REV. 1, 60-61 ("Fourth Amendment doctrine, moreover, is circular, for someone can have a reasonable expectation of privacy in an area if and only if the Court has held that a search in that area would be unreasonable.").

[17] Cloud, *Symposium: Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendmen*t.

Justice Harlan's formula seem to be highly dependent on what judges divine a person or 'society' would expect, without determining in any half objective way what these expectations actually are. And—at the same time—such standards ignore that rulings on privacy recast these expectations.

b. <u>But Not Back to 'The Castle'</u>

While the time has come to leave behind the reasonable expectation standard, this is not to say that the courts should revert to pre-*Katz* Fourth Amendment analysis, which gave considerable weight to the home as the locus of privacy. In *Katz* the majority ruled that "the Fourth Amendment protects people, not places," rejecting the 'trespass' doctrine enunciated in *Olmstead.* However, even after this, the home remained largely inviolable in the eyes of the courts. It seems *Katz* did not detach Fourth Amendment safeguards from the home but rather extended the sphere of privacy beyond it to other protected spaces. Information collected about events in one's home is still often considered *a priori* a violation of privacy, while much more license is granted to the state in collecting information about conduct in public and commercial spaces. As Justice Scalia put it, "'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.' With few exceptions, the question whether a warrantless search of a home is reasonable and

hence constitutional must be answered no."[18] This is an idea that has deep roots in American and English common law: "zealous and frequent repetition of the adage that a 'man's house is his castle,' made it abundantly clear that both in England and the Colonies 'the freedom of one's house' was one of the most vital elements of English liberty."[19] In *Dow Chemical Company v. United States*, the court established the expectation of privacy was lower in an industrial plant than a home, because the latter "is fundamentally a sanctuary, where personal concepts of self and family are forged, where relationships are nurtured and where people normally feel free to express themselves in intimate ways."[20]

The inviolability of the home and the private/public distinction in privacy law has been roundly criticized by feminist scholars. Catharine MacKinnon writes the problem with granting the home extra protection is that "while the private has been a refuge for some, it has been a hellhole for others, often at the same time."[21] Linda McClain points out that freedom from state interference in the home "renders men unaccountable for what is done in private-rape, battery, and other exploitation."[22]

---

[18] Kyllo v. United States, 533 U.S. 27 (2001).
[19] Payton v. New York, 445 U.S. 573, 591–98 (1980).
[20] Dow. Chem. Co. v. United States, 749 F.2d 307, 314 (6th Cir. 1984), *aff'd*, 476 U.S. 227 (1986).
[21] Catharine A. MacKinnon, *Reflections on Sex Equality Under Law*, 100 YALE L. J. 1281, 1311 (1991).
[22] Linda C. McClain, *Inviolability and Privacy: The Castle, the Sanctuary, and the Body*, 7 YALE J.L. & HUMAN. 195, 209 (1995).

This article assumes that the private/public distinction is rapidly declining in importance in general[23] and with regard to privacy in particular.[24] Marc Jonathon Blitz made the case compelling with regard to the cyber age and hence is quoted here at some length:

> "The 1969 case Stanley v. Georgia forbade the government from restricting the books that an individual may read or the films he may watch "in the privacy of his own home." Since that time, the Supreme Court has repeatedly emphasized that Stanley's protection applies solely within the physical boundaries of the home: While obscene books or films are protected inside of the home, they are not protected en route to it—whether in a package sent by mail, in a suitcase one is carrying to one's house, or in a stream of data obtained through the Internet.
>
> However adequate this narrow reading of Stanley may have been in the four decades since the case was decided, it is ill-suited to the twenty-first century, where the in-home cultural life protected by the Court in Stanley inevitably spills over into, or connects with, electronic realms beyond it. Individuals increasingly watch films not, as the defendant in Stanley did, by bringing an eight millimeter film or other physical copy of the film into their house, but by streaming it through the Internet. Especially as eReaders, such as the Kindle, and tablets, such as the iPad, proliferate, individuals read books by downloading digital copies of them. They store their own artistic and written work not in a desk drawer or in a safe, but in the "cloud" of data storage offered to them on far-away servers."

Privacy, it follows, is hence best viewed as a personal sphere that follows an individual irrespective of location. This is a version of what Christopher Slobogin refers as the protection-of-personhood theory of privacy, which "views the right to

---

[23] Amitai Etzioni, *The Bankruptcy of Liberalism and Conservatism*, 128 PSQ 39 (2013).

[24] Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places And The Right to Anonymity*, 72 MISS. L. J. 213 (2002). Scott E. Sundby, *Everyman's Fourth Amendment: Privacy or Mutual Trust between Government and Citizen?*, 94 Columbia Law Review 1751, 1758–9(Oct., 1994), Bethany L. Dickman, *Untying Knotts: The Application of Mosaic Theory to GPS Surveillance in United States v. Maryland* 60 AM. U. L. REV. 731 (2011).

privacy as a means of ensuring individuals are free to define themselves."[25] Privacy plays the same role whether one is in the home or out in public: "because a substantial part of our personality is developed in public venues, through rituals of our daily lives that occur outside the home and outside the family, cameras that stultify public conduct can stifle personality development."[26] If the government uses a long distance 'shotgun mic' to eavesdrop on conversations of two persons walking in a public park, such a search is clearly more intrusive than if the government measured the heat setting in their kitchen. This is the case because conversations are much more revealing about the person, including their medical condition, political views and so on than is their preferred heat setting. (I turn below to the question whether information that reveals that one is committing a crime deserves extra protection.) In short, privacy is best not home bound.

c. A 'social policy' model of the Fourth Amendment

One way to proceed is to follow a version of what Orin Kerr calls "the policy model."[27] This is an instrumentalist approach that relies on normative judgments: "Judges must consider the consequences of regulating a particular type of government activity, weigh privacy and security interests, and opt for

[25] Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places And The Right to Anonymity*, 72 MISS. L. J. 213, 256 (2002)
[26] *Id.* at 257.
[27] *Id.* at 519.

the better rule."[28] The article next outlines the social, philosophical, and normative assumptions for such a model.

(i) In seeking to base a privacy doctrine not on the usual foundations of expectations or location, this article draws on a liberal communitarian philosophy that assumes that individual rights, such as the right to privacy, must be balanced with concerns for the common good, such as public health and national security.[29] In contrast, authoritarian and East Asian communitarians tend be exclusively concerned with the common good or pay mind to rights only to the extent that they serve the rulers' aims.[30] And at the opposite end of the spectrum, libertarians and several contemporary liberals privilege individual rights and autonomy over societal formulations of the common good. (Although the term 'common good' is not one often found in legal literature, its referent is rather close to what is meant by 'public interest,' which courts frequently recognize, with a similar concept found in the U.S. Constitution's reference to the quest for a "more perfect union.")

The Fourth Amendment reads, "The right of the people to be secure in their persons, houses, papers, and effects, against *unreasonable* searches and seizures, shall not be violated." This is a prime example of a liberal communitarian text because it does not employ the absolute, rights-focused language of many

[28] *Id.*

amendments (i.e., "Congress shall make *no* law"), but recognizes on the face of it that there are reasonable searches, understood as those in which a compelling public interest takes precedence over personal privacy.

(ii) This article assumes that the communitarian balance is meta-stable. That is, for societies to maintain a sound communitarian regime—a careful balance between individual rights and the common good—societies must constantly adjust their public policies and laws in response to changing external circumstances (e.g., 9/11) and internal developments (e.g., FBI overreach). Moreover, given that societal steering mechanisms are rather loose, societies tend to over steer and must correct their corrections with still further adjustments. For example, in the mid-1970s the Church and Pike Committees investigated abuses by the CIA, FBI and NSA, uncovering "domestic spying on Americans, harassment and disruption of targeted individuals and groups, assassination plots targeting foreign leaders, infiltration and manipulation of media and business."[31] As a result, Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA) and created the Foreign Intelligence Surveillance Court to limit the surveillance of American citizens by the U.S. government.[32] After 9/11, several reports concluded that the reforms had gone too far by blocking the type of interagency intelligence sharing

that could have forestalled the terrorist attacks.[33] As a result, the Patriot Act was enacted in a great rush and, according to its critics, sacrificed privacy excessively in order to enhance security and "correct" what are considered the excesses of the reforms the Church and Pike committees set into motion. Since then, the Patriot Act itself has been recalibrated.[34]

At each point in time, one must hence ask whether the society is tilting too far in one direction or the other. Civil libertarians tend to hold that rights in general and privacy in particular are not adequately protected. The government tends to hold that national security and public safety require additional limitations on privacy. It is the mission of legal scholars, public intellectuals, and concerned citizens to nurture normative dialogues that help sort out in which direction corrections must next be made.[35] (Note that often some tightening in one area ought to be combined with some easing in others. For instance, currently a case can be made that TSA screening regulations are too tight, while the monitoring of

---

[34] For a critical analysis of the "Information Sharing Paradigm" that has arisen in law enforcement and intelligence community since 9/11, *see* Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VIL. L. REV. 260 (2006).

[35] Alexander Aleinikoff, writing in 1987, argued that the courts had entered the "age of balancing." "Balancing has been a vehicle primarily for weakening earlier categorical doctrines restricting governmental power to search and seize." T. Alexander Aleinikoff, *Constitutional Law in the Age of Balancing*, 96 YALE L. J. 943, 965 (1987). Many civil libertarians have argued that post-9/11, Fourth Amendment rights are being systematically eroded in the name of national security. *See* Jay Stanley, *Reviving the Fourth Amendment and American Privacy*, ACLU, May 28, 2010, http://www.aclu.org/blog/national-security-technology-and-liberty/reviving-fourth-amendment-and-american-privacy. *See also* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 478 (2011) ("The theory of equilibrium-adjustment posits that the Supreme Court adjusts the scope of Fourth Amendment protection in response to new facts in order to restore the status quo level of protection. When changing technology or social practice expands government power, the Supreme Court tightens Fourth Amendment protection; when it threatens government power, the Supreme Court loosens constitutional protection.).

whether visitors and temporary residents committed to leave the U.S. actually did so is too loose).

Orin Kerr and Peter Swire engage in an important dialogue on whether the issues present above are best suited for treatment by the courts or by Congress, and whether they are largely viewed through the prism of the Fourth Amendment or Congressional acts. The following discussion treats both as if they were an amalgam.

(iii) Four criteria help specify the liberal communitarian approach to privacy.[36] First, a liberal democratic government will limit privacy only if it faces a well-documented and large scale threat to the common good (such as public safety or public health), not merely a hypothetical or one limited to few individuals or localities. (I avoid the term "clear and present danger," despite the similarity in meaning, because it has a specific legal reference, not here intended.) The main reason this threshold must be cleared is because modifying legal precepts—and with them the ethical, social, public philosophies that underlie them—endangers their legitimacy. Changes, therefore, should not be undertaken unless there is strong evidence that either the common good or privacy have been significantly undermined.

[36] *See* Amitai Etzioni, *The Limits of Privacy* (1999).

Secondly, if the finding is that the common good needs shoring up, one best seek to establish whether this goal can be achieved without introducing new limits on privacy. For instance, this is achieved when one removes personally identifying information (such as names, addresses and social security numbers) when medical records are needed by researchers, thus allowing access to data previously not accessible, e.g., of Medicare databanks. Various technical difficulties arise in securing the anonymity of the data. Several ingenious suggestions have been made to cope with this challenge.[37] Conversely, if privacy needs shoring up, one should look for ways to proceed that impose no "losses" to the common good. For instance, introducing audit trails.

Thirdly, to the extent that privacy-curbing measures must be introduced, they should be as little intrusive as possible. For example, many agree that drug tests should be conducted on those directly responsible for the lives of others, such as school bus drivers. Some employers, however, resort to highly intrusive visual surveillance to ensure that the sample is taken from the person who delivers it. Instead, one can rely on the much less intrusive procedure of measuring the temperature of the sample immediately upon delivery.

[37] See Note 78 below.

Fourthly, measures that ameliorate undesirable side effects of necessary privacy-diminishing measures are to be preferred over those that ignore these effects. Thus, if contact tracing is deemed necessary in order to fight the spread of infectious diseases to protect public health, efforts must be made to protect the anonymity of those involved. A third party may inform those who were in contact with an affected individual about such exposure and the therapeutic and protective measures they ought to next undertake, without disclosing the identity of the diagnosed person.

The application of these four balancing criteria helps to determine which correctives to a society's course are both needed and not excessive. This article focuses on the third criteria and seeks to address the question: what is least intrusive?

Part II. Privacy as a three dimensional cube

In this section I attempt to show that in order to maintain privacy in the cyber age, boundaries on information that may be used by the government should be considered along three major dimensions: The level of sensitivity of the information, the volume of information collected, and the extent of cybernation (defined as digitization, processing, and distribution). These considerations guide

one to find the lowest level of intrusiveness holding constant the level of common good. (A society ought to tolerate more intrusiveness if there are valid reasons to hold that the threat to the public has significantly increased, e.g., there is an outbreak of a pandemic—and reassert a lower level of intrusiveness when such a threat has subsided.)

a. Sensitivity

One dimension is the level of sensitivity of the information. For instance, data about the person's medical condition is considered highly sensitive, as are one's political beliefs and conduct (e.g., voting) and personal thoughts. Financial information is ranked as less sensitive than medical information, while publically presented information (e.g., license plates) and routine consumer choices much less so.

These rankings are not based on "expectations of privacy" or on what this or that judge divines as societal expectations, but on acts of Congress.[38] Rather, they reflect shared social values and are the product of politics in the good sense of the term, of liberal democratic processes, and moral dialogues.[39] (Different nations may rank differently what they consider sensitive. For example, France strongly

[38] Shaun Spencer raises concerns around legislating privacy protections. *See* Shaun Spencer, *Reasonable Expectatoins and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 860 (2002) ("Given the powerful influence of various lobbies opposed to strong privacy protection, that role may best be described as a sine qua non. That is, unless the public has a strong desire for privacy in a particular area, attempts to pass legislation establishing that area as a private sphere are doomed to fail…To the extent that legislatures base privacy legislation on social values and norms, they necessarily rely on the same changing expectations as the judicial conception of privacy.")

[39] AMITAI ETZIONI, FROM EMPIRE TO COMMUNITY: A NEW APPROACH TO INTERNATIONAL RELATIONS 67–71(2004).

restricts the collection of information by the government about race, ethnicity, and religion although it rationale is not the protection of privacy but rather a strong assimilationist policy and separation of state and church.) For those who analyze the law in terms of the law and economics paradigm, disclosure of sensitive data causes more harm to the person by objective standards than data that are not sensitive. Thus, disclosure of one's medical condition may lead one to lose one's job or not be hired, be unable obtain a loan, or incur higher insurance costs, among other harms. In contrast, disclosure of the kinds of bread, cheese, or sheets one buys—may affect mainly the kind and amount of spam they receive.

A re-examination of *Kyllo* helps highlight this principle. If one goes by *Katz*, the legality of a thermal imaging search from outside the home depends on what one presumes personal and societal expectations to be. At least, in middle class American suburbs, people may consider such a heat reading a violation of their expectations. If one clings to the idea that 'my home is my castle,' measuring the heat inside the home is indeed a major violation of privacy. However, if one goes by the cyber age privacy doctrine here outlined such readings ranks very low on sensitivity—because they reveal nothing about the resident's medical, financial, or political preferences, let alone their thoughts. In effect, they detect an extremely low bandwidth of information. The information revealed is less consequential than what kind of cereal the person purchased or which brand of coffee

One may argue that the information about the level of heating is actually particularly sensitive because it reveals that a crime is being committed. Preventing crime is obviously a contribution to the common good. And given that in 2011 fewer than half of violent crimes and 20% of property crimes in the U.S. were resolved, some may well hold that public authorities are not excessively indulged when dealing with crime.[40] As to harm to the individuals involved, they would be harmed only if they had a right to commit a crime. As to the presumption of innocence, there is the public safety exception. The arguments against the notion that crime committed in a home (e.g., spousal abuse) deserves more protection than one committed in public, were already presented above. What is new here is that historically, when the Constitution was written, searching a home required a person to enter or peep, which would entail a high level of intrusiveness because the intruder could not but note other potentially sensitive information besides whether or not a crime was being committed. However, technologies that have a very narrow and crime-specific bandwidth (e.g., dogs that sniff for bombs or sensors that measure abnormal levels of heat) and are, hence, very lowly-intrusive, should be allowed. One may disagree with this line of analysis, but still accept that basic point that the less-intrusive collection of insensitive information should be tolerated, while collection of highly-sensitive information should be banned

[40] "Offenses Cleared," Uniform Crime Report: Crime in the United States 2011, Federal Bureau of Investigation (October 2012).

Many court cases treat the voluntary release of information to others (and by them to still others, discussed below under the third party doctrine) as if they all had the same level of sensitivity,[41] including phone numbers dialed,[42] copies of written checks,[43] documents given to an accountant,[44] newspaper records,[45] and even papers held by a defendant's attorney.[46] A privacy doctrine that follows the principles here outlined would grant persons more say about the secondary usages of sensitive information, while recognizing that the less sensitive information may be used and passed on without the individual's explicit consent.

Over the years, Congress has pieced together privacy law by addressing the protection of one kind of sensitive information at a time, rather than treating them in a comprehensive fashion. Thus, in 1973, the Department of Health, Education and Welfare developed the Code of Fair Information Practices to govern the collection and use of information by the federal government. The principles of the code were incorporated in the Privacy Act of 1974, which "prohibits unauthorized disclosures of the records [the federal government] protects. It also gives individuals the right to review records about themselves, to find out if these records have been disclosed, and to request corrections or amendments of these

[41] The following examples are laid out in Swire, *Katz is Dead. Long Live Katz,* 908 –9.
[42] Smith v. Maryland, 442 U.S. 735, 745 (1979).
[43] United States v. Miller, 425 U.S. 435 (1976).
[44] Couch v. United States, 409 U.S. 322 (1973).
[45] Zurcher v. Stanford Daily, 436 U.S. 547 (1978).
[46] Fisher v. United States, 425 U.S. 391 (1976).

records, unless the records are legally exempt."[47] The Privacy Act applies only to the federal government and has not been expanded to include records kept by the private sector. In 1986, the Electronic Communications Privacy Act (EPCA) restricted wiretapping, regulated government access to electronic communication stored by third parties, and prohibited the collection of communications content (i.e., what was said, not who was called) by pen registers. After the Supreme Court ruled in the 1976 case *United States v. Miller* that there was no reasonable expectation of privacy for records at financial institutions, Congress passed The Right to Financial Privacy Act,[48] which extended Fourth Amendment protections to these records. As required by the 1996 Health Insurance Portability and Accountability Act (HIPAA), in 2002 the Department of Health and Human Services published the final form of "the Privacy Rule," which set the "standards for the electronic exchange, privacy and security of health information."[49] This accumulation of privacy protections includes laws covering specific sectors—or responding to specific events—but not any overarching design. A well-known case in point is Congress' enactment of The Video Privacy Protection Act after the

[47] *Privacy Act of 1974, as amended*, FEDERAL TRADE COMMISSION, available at: http://www.ftc.gov/foia/privacy_act.shtm (accessed April 7, 2013).
[48] The Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-342.
[49] Summary of the HIPAA Privacy Rule, Department of Health and Human Services, http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/

video rental records of Supreme Court nominee Judge Robert Bork were obtained by a Washington, D.C. newspaper.[50]

Congress could help to establish a privacy doctrine for the cyber age by reviewing what by now has been fairly called an incomplete "patchwork of federal laws and regulations" and providing a comprehensive overall ranking of protections based on the sensitivity of the data.[51]

b. Volume

The second dimension that a cyber age privacy doctrine should draw on is the volume of information collected. Volume refers the total amount of information collected about the same person holding constant the level of sensitivity. Volume reflects the extent of time surveillance is applied (the issue raised in *Jones*); the amount of information collected at each point in time (e.g., just emails sent to a specific person or all emails stored on a hard drive?); the bandwidth of information collected at any one point in time (e.g., only the addresses of email sent or also their content?). A single piece of low-sensitivity data deserves the least protection, and a high volume of sensitive information should receive the most protection.

[50] The Video Privacy Protection Act of 1988, 18 U.S.C. § 2710

[51] Gina Stevens, *Privacy Protections for Personal Information Online*, Congressional Research Service, Apr. 6, 2011.

Under such a cyber age privacy doctrine, different surveillance and search technologies differ in their intrusiveness. Least intrusive are those which collect only discreet pieces of information of the least sensitive kind. These include speed detection cameras, toll booths, and screening gates, because they all reveal, basically, one piece of information of relatively low sensitivity. Radiation detectors, heat reading devices and bomb and drug-sniffing dogs belong into this category, not only because of the kind of information (low or not sensitive) they collect, but also because the bandwidth of the information they collect is very low (just one facet, indeed a very narrow one, and for a short duration).

Typical CCTVs—privately owned, mounted on one's business, parking lot, or residential lobby—belong into the middle range because they pick up several facets (location, physical appearance, who one associates with), but do so only for only a brief period of time and in one locality. The opposite holds for Microsoft's Domain Awareness System, first tested in New York City in 2012. The program makes public data—like that from the city's 3,000 CCTV cameras, arrest records, 911 calls, license plate readers, and radiation detectors—easily and instantly accessible to the police. While the system does not yet utilize facial recognition, it could be readily expanded to include such technology.

Phone tapping—especially if not minimized (see below) and continued for extended period of time—and computer searches, collect more volume. (This

should not be conflated with considerations that come under the third dimension, whether these facts are stored, collated, analyzed and distributed, i.e., the elements of cybernation.)

Drones are particularly intrusive because they involve much greater bandwidth and have the potential to engage in very prolonged surveillance at relatively low costs (compared to, say, a stake out).

These volume rankings must be adapted as technologies change. The extent to which combining technologies is intrusive depends on the volume (duration and bandwidth, holding sensitivity constant) collected.

When the issue of extending privacy protection beyond spot collection arose in *Jones*, several legal scholars, in particular Orin Kerr, pointed to the difficulties in determining when the volume of collection was reasonable and when it became excessively intrusive. Kerr writes: "In *Jones*, the GPS device was installed for 28 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.' May indeed. If 28 days is too far, how about 21 days? Or 14 days? Or 3.6 days? Where is the line?"[52] 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 must be charged or released, the voting and driving age, the

[52] *Id.* at 24.

number of jurors and so on. One may say that they reflect what a "reasonable" person would rule. Actually they reflect what judges consider a compromise between a restriction that is clearly excessive and clearly inadequate—a line that has been adjusted often. There is no reason the volume of collection should not be similarly governed.

c. Cybernation: Storing, analysis, and access

The third dimension seems to be the one that is increasing in importance and regarding which law and legal theory have the most catching up to do. To return to the opening deliberations, historically, much attention was paid to the question whether the government can legally collect certain kinds of information under specific conditions. This was reasonable because most violations of privacy occurred through search and surveillance that implicated this first-level collection of spot information. True, some significant violations also occurred as a result of collating information, storing it, analyzing it and distributing it. However, to reiterate, as long as records were paper bound, which practically all were, these secondary violations of privacy were inherently limited when compared to those enabled by the digitization of data and the use of computers, i.e., by cybernation.

To illustrate this cardinal transformative development, a comparison: In one state, a car passes through a tollbooth, a picture of its license plate is taken—and then this information is immediately deleted from the computer if the proper

payment is made. In another state, the same information, augmented with a photo of the driver, is automatically transmitted to a central data bank. Here, it is combined with many thousands of other pieces of information about the same person, from locations he has visited (based on cell tower triangulation) to his magazine subscriptions, recent purchases and so on. The information is regularly analyzed by artificial intelligence systems to determine if people are engaged in any unusual behavior, what places of worship they frequent (flagging Mosques), which political events they attend (flagging those who are often involved in protests), and if they stop at gun shows. The findings are widely distributed to local police and the intelligence community, and can be gained by the press and divorce lawyers.

Both systems are based on spot information; that is, pieces of information pertaining to a very limited, specific event or point in time and typically of little significance in themselves—as in the case in the first state. However, if such information is combined, analyzed, and distributed, as depicted in the second scenario, it provides a very comprehensive and revealing profile of one's personal life. In short, the most serious violations of privacy are often perpetuated not by surveillance or information collection per se, but by combination, manipulation, and data sharing—by cybernation. The more information is cybernated, the more intrusive it becomes.

Part III. Limiting intrusion by cybernation

There are in place two major systematic approaches to deal with privacy violations that result from secondary uses, namely the third party doctrine and the EU Data Protection Directive (DPD). The third party doctrine holds that once a person voluntarily discloses a fact to another party, that party is free to pass on (or sell) this information to third parties and the various parties are free to further process this information, collate it with other data, draw inferences and so on—in short, to cybernate it.[53]

This approach is challenged by critics who note that in the cyber age much of our private lives are lived in a cyber world operated by third parties like Google and Facebook. Thus, Matthew Lawless writes that,

> "the third party doctrine gives effect to the criticism often aimed at the 'reasonable expectation of privacy' principle, by holding that individuals can only reasonably expect privacy where the Court gives them that privacy. Because the third party doctrine fails to address true societal expectations of privacy (as evident by its failure to protect any information entered into a search engine), it reinforces the privacy norms of a politically and temporally insulated judiciary: once people know their searches are exposed, then—by the time these cases are contested—there will, in truth, be no expectation of privacy."[54]

---

[53] Information voluntarily handed over to another party does not receive Fourth Amendment protection "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." United States v. Miller, 425 U.S. 435, 443 (1976); *see also* Orin Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 569–70 (2009). Earlier cases that built up this doctrine include Lee v. United States 343 U.S. 747 (1952); Couch v. United States 409 U.S. 322 (1973).

[54] Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2 UCLA J.L. & TECH. 1 (2007)

However, even without drawing on whatever the societal expectation of privacy is, one notes that considerable harm will come to people and that core societal values would be violated, if the third party doctrine is given free rein. This observation is strengthened by the fact that various exceptions to the third party doctrine are already in place, for instance special rules for medical and financial information. However, according to Greg Nojeim, these rules do not provide the same level of protection granted by the Fourth Amendment protection. He notes that "privacy statutes that protect some categories of sensitive personal information generally do not require warrants for law enforcement access."[55] Furthermore, Matthew Tokson argues that "The conflation of disclosure to automated Internet systems with disclosure to human beings" has led the court to exclude a great deal of personal information from Fourth Amendment protection, including "Internet protocol ("IP") addresses, e-mail to/from information, information about the volume of data transmitted to a user, name, address, and credit card information, and even the contents of a user's e-mails."[56]

The European Union's DPD in effect takes the opposite view, namely that any secondary use of personal information released by the person or collected about him requires the explicit *a priori* approval of the original individual 'owner'

---

[55] Orin Kerr and Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, ABA J., August 1, 2012, available at: http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/.

[56] Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 586 (2011).

of the information, and that this consent cannot be delegated to an agent or machine.[57] The details of DPD are complex and changing.[58] For instance, it made exceptions for many areas from this rule, for instance when the data are needed for research, public health, or law enforcement, among others. In January 2012, the European Commission passed draft legislation that would update the existing data protection law. This legislation includes an 'opt in' provision: "As a general rule, any processing of personal data will require providing clear and simple information to concerned individuals as well as obtaining specific and explicit consent by such individuals for the processing of their data." Data show that information about a person is used many times each day by a large variety of users. Hence, if such a policy were systematically enforced, each Internet user would have to respond to scores if not hundreds of requests per day even for uses of non-sensitive information. It seems that in this area, as in many others, the way DPD rules survive is by very often not enforcing them. Whenever I meet Europeans, and following public lectures in the EU, I ask if anyone has been ever asked to consent to the use of personal information that they had previously released. I have found only one person so far. He said that he got such a request—from Amazon. Other

[57] Daniel Cooper, *Consent in EU Data Protection Law*, EUROPEAN PRIVACY ASSOCIATION, available at http://www.europeanprivacyassociation.eu/public/download/EPA%20Editorial_%20Consent%20in%20EU%20Data%20Protection%20Law.pdf (accessed April 7, 2013).

[58] *Why do we need an EU data protection reform?*, EUROPEAN COMMISSION, available at http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf (accessed April 7, 2013).

sources indicate that compliance is, at best, "erratic".[59] The penalties for violating the DPD seem to be miniscule and rarely collected. No wonder a large majority of the EU public—70 percent—fear that their personal data may be misused.[60]

In short, neither of these approaches is satisfactory.

In addition, there are in place a large number of laws, regulations, and guidelines that deal with limited particular usages of personal information beyond the collection point. However (a) a very large number of them deal with only one dimension of the cube, and often only with one element of cybernation, limiting either storage, or analysis, or distribution. (b) They reflect the helter-skelter way they were introduced, and do not provide a systematic doctrine of cyber privacy. They are best viewed as building blocks, which, if subjected to considerable legal scholarship and legislation, could provide the needed doctrine. They are like a score of characters in search of an author.

One of the key principles for such a doctrine is that the legal system can be more tolerant of the primary point spot collection of personal information (a) the more limited the volume (duration and bandwidth) of the collection[61] and (b) the

---

[59] Erica Newland, "CDT Comments on EU Data Protection Directive," Center for Democracy and Technology, January 20, 2011, https://www.cdt.org/blogs/erica-newland/cdt-comments-eu-data-protection-directive

[60] "Data protection reform: Frequently asked questions," Europa, January 25, 2012, http://europa.eu/rapid/press-release_MEMO-12-41_en.htm?locale=fr.

[61] In the wake of *Jones*, Professor Susan Freiwald identified four factors that the courts use to extend Fourth Amendment protection to new surveillance technologies that "make sense." These include whether the target is unaware of the surveillance; it covers items that the people consider private; it is continuous; and it is indiscriminate (covers more information than is necessary for establishing guilt). Susan Freiwald, *The Four Factor Test*, THE SELECTED WORKS OF SUSAN FREIWALD, available at: http://works.bepress.com/susan_freiwald/11.

more limited and regulated cybernation is—holding constant the level of sensitivity of the information. (That is, much more latitude can be granted to the collection and cybernation of insensitive information, stricter limitation on highly sensitive information, and a middle level of protection in between). The same holds for the threat level to the common good.

In other words, a cyber age privacy doctrine can be much more tolerant of primary collection conducted within a system of laws and regulations that are effectively enforced to ensure that cybernation is limited, properly supervised, and employed for legitimate purposes —and much less so, if the opposite holds. One may refer to this rule as the inverse relationship between primary license and secondary constraints.

Another key principle is a ban on using insensitive information to divine the sensitive—e.g., using information about routine consumer purchases to divine one's medical condition—because it is just as intrusive as collecting and employing sensitive information.[62] This is essential because currently such behavior is rather common.[63] Thus, under the suggested law, Target would be

---

[62] People often trust assurances that their sensitive information (names and social security number) can be deleted when their data is collected in large databases. In fact, scientists have shown that individuals can be easily "deanonymized." Paul Ohm writes that this misunderstanding has given the public a false sense of security and has lead to inadequate privacy protections, laws and regulations. *See* Peter Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010). *See also* Marcia Stepanek, *Weblining*, BusinessWeek, April 3, 2000, at http://www.businessweek.com/2000/00_14/b3675027.htm; Jennifer Golbeck, Christina Robles & Karen Turner, *Predicting Personality with Social Media*, CHI EXTENDED ABSTRACTS 2011, 253-262.

[63] Marcy Peek, Passing Beyond Identity on the Internet: Espionage and Counterespionage in the Internet Age, 28 VT. L. REV. 91, 94 (2003) (evaluating ways to resist discriminatory marketing in cyberspace); Marcia Stepanek,

prevented from sending coupons for baby items to a teenage girl after the chain store's analysis of her recent purchases suggested she might be pregnant.[64]

Kerr correctly points out that it would be exceedingly difficult to cover the private sector by drawing on the Fourth Amendment and points, instead, to the 1986 Electronic Communications Privacy Act (ECPA) to show that Congress can enact laws that protect people from intrusion both by the government and by private actors.[65] To further advance the cyber age privacy doctrine, much more attention needs to be paid to private actors. Privacy rights, like others, are basically held against the government, to protect people from undue intrusion by public authorities. However, increasingly cybernation is carried out by the private sector. There are corporations that make shadowing Internet users—and keeping very detailed dossiers on them—their main line of business. According to Slobogin,

> "Companies like Acxiom, Docussearch, ChoicePoint, and Oracle can provide the inquirer with a wide array of data about any of us, including: basic demographic information, income, net worth, real property holdings, social security number, current and previous addresses, phone numbers and fax numbers, names of neighbors, driver records, license plate and VIN numbers, bankruptcy and debtor filings, employment, business and criminal

---

Weblining, BUS. WK., Apr. 3, 2000, http://www.businessweek.com/2000/00_14/b3675027.htm (A data broker company Acxiom matches names against housing, education, and incomes in order to identify the unpublicized ethnicity of an individual or group.); Nicholas Carr, Tracking Is an Assault on Liberty, With Real Dangers, WALL ST. J., Aug. 7–8, 2010, at W1 ("It used to be . . . you had to get a warrant to monitor a person or a group of people. Today, it is increasingly easy to monitor ideas."); Amitai Etzioni, *Privacy Merchants: What Is To Be Done?*, 14 PENN. J. CONST. L, 929, 948-950 (2012).

[64] *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, FORBES, Feb. 16, 2012, http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

[65] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 871–2 (2004).

> records, bank account balances and activity, stock purchases, and credit card activity."[66]

And these data are routinely made available to the government, including the FBI. Unless this private cybernation is covered, the cyber age privacy doctrine will be woefully incomplete.[67]

Given that private actors are very actively engaged in cybernation and often tailor their work so that it might be used by the government (even if no contract is in place and they are, hence, not subject to the limits imposed on the government), extending privacy doctrine beyond the public/private divide is of pivotal importance for the future of privacy in the cyber age. Admittedly, applying to the private sector similar restrictions and regulations that control the government is politically unfeasible. However, as one who analyzes the conditions of society from a normative viewpoint, I am duty bound to point out that it makes ever less sense to maintain this distinction.[68] Privacy will be increasingly lost in the cyber age, with little or no gain to the common good, unless private actors—and not just the government—are more reined in. To what extent this may be achieved by self regulation, changes in norms, increased transparency, or government regulation is a question not here addressed.

---

[66] Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 320 (2008).

[67] For further discussion on these matters, see Amitai Etzioni, *The Privacy Merchants: What Is To Be Done?*, 14 PENN. J. CONST. L. 929 (March 2012); Amitai Etzioni, *The Bankruptcy of Liberalism and Conservatism*, 128 PSQ 39 (2013) (discussing the collapse of the public-private divide).

[68] For more discussion, see Amitai Etzioni, *The Bankruptcy of Liberalism and Conservatism*, 128 PSQ 39 (2013).

For this doctrine to be further developed laws and court rulings ought to be three dimensional.[69] These laws and court cases best specify not merely whether a particular collection of personal information is a 'search,' but also what level of sensitivity can be tolerated and to what extent the information may be stored, massaged, and distributed. This may seem—and is—a tall, if not impossible, order. However, as is next illustrated, a considerable number of measures are already in place that are, in effect, at least two dimensional. These, though, suffer from the fact that they have been introduced each on their own and do not reflect an overarching doctrine of privacy and, hence, reveal great inconsistencies that need to be remedied. I cannot stress enough that the following are but selective examples of such measures.

One should note that a very early attempt to deal with the issue—basically, in terms here used, by banning a form of cybernation—utterly failed. In 2003, Congress shut down the Pentagon's "Total Information Awareness" program, which was created to detect potential terrorists by using data mining technologies to analyze unprecedented amounts personal transaction data. However, a report by the *Wall Street Journal* in 2008 revealed that the most important components of

[69] Kerr sees a greater role here for Congress, while Swire for the courts. *See* Peter P. Swire, *Katz is Dead. Long Live Katz,* 102 MICH. L. REV. 904, 912 (2002) and Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution,* 102 MICH. L. REV. (2004). This article is unable to add to these deliberations other than to recognize that both are needed and neither seems able to keep up with changing technologies.

T.I.A. were simply "shifted to the NSA" and "put in the so-called black budget, where it would receive less scrutiny and bolster other data-sifting efforts."[70]

Minimization is one way of addressing the volume issue as Swire pointed out in his groundbreaking article on *Jones* and mosaic theory.[71] Accordingly, when the FBI taps a phone, even for an extended period of time, the intrusion can be reduced significantly if the FBI either stops listening when it hears that the conversation is not relevant to the investigation (e.g., a child is calling the suspect under surveillance) or lock away those segments of the taped correspondence that turn out to be irrelevant.[72] For this rule to be integrated into the doctrine, it may be waived for insensitive information. That is, there would be no need to minimize if the child asked, say, to watch TV, but activated if she asked, say, about the medical news about a family member.

Another example of a safeguard against excessive privacy intrusions is the requirement that certain content be deleted after a specific time period. Most private companies that utilize CCTV erase video footage after a set number of days, for instance after a week. Admittedly, their reasons for doing so may be simply economic; however the effect is still to limit the volume of collection and potential for subsequent abuse. Note that that there are no legal requirements to

---

[70] Siobhan Gorman, *NSA's Domestic Spying Grows As Agency Sweeps Up Data,* WALL STREET J., Mar. 10, 2008.
[71] Peter P. Swire, A *Reasonableness Approach to Searches After the Jones GPS Tracking Case,* 64 STAN. L. REV. ONLINE 57 (2012).
[72] Gary T. Marx, *Ethics for the New Surveillance,* 14 THE INFORMATION SOCIETY: AN INTERNATIONAL JOURNAL 171, 178 (1998).

erase these tapes. However, such laws ought to be considered. (Europeans are increasingly recognizing a “right to be forgotten.”) It would be in the public interest to require that footage be kept for a fixed period of time (as it has proven useful in fighting crime and terrorism), but also ban under most circumstances the integration of the video feed into encompassing and cybernated systems, of the kind Microsoft has developed (discussed above).

The treatment of private local CCTVs should be examined in the context of the ways other such spot collection information is treated. Because the bandwidth of information collected by tool booths, speed cameras and radiation detectors is very narrow, one might be permitted to store it longer and feed it into cybernated systems. By contrast, cell phone tracking can be utilized to collect a great volume and bandwidth of information about a person’s location and activities. People carry their phones to many places they cannot take their cars, where no video cameras or radiation detectors will be found, including sensitive places such as political meetings, houses of worship, and residences. (These rules must be constantly updated as what various technologies can observe and retain, constantly changes.)

Regulations to keep information paper bound have been introduced for reasons other than protecting privacy, but these requirements still have the effect of limiting intrusiveness. For example, Congress prevents the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) from computerizing gun records when

such information is collected during background checks.[73] In 2013, an amendment to the anti-insider trading STOCK Act exempted 28,000 executive branch staff from having to post their financial disclosure forms "online in a searchable, sortable and downloadable format."[74] These bans remind one, that not all the privacy measures that are in place are legitimate and that some are best scaled back rather than enhanced.[75]

A related issue is raised by the cybernation of arrest records. Arrest records should be, but are not, considered highly-sensitive information. When these records, especially those concern people who were subsequently released without any charges, were paper bound, the damage they inflicted on most people's reputations was limited. However, as a result of cybernation, they have become much more problematic. Under the suggested doctrine, arrest records of people not charged after a given period of time would be available only to law enforcement officers. The opposite might be said about data banks that alert the public to physicians that have been denied privileges for cause, a very high threshold that indicates serious ethical shortcomings.

Many computer systems ("clouds" included) encrypt their data and a few have introduced audit trails. The cyber age privacy doctrine might require that all

---

[73] Erica Goode and Sheryl Gay Stolberg, *Legal Curbs Said to Hamper A.T.F. in Gun Inquiries*, N.Y. TIMES, Dec. 25, 2012.
[74] Tamara Keith, *How Congress Quietly Overhauled Its Insider-Trading Law*, NPR, Apr. 16, 2013, http://m.npr.org/news/Politics/177496734.
[75] AMITAI ETZIONI, THE LIMITS OF PRIVACY (2000).

data banks that contain sensitive information be encrypted and include at least some rudimentary form of an audit trail.

Technologies can be recalibrated to collect the 'need to know' information while shielding extraneous but highly sensitive, information from observation. For example, when law enforcement collects DNA samples from convicted criminals or arrested individuals, FBI analysts create DNA profiles using so-called 'junk DNA' "because it is not 'associated with any known physical or medical characteristics,' and thus theoretically poses only a minimal invasion of privacy."[76] Storing these "genetic fingerprints" in national databases is much less intrusive than retaining data produced by blood samples, which reveal "reveal sensitive medical or biological information."[77] In 2013, the TSA stopped its use of body scanners that revealed almost nude images, using instead scanners that produce "cartoon-like" images, on which the scanners mark places hidden objects are found.[78] This did not affect the volume of collection, but lessened the sensitivity of the content.

Other measures must address the fact that often data can be "re-identified" or "de-anonymized." In 2006, AOL released the search records—stripped of "personal identifiers"—of over 600,000 people. An investigation by the *New York*

---

[76] Anna C. Henning, *Compulsory DNA Collection: A Fourth Amendment Analysis*, CONGRESSIONAL RESEARCH SERVICE R40077, at 2, Feb. 16, 2010.
[77] *Id.* at 13.
[78] Jack Nicas, TSA to Halt Revealing Body Scans at Airports, WALL STREET JOURNAL, Jan. 18, 2013.

Times, however, demonstrated that intimate information—including names and faces—can be gleaned from such purportedly anonymous data. This risk is mitigated by the development of statistical methods that prevent such undertakings, such as "differential privacy," which allows curators of large databases to release the results of socially beneficial data analysis without compromising the privacy of the respondents who make up the sample.[79]

Many more examples could be provided. However, the above list may suffice to show that, while there are numerous measures in place that deal with various elements of the privacy cube, these have not been introduced with systematic attention to the guiding principles needed for the cyber age.

[79] Cynthia Dwork, *Differential Privacy: A Survey of Results*, in M. Agrawal et al. (Eds.): TAMC, LNCS 4978, pp. 1–19 (2008) (Roughly speaking, differential privacy ensures that the removal or addition of a single database item does not (substantially) affect the outcome of any analysis. It follows that no risk is incurred by joining the database, providing a mathematically rigorous means of coping with the fact that distributional information may be disclosive.").