The John Marshall Journal of Information Technology & Privacy Law

Volume 29
Issue 3 *Journal of Computer & Information Law - Spring/Summer 2012*

Article 7

Summer 2012

A Liberal Communitarian Conception of Privacy, 29 J. Marshall J. Computer & Info. L. 419 (2012)

Amitai Etzioni

ARTICLES

A LIBERAL COMMUNITARIAN CONCEPTION OF PRIVACY

AMITAI ETZIONI*

ABSTRACT

In a large and complex society, anti-social behavior cannot be restrained by government intervention alone—without it becoming a police state. Informal social controls are necessary to keep deviance from societal norms and values at a socially acceptable level, and one of the levers of this social pressure is the observation of and reaction to the personal conduct of members of one's community. This article argues that in several areas of contemporary American life decreasing privacy by strengthening informal social controls will lessen the need for state surveillance and regulation, which tends to be act with a heavier hand and is *more* invasive than its informal counterpart.

This article[1] suggests that in the contemporary American context:

(a) Increased protection of social privacy will lead to more government scrutiny. Hence, when one seeks to regulate social media in order to better protect privacy, one ought to take into account that such regulation is likely to undermine informal social controls, which in turn will lead to greater government surveillance and intrusion.[2] Parents, colleges, and the community in general should be accorded a

* University Professor and Director of the Institute for Communitarian Policy Studies at The George Washington University.

1. The author is indebted to Ashley McKinless for research assistance and to Erin Syring, Jeff Gianattasio, and Chris Slobogin for commentaries on a previous draft. He also benefited from discussion with Orin Kerr. The article draws on previous work of the author, including AMITAI ETZIONI, THE LIMITS OF PRIVACY (Basic Books 2000); Amitai Etzioni, *Implications of Select New Technologies For Individual Rights and Public Safety,* HARV. J.L. & TECH. 15.2 258-290 (2002); Amitai Etzioni, *Children and Free Speech*, *in* The Common Good (Polity Press 2004), at 56-94; Amitai Etzioni, *The Privacy Merchants: What Is To Be Done?*, U. PA. J. CONST. L. 14.4 (2012).

2. Privacy issues have taken the center stage in recent years due to a confluence of factors, including widespread adoption of the Internet, social media and mobile phones, as well as economic incentives for companies to monetize consumer information. *See* Nicole A.

relatively high level of access to information about personal conduct. *See* Part I.

(b) "The expectation of privacy" as a foundation for legal rulings and public policy should be allowed to fade away, and determining what constitutes a reasonable standard of privacy should draw on four explicit criteria. Accordingly, before limiting the scope of privacy, courts and policy makers should consider:

i. The import of challenges to core values;

ii. The availability of voluntary means to cope with these challenges;

iii. Ways to minimize the intrusion if one is deemed necessary; and

iv. Attention to unanticipated consequences. (This might be called a social policy model but it has clear foundations in the constitution.) *See* Part II.

(c) If a free society can tolerate more surveillance, the greater is the surveillance of surveillance. The more government agencies are subject to oversight and their agents are accountable, including to those higher in rank, the legislature, and to the public, the more leeway they can be accorded. *See* Part III for a new mechanism for public oversight.

(d) Sensitive information should be better protected than insensitive information, and the use of insensitive information to ferret out that which is more sensitive should be treated as akin to mining sensitive information. *See* Part IV.

I. INTRODUCTION

A liberal communtarian conception of privacy starts by taking for granted that citizens face two or more fully legitimate concerns (or conceptions of utility), and hence citizens should not *a priori* privilege any. High among these concerns is the protection of individual rights and of the common good. In the following discussion, the focus is on one right – the right for privacy – and two categories of the common good—the moral order (to be defined shortly) and homeland security. Indeed, the particular kind of communitarianism here followed is referred to as liberal because it combines concerns pertaining to individual rights with those for the common good.[3] This social philosophy is reflected in the American Constitution in the references to both individual rights and the general welfare, and in the age-long dialogue between Jeffersonian and Hamiltonian theories of government.[4]

Ozer, *Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. L. & SOC. CHANGE 215, 233 (2012).

3. *See* AMITAI ETZIONI, THE NEW GOLDEN RULE: COMMUNITY AND MORALITY IN A DEMOCRATIC SOCIETY (Basic Books 1996).

4. E.J. DIONNE, OUR DIVIDED POLITICAL HEART: THE BATTLE FOR THE AMERICAN IDEA IN AN AGE OF DISCONTENT (Bloomsbury USA 2013).

This liberal communitarian approach differs from those approaches which strongly advocate for individuals' rights in general, particularly privacy rights, set a very high bar that must be cleared before rights can be limited, and put the onus of proof on those who seek such concessions.[5] The liberal comunitarian approach also parts from those who hold that security must be protected and when needs conflict with rights, security should be privileged. Authoritarian communities and East Asian communitarians tend to be concerned with either the common good or rights to the extent that the rights are upheld to serve the rulers.[6]

The text of the Fourth Amendment reflects this liberal communitarian approach. Unlike the absolute language of the First Amendment ("Congress shall make no law. . ."), the Fourth Amendment bans only unreasonable search, and thus, on the face of it, recognizes a whole category of searches that are reasonable. Often, they are reasonable because they serve the common good (or, the public interest).[7]

II. IT TAKES A VILLAGE TO PREVENT A CRIME: THE HYDRAULIC RELATIONSHIP BETWEEN SOCIAL PRIVACY AND GOVERNMENT SCRUTINY

The moral order of a community is based on two elements. The first is the community's moral culture, which is a set of shared values to which the community members subscribe and which are specified into behavioral norms of do's and do not's. The second is a set of informal social controls that reward those who heed the norms and penalize those who violate the norms. The stronger the moral order, there exists less of a need for policing, courts, jails, and all of the associated economic and human costs of coercive control by the government.[8] To put it the other

5. ACLU, *Keep America Safe and Free,* http://www.aclu.org/key-issues.

6. Russell A. Fox, *Confucian and Communitarian Responses to Liberal Democracy*, 59 REV. OF POL. 561 (1997); Joseph Chan, *A Confucian Perspective on Human Rights for Contemporary China*, in THE EAST ASIAN CHALLENGE FOR HUMAN RIGHTS (Joanne R. Bauer & Daniel A. Bell eds. 1999), at 212.

7. This approach presumes that one can define the common good and measure it, and that the issue is more than dealing merely with a clash of a large number of private interests, a subject not further explored here. *See* AMITAI ETZIONI, THE COMMON GOOD (Polity Press 2004); AMITAI ETZIONI, THE NEW GOLDEN RULE: COMMUNITY AND MORALITY IN A DEMOCRATIC SOCIETY (Basic Books 1996).

8. For a discussion of the legal implications of strong or weak informal social controls, *see* James S. Coleman, *The Creation and Destruction of Social Capital: Implications for the Law,* 3 NOTRE DAME J.L. ETHICS & PUB. POL'Y 375, 392 (1988) (Coleman defines "social capital" as the social organizations, such as the family, school, and community, that facilitate the provision of public goods, including "social norms and sanctions that enforce them").

way around, crime and punishment are indicators of communal failure, of a weak moral order, and weak informal controls.

For the moral order to function, privacy must be limited. Privacy must be limited because in order to activate informal social controls, members of the community must be aware that anti-social behavior is occurring. To proceed, we must introduce/operate under a sociological definition of privacy: privacy is a societal license to keep some areas of one's behavior, emotions, and thought invisible and inaudible, and thus free from communal surveillance and control.

To illustrate, the following is a relatively simple example of a community's moral order. One can add a chemical to the waters of a swimming pool that will produce a blue cloud around individuals who relieve themselves in the pool. There is no sociological study to prove the effectiveness of this chemical; however, the possibility of this anti-social behavior, once private, becoming public should diminish the occurrence of this behavior, without drawing on law enforcement.

There is also the tendency to assume that whatever takes place in one's private space should be granted privacy protection, the idea that "my home is my castle." Much of the literature on privacy and legal cases concerns the boundaries of this private space, as highlighted by *Katz v. United States*,[9] *Kyllo v. United States*,[10] and various cases concerning searches of one's car or luggage. However, another view has expressed that even though spousal abuse seems to occur within the confines of a person's home, concerns for privacy should not stop the community from investigating such conduct.[11] One may say that when such suspicions arise, the authorities can be notified and a warrant granted by the courts to investigate the matter. However, the community can intervene legitimately before there is enough evidence to permit the involvement of law enforcement. If the community feels freer to ask spouses about their conditions (say if bruises are visible or screams emanate from their homes) and to censure members of the community who are held to be abusive, there will be less spousal abuse and less need for government action.

This is possible because in contemporary liberal democratic societies the punishments of informal social control are as a rule relatively light, and hence if they are excessively activated – the harm is limited. At the same time, informal social control often prevents misconduct from escalating into a crime. Most people will choose to "behave" rather than face the censure of their community, as long as they are members of such

9. Katz v. United States, 389 U.S. 347 (1967).

10. Kyllo v. United States, 533 U.S. 27 (2001).

11. For a critique of the public/private distinction as related to domestic abuse, *see* Elizabeth M. Schneider, *The Violence of Privacy*, 23 CONN. L. REV. 973 (1991); *see also* KRISTIN A. KELLY, DOMESTIC VIOLENCE AND THE POLITICS OF PRIVACY (Cornell University Press 2002).

communities that have pro-social norms. The opposite effect would hold true in traditional or authoritarian societies, such as North Korea and Saudi Arabia, and in those societies in which social pressures are as overwhelming as they are in many parts of Japan.[12] In these societies informal controls are excessive so the scopes of invisible behavior and privacy are more expansive.

A. Parental Surveillance of Minors

Informal social controls suffer when minors are treated as individuals with strong rights or privacy against their parents, as some civil libertarians and librarians hold. From a communitarian viewpoint, parents and children are members of a small community (the family) and the parents are agents of more extended communities, responsible for the social conduct of their children. Although children are to be viewed as accumulating more rights as they grow older, in principle, the default position ought to be—in order for the moral order to work and the role of the state to be limited—that parents have not merely a right but a duty to monitor the behavior of their children. As new technologies make it easier for children to conceal their behavior, the moral order is served when the parents also take advantage of technological advances in order to discharge their parental responsibilities.

The Telecommunications Act of 1996 required new televisions to include a V-chip that allows users to block all programming that carries a particular rating. The rating system was created and voluntarily adopted by the television industry, and the blocking can only be activated by individuals who choose if and how to use their V-chip. Nevertheless some civil libertarians objected, calling the system "government-backed censorship" that would "empower bureaucrats and television executives to make decisions for parents."[13] One legal scholar wrote that the V-chip "raises the possibility that in the Information Age, control of filters may be one of the most important forms of power over human thought and expression. In the Information Age, the informational filter, not information itself, is king."[14] There are similar developments online including software such as "NetSnitch" and "NetNanny" that allow parents to monitor (though not block) what websites their children visit. Marc Rotenberg of the Electronic Information Privacy Center com-

12. Chie Muroga Jex, Social Conformity and Nationalism in Japan: A Perspective from Japanese Expertise (LAP LAMBERT Academic Publishing 2011).

13. Press Release, American Civil Liberties Union, ACLU Expresses Concerns on Rating Scheme; Says 'Voluntary' System is Gov't-Backed Censorship (Feb. 29, 1996) http://www.aclu.org/news/n022996b.html; *see* Paul Farhi, *FCC Set to Back V-Chip*, Wash. Post, Mar. 6, 1998, at G03.

14. Jack M. Balkin, *Media Filters, The V-Chip and the Foundations of Broadcast Regulation*, 45 Duke L. J. 1133 (1996).

mented that this "[s]ounds like Orwellian parenting. . .you might as well drop a video camera in your kid's bedroom."[15]

Such objections to protective measures for minors of all ages are problematic on two grounds. First, there is a need to consider age-gradations.[16] Minors, especially younger ones, have not yet developed basic moral values or rational decision-making capabilities—both of which are relevant in determining what rights they should be afforded. Second, parents and educators have a social and moral duty to shape the cultural environment in which children develop, a duty that cannot be fulfilled if they are unable to monitor what is exposed to their minor children. If in the name of protecting the privacy of minors, parents are hobbled in discharging their duties, the state will end up with having to deal with more minors, and later adults, who engage in anti-social behavior.

B. College Students

When minors become legal adults and attend college, their privacy rights against their parents are much stronger than those of minority age. Still, there are situations in which the moral order would benefit and government policing could be reduced if the parents received more information from the colleges about their children-students' record and conduct.

Colleges used to act *in loco parentis*. However, as of the 1960s they greatly curtailed this role. At the same time, they also increased the privacy protection of the students not so much from the state, but rather against their parents. The Family Educational Rights and Privacy Act (FERPA) of 1974 limited the educational information that schools can share with parents. FERPA has prevented colleges from reporting troubling signs, such as signs of substance-abuse and mental disturbance, to parents.[17] FERPA was amended in 1998 to allow for (though not require) parental notification when a student violates the school's

15. *New Software Tracks Kids on Internet Without Blocking Sites,* Augusta Chron., Aug. 4, 1997, http://chronicle.augusta.com/stories/1997/08/04/tec_212418.shtml.

16. The treatment pediatric patient privacy and consent provides an example of maturity and age-graded privacy considerations. The "mature minor doctrine" allows courts to take into weigh factors such as age, education, and perceived judgment capacity when deciding the degree of medical privacy afforded to a minor vis-à-vis their parents. Amy L. McGuire & Courtenay R. Bruce, *Keeping Children's Secrets: Confidentiality in the Physician-Patient Relationship,* 8 Hous. J. Health L. & Pol'y 315, 333 (2009) ("In deciding on a general policy regarding patient confidentiality, physicians ought to consider, weigh and prioritize the patient's developing autonomy and level of maturity, the importance of trust in the therapeutic relationship, the family dynamics, respect for the parent-child relationship and the parents' right to rear their child as the deem appropriate").

17. Elizabeth Bernstein, *Colleges Move Boldly on Student Drinking,* Wall St. J., Dec. 6, 2007, http://online.wsj.com/article/SB119690910535115405.html?mod=hpp_us_editors_picks.

drinking and drug policy.[18] Recently, the shooting of students by other students, for example at Virginia Tech in 2005, has further pushed colleges to realize that family ties and roles do not stop when a child ceases to legally be a minor and enrolls in a college. As the preceding analysis suggests, colleges are now making it more possible for parents to act as agents of informal social controls.[19]

These changes in policies are not without controversy.[20] The new laws, regulations and college policies should be amended to enable students to appeal to the school to not share information with their families if the students can show that such notification may cause harm to the students. On the contrary, the more families can be mobilized to help curb anti-social behavior, the less colleges will have to draw on public authorities to curb student anti-social behavor, unless they themselves are inclined to return to serve *in loco parentis.*

C. Tracking Rental Cars

As will become clear below, there are many areas in which the privacy of customers and employees should be better protected from corporate surveillance. However, there are situations in which new informal controls by corporations do serve the common good and reduce the need for governmental coercive controls. One case in point is the GPS devices that many car rental companies install in their vehicles. This technology allows the car rental companies to locate stolen or lost vehicles, provide roadside or emergency assistance, and track where and how fast renters drive. Acme Rental tracked renters' speed and charged them $150.00

18. Some argue that the emergency exception included in FERPA is too narrowly defined leading schools to "default to the nondisclosure option rather than disclosing information to third parties, such as parents, when students threaten to harm themselves or others." She notes that Congress and the Courts have the ability to correct this as societal attitudes about safety and privacy shift—as evidenced by the changes made to FERPA to notify parents about illegal substance use. *See* Stephanie Humphries, *Institutes of Higher Education, Safety Swords, and Privacy Shields: Reconciling FERPA and the Common Law,* 35 J.C. & U.L. 145 (2008).

19. For a study on the impact of the passage of the Higher Education Amendments of 1998, which amended the Family Education Rights and Privacy Act of 1974 to make it easier for colleges and universities to notify parents when their student broke institutional policies or drug and alcohol rules, *see* John W. Lowery, Carolyn J. Palmer & Donald D. Gehring, *Policies and Practices of Parental Notification for Student Alcohol Violations,* 42 NASPA J. 415 (2004) (stating before the 1998 amendment, 13.8% of the institutions in the study had formal written parental notification policies; in 2002, 45.8% reported to have one).

20. For more discussion on policy changes, *see* William DeJong, *Discouraging Mischief: Using Environmental Management to Curb High-Risk Drinking,* Prevention File: 14 Alcohol, Tobacco, and Other Drugs (1999); *see also* John W. Lowery, Carolyn J. Palmer & Donald G. Gehring, *Policies and Practices of Parental Notification for Student Alcohol Violations*, 42 NAPSA J. 4 (2004).

every time they exceeded the speed limit by a certain amount for over two minutes. The company was sued and the Connecticut Supreme Court found that the fee was excessive, but not that the GPS tracking was unlawful.[21]

Speaking about the case, Richard Smith of the Privacy Foundation states that "giving out speeding tickets is the job of the police, not of private industry."[22] He does not explain why limiting dangerous driving is more justified when done by the government than by those whose vehicles are involved. David Sobel, general counsel of the Electronic Privacy Information Center, adds the concern that driving records saved by rental companies could be accessed by lawyers and police.[23] As speeding is illegal, what is the reason such records should not be available? Aviel D. Rubin, the technical director of the Information Security Institute at Johns Hopkins University, goes a step further, arguing, "[t]he only way to get real privacy is not to collect the information in the first place."[24] This is the kind of one-sided advocacy that communitarians seek to avoid. Encouraging drivers to drive safely is for the common good, and as long as drivers are informed of corporate controls, they can readily take their business elsewhere if they find these controls too intrusive. They can hardly do so to avoid government controls.

So far this Article has showed that allowing informal social control to work by limiting social privacy is preferable to government surveillance as a way to control anti-social behavior. However, this of course does not mean that peeping toms should be encouraged or that people should be free to spy on each other. The question hence arises as to which matters are to be left private in the social context?

One answer is given that in contemporary America, people chose which communities to live in—the average American moves once every five years—the level of privacy can vary by setting to meet different preferences.[25] Some communities afford less privacy and more informal order versus other communities that have the opposite profile. People may choose to join groups such as Alcoholic Anonymous, in which significant

---

21. Anita Ramasastry, *Tracking Every Move You Make: Can Car Rental Companies Use Technology to Monitor Our Driving? A Connecticut Court's Ruling Highlights an Important Question*, FINDLAW (Aug. 23, 2005), at http://writ.news.findlaw.com/ramasastry/20050823.html.

22. Robert Lemos, *Car Spy Pushes Privacy Limit,* ZDNET (Jun. 20, 2001), at http://www.zdnet.com/news/car-spy-pushes-privacy-limit/116132.

23. David Wichner, *Rental Car Tracking Results in Lawsuit,* RENSE.COM, http://rense.com/general26/rentalcarsatellite.htm.

24. John Schwartz, *This Car Can Talk. And What It Says May Cause Concern,* N.Y. TIMES (Dec. 29, 2003), http://www.nytimes.com/2003/12/29/business/this-car-can-talk-what-it-says-may-cause-concern.html?pagewanted=4&src=pm.

25. Stephen Ansolabehere & John Lovett, *Measuring the Political Consequences of Residential Mobility* (CCES Working Paper Series 2008).

disclosure is demanded precisely in order to enhance informal social controls. Others who hold privacy more dearly may well prefer to live in a city, especially in high-rise buildings in which anonymity and privacy are more readily available. Still, others may labor to decrease controls in their communities and increase privacy, e.g., by changing the rules of their residential association. True, because of economic and social conditions, the geographic mobility of some people is rather limited; they must stay where they can earn a livelihood. Still, they have a measure of choice, whether to keep largely to themselves or be more socially engaged which often entails less privacy.

In short, in civil society people are relatively free to choose the balance between moral order and privacy they prefer. And they can engage more in communities whose moral order promotes those values that they share. (Reference is to informal social controls, not to formal, governmental controls.) However they cannot avoid the sociological laws of gravity: moral order rests in part on visibility of disapproved behavior, and *ipso facto* entails limiting privacy.

In addition, informal social controls are essential because the volume of transactions in a modern society is so large that there never can be enough accountants, inspectors, border guards, custom officials, and police to limit anti-social behavior to a level a free society can tolerate. Moreover, these official enforcers themselves need to be policed, as has long been captured in the refrain, Who Will Guard the Guardians? Hence, the only way a desired level of civility can be attained is if: (a) a large number of the members of society (including the law enforcement personnel) will "behave" because they believe that it is their civil or moral duty; and (b) a good part of the enforcement will be left to informal social controls which draw on limited privacy.

D. Virtual Community Ersatz

In earlier eras, when people lived in small communities, visibility was readily attained and social controls were regularly activated. With modernity, as communities grew in size and geographic mobility vastly increased, a great deal of visibility was lost and social controls were considerably weakened. Some sociologists hold that modern men and women lead an atomized life, bereft of social bonds, and hence, tend to engage in a high level of anti-social behavior that can be restrained solely by the state.

Actually, communities, albeit in a much attenuated form, can be found in many parts of modern societies. These include immediate and extended families, social bonds shared among those of the same ethnic or racial background (e.g. Chinatown, Spanish Harlem), those sharing in sexual orientation (e.g. Castro in San Francisco), vocation (e.g. academic

communities), and many others. And virtual communities supplement off-line interaction and are also able to form communities in their own right, complete with strong relationships among members.[26] Moreover, virtual communities have developed moral norms, such as principles of generalized reciprocity and assistance.[27]

Even in contexts of anonymity, which hinders social controls, virtual communities have developed tools that help enforce social norms. Informal social control by social exclusion is practiced to limit "flaming," the practice of posting or sending insults or inflammatory messages on the Internet.[28]

On Reddit, a social news website, users post Internet links and vote to indicate "like" or "dislike," which decides what content is displayed on the site.[29] Thus, if a user shares content that others find offensive, the virtual community has the tools to discourage them. The popular auction site, eBay, utilizes a rating system in which negative and positive reviews are aggregated and linked to a specific username, and users can respond to feedback they receive if they believe that it was unfair.[30] A study of this reputational system finds that these systems are effective at minimizing fraud. For example, 99.99% of eBay auctions occur without problems.[31] That is, even if the offline identity of the parties is not known, informal reputational systems can be quite effective, as long as behavior is visible to the community.

---

26. Paul DiMaggio, Eszter Hargittai, W. Russell Neuman, & John P. Robinson, *Social Implications of the Internet*, 27 ANN. REV. SOCIOLOGY 307 (2001); Dietland Stolle, *Trusting Strangers – The Concept of Generalized Trust in Perspective,* ÖZP (2002), http://www.oezp.at/pdfs/2002-4-02.pdf; Amitai Etzioni & Oren Etzioni, *Face-to-Face and Computer-Mediated Communities, A Comparative Analysis,* 15 INFO. SOC'Y 241 (1999); Gustave S. Mesch & Ilan Talmud, *Online Friendship Formation, Communication Channels, and Social Closeness,* INT'L J. INTERNET SCI., 2006, at 29.

27. Barry Wellman & Milena Gulia, *Net Surfers Don't Ride Alone: Virtual Communities as Communities*, (1997), http://groups.chass.utoronto.ca/netlab/wp-content/uploads/2012/05/Net-Surfers-Dont-Ride-Alone-Virtual-Community-as-Community.pdf; Lorne Tepperman & James Curtis, *Social Problems of the Future,* 8 J. FUTURES STUD. 21 (2003), http://www.jfs.tku.edu.tw/8-1/A03.pdf; Victoria Jobling, *Anonymity: The Default for Cyber-Bullies on Social Network*s, at http://networkconference.netstudies.org/2011/04/anonymity-the-default-identity-for-cyber-bullies-on-social-networks/.

28. David S. Wall & Matthew Williams, *Policing Diversity in Virtual Communities,* CRIMINOLOGY & CRIM. JUST., 2007, at 391.

29. http://www.reddit.com/.

30. Paul Resnick et al., *The Value of Reputation on eBay: A Controlled Experiment,* EXPERIMENTAL ECON., 2006, at 80.

31. Peter Kollock, *The Production of Trust in Online Markets,* (1999), http://www.connectedaction.net/wp-content/uploads/2009/05/1999-peter-kollock-the-production-of-trust-in-online-markets.htm; *see also* Sara Bartlett, *Trust Me! I'm on eBay,* at http://networkconference.netstudies.org/2011/04/trust-me-im-on-ebay/.

At the same time, there is little reason to doubt that informal social controls work best in the virtual world where one's virtual identity is connected to one's actual identity. Hence the importance of Facebook, which is used by more people than any other social media and requires participants to provide their "real" offline identity. Much has been made, quite properly, of the fact that people, especially young ones, post on Facebook (and elsewhere) much information on the assumption that it will be available only to select friends (low visibility, and hence relatively private), or without considering the privacy issue, or misunderstanding or misusing the complicated privacy protection measures Facebook and other sites provide.[32] Various harms are reported to follow and various changes have been made to better protect privacy in the virtual world.[33]

Much less attention is paid to the fact that, as a result, the virtual world has acquired more of the capacities typically possessed by offline communities to control anti-social behavior. When information on Facebook can affect one's ability to attain employment, gain admittance to college, run for public office, or be well regarded in their community—users are deterred from acting inappropriately, which would be much less the case if there was more anonymity. A minor esoteric example of the ways social controls work in the virtual world is found in the case of a married woman who accepted a "friend request" from a woman, only to discover from online pictures of her new friend that they in fact shared the same adulterous husband.[34] Many college admissions offices look at applicants' Facebook as part of the decision making process. Thomas Griffin, director of undergraduate admissions at North Carolina State University, told the *Wall Street Journal* that, "several applicants a year have been rejected in part because of information on social-networking

32. For a comprehensive analysis privacy concerns surrounding Facebook, including relevant law and policy, *see* James Grimmelman, *Saving Facebook,* 94 IOWA L. REV. 1137 (2009) (suggesting that three social imperatives—identity, relationships, and community—the lead people to engage in online social networks despite the risks to privacy this entails. It is essential to understand such social motivations in order to craft successful policies to protect users' privacy on sites such as Facebook); *see also* Peter Swire, *Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment,* 90 N. CAR. L. REV. 109 (2012) (discussing points to "substantial public concerns about privacy and social networks, growing policy discussions about possible regulatory limits, and increased enforcement actions).

33. Cecilia Kang, *Facebook Settles FTC Privacy Complaint, Agrees to Ask Users' Permission for Changes,* WASH. POST (Nov. 29, 2011), http://www.washingtonpost.com/business/technology/facebook-settles-ftc-privacy-complaint-agrees-to-ask-users-permission-for-changes/2011/11/29/gIQAqyJC9N story.html; Barbara Ortutay, *Facebook Takes Steps to Address Privacy Concerns,* HUFFINGTON POST (Mar. 23, 2012), http://www.huffingtonpost.com/huff-wires/20120323/us-tec-facebook-privacy/.

34. Manual Valdes, *Facebook "Friend" Request Exposes Man's Other Wife,* PITTSBURG POST-GAZETTE (May 9, 2012), http://www.postgazette.com/stories/news/us/facebook-friend-request-exposes-mans-other-wife-221701/.

sites."[35]

One may suggest that people will not improve their behavior but simply cease posting photos from their drunken parties or inflammatory texts on their Facebook account. However, they cannot prevent "friends" from posting group photos or texts. And the fact that people are willing to pay companies to scrub the Internet to preserve their reputation shows that they do in fact care.[36]

Anonymity is a form of privacy because it reduces visibility, which—to reiterate—is essential for ensuring political dissent, innovation, and individualization. However, given that most virtual forums of dialogue and interaction allow people to use an alias, anonymity has led to much more polarized, coarse, uncivil social platforms, often riddled with racist, sexist, homophobic and xenophobic expressions. Indeed, in the virtual world these forms of interaction dominate. By providing many more opportunities for validated identity interactions, the virtual world can be moved closer to the communal virtues of the real world and norms of more civil discourse will be encouraged. These observations should give a pause to those who promote more automatic (as distinct from opt in) privacy controls in those few social media that require disclosed identity. A nudge toward civility is called for here.

In short, virtual communities can and do provide some of the elements of "real" communities such as the informal social controls that limit the role of the state.[37] However, in this virtual realm these controls also require visibility and hence limit users' privacy. The controls seem to work best when people's identities online are connected to their offline identities.

III. THE LAW, INFORMAL CONTROLS, AND PRIVACY

So far this article has briefly visited several examples in which making more room for visibility in the social realm is expected to support the moral order and reduce the need for governmental coercive controls. In some other cases, public authorities can activate these controls or

35. John Hechinger, *College Applicants, Beware: Your Facebook Page Is Showing*, WALL ST. J. (Sept. 18, 2008), http://online.wsj.com/article/ SB122170459104151023.html.

36. An example of such a company is Reputation.com, http://www.reputation.com.

37. Others have made the case for the use of informal social control, "peer governance," as opposed to centralized regulatory systems, to prevent disruptive behavior on the Internet. "[A]llowing each individual to make his or her own decisions. . .regarding when and with who to connect" would enable "private parties to protect themselves against whatever they consider to be antisocial activity," without sacrificing "an Internet that reflects and tolerates diverse values." David R. Johnson, Susan P. Crawford, & John G. Palfrey, Jr., *The Accountable Internet: Peer Production of Internet Governance,* 9 VA. J. L. & TECH. 9, 15 (2004).

strengthen them, thus using the law to minimize the use of the law. Some brief examples follow:

A. Shaming

Those convicted of driving under the influence of alcohol in Fort Bend County, Texas were required to place "DUI" bumper stickers on their cars.[38] Another judge ordered a woman convicted of purchasing controlled substance in front of her children to place a notice in the local newspaper detailing her offense.[39] A man was ordered to place an ad in his local newspaper, accompanied by his photo, reading, "I am Stephen Germershausen . . . I was convicted of child molestation . . . If you are a child molester, get professional help immediately, or you may find your picture and name in the paper."[40]

Such shaming was criticized by the ACLU which protested that "gratuitous humiliation of the individual serves no societal purpose at all . . . and there's been no research to suggest it has been effective in reducing crime."[41] In his dissent in *United States v. Gementera*,[42] a case which upheld the legality of requiring an offender to wear a sign that specified his crime while doing community service, Justice Hawkins argued that "[w]hen one shames another person, the goal is to . . . dehumanize him. To affirm the imposition of such punishments recalls a time in our history when pillories and stocks were the order of the day."[43]

Such criticisms do not take into account that if one assumes that the offenses at issue cannot be simply ignored (none of the critics suggested better ways of dealing with them), the main alternative is to jail the offenders. This involves shaming in addition to the loss of liberty and the attending public and social costs. In short, shaming, which activates in-

38. Dan M. Kahan, *What do Alternative Sanctions Mean?*, 63 U. Chi. L. Rev. 635 (1996), cited in *Sentencing Lawbreakers to a Dose of Shame*, Civic Renewal (CQ Researcher), Mar. 21, 1997, at 252.

39. Jan Hoffman, *Crime and Punishment: Shame Gains Popularity*, N.Y. Times, Jan. 16, 1997, at A1, cited in *Sentencing Lawbreakers to a Dose of Shame*, Civic Renewal (CQ Researcher), Mar. 21, 1997, at 252.

40. Toni M. Mossaro, *Shame, Culture, and American Criminal Law,* 89 Mich. L. Rev. 1880 (1991); *see* Anne Marie McAlinden, The Shaming of Sexual Offenders: Risk, Redistribution and Reintegration at 42, 165 (Hart Publishing 2007).

41. Tony Allen-Mills, *American Criminals Sentenced to Shame*, Sunday Times, Apr. 20, 1997.

42. United States v. Gementera, 379 F.3d 596 (9th Cir. 2004).

43. *Id.*; Dan Kahan, who once wrote in favor of the court's use of shaming sanctions, recanted and now argues that "[w]hat's really wrong with shaming penalties. . .is that they are deeply partisan: when society pick them, it picks sides, aligning itself with those who subscribe to norms that give pride of place to community and social differentiation rather than to individuality and equality." Dan M. Kahan, *What's Really Wrong with Shaming Sanctions,* Yale L. Leg. Scholarship Rep., Paper 102 (2006), *http://digitalcommons.law.yale.edu/fss_papers/102.*

formal social controls and reduces the coercive controls, is a preferred method of promoting law and order for suitable offenses and offenders.[44]

B. Defamation (Libel and Slander)

In countries where it is relatively easy to be sued for defamation, people are less likely to censure and report or publish information about anti-social behavior for fear of inviting a lawsuit. This in turn hinders the activation of communal controls. Many believe this is the case in Great Britain, home to the "libel capital of the world." The relative ease with which authors, journalists and publishers can be sued for writing about sensitive information has weakened what would otherwise be a source of informal social control—critical investigative reporting. Free speech advocates claim "libel laws in England have really constrained and chilled speech for a long time," as wealthy individuals and companies are able to essentially buy off public scrutiny with the threat of a lawsuit.[45] The American way is often lauded on Free Speech grounds. The current analysis suggests that it is to be preferred also on the grounds that it helps to activate community and reduce the role of the state.[46]

C. Second Chances

The idea that people deserve a second chance is an important American value. It dates back to those who moved to the New World in search of a fresh start, and reflects the Judeo-Christian belief in redemption, as well as the therapeutic culture's notion that there are few inherently bad people. Because arrest records were retained in paper ledgers and reports of anti-social behavior were circulated mostly by local newspapers, visibility was limited and there was a sense of increased privacy. Therefore, the possibility of earning a second chance was more likely during these times.

---

44. Not all shaming sentences are created equal; according to the theory set out in John Braithwaite, Crime, Shame and Reintegration (Cambridge University Press 1989) ("societies have lower crimes rates if they communicate shame about crime effectively"). The author draws a distinction between reintegrative shaming, which "communicates shame to a wrongdoer in a way that encourages him or her to desist," and stigmatization which treat criminals as bad people—not people who have done bad things—and leads to more antisocial behavior. John Braithwaite, *Shame and Criminal Justice*, 42 Canadian J. Criminology 281, 282 (2000).

45. Eric Pfanner, *Britain to Seek Curbs to 'Libel Tourism'*, N.Y. Times (May 9, 2012), http://www.nytimes.com/2012/05/10/business/media/britain-to-seek-curbs-to-libel-tourism.html.

46. For a comparative discussion of libel law in the U.S. and Great Britain, *see* Richard Garnett & Megan Richardson, *Libel Tourism or Just Redress? Reconciling the (English) Right to Reputation with the (American) Right to Free Speech in Cross-border Libel Cases,* 5 J. Priv. Int'l L. 471 (2009).

The onset of the cyber age is charged with killing second chances as a source of privacy.[47] For example, by digitizing local public records, the Internet prevents people from throwing off their past. An individual's public records now follows him wherever he goes. As a result, Beth Givens, director of the Privacy Rights Clearinghouse, writes that Internet databases cause a loss of "social forgiveness."[48] Others find that when companies "rely on background checks to screen workers, [they] risk imposing unfair barriers to rehabilitated criminals."[49]

Data however strongly indicate that most convicted criminals did not use their second chance. For example, sixty-seven percent (67%) of prisoners released in fifteen states in 1994 were re-arrested for a new offense within three years.[50]

The National Practitioner Data Bank allows hospitals to find out whether a doctor's license has been revoked or the doctor has ever been disciplined. Generally, a doctor's license is revoked only if he commits a serious offense. Prior to online access to a doctor's revocation and discipline history, physicians who were disbarred in one state would move to another state in order to continue practicing and commit the same offenses. Few would consider continued obscurity of a doctor's past offenses good public policy. (Note that in this case, access to data bases is limited to those who consider retaining them. In effect, the preceding analysis of the moral order urges that their names be revealed to the general public.)

All of this is not to suggest that one should ignore those who can be rehabilitated or deny them their second chances. A mixture of technological and legal means can replace the measures that were once naturally woven into the fabric of communities. There are laws that protect the privacy of those who have repaid their debt to society from discrimina-

47. James Jacobs & Tamara Crepet, *The Expanding Scope, Use, and Availability of Criminal Records,* 11 N.Y.U. J. LEGIS. & PUB. POL'Y 177, 178-179 (2008) (referring to criminal records as a "negative curriculum vitae" and argue that the expanding "availability, use and scope of criminal records poses a serious challenge to reformers seeking to smooth the re-entry of ex-offenders into the community" and, ironically, may actually lead to *more* crime because "restricted socio-economic opportunities make reoffending more likely").

48. Kim Zetter, *Bad Data Fouls Background Check,* WIRED (Mar. 11, 2005), http://www.wired.com/politics/security/news/2005/03/66856?currentPage=all.

49. Ann Zimmerman & Kortney Stringer, *As Background Checks Proliferate, Ex-Cons Face a Lock on Jobs,* WALL ST. J. (Aug. 26, 2004), http://online.wsj.com/article/SB10934781 9251301442.html; *see* Brad Stone, *If You Run a Red Light, Will Everyone Know?,* N.Y. TIMES (Aug. 3, 2008), http://www.nytimes.com/2008/08/03/technology/03essay.html.

50. *Percent of Released Prisoners Returning to Incarceration,* CRIME IN AMERICA.NET (Sept. 29, 2010), http://crimeinamerica.net/2010/09/29/percent-of-released-prisoners-returning-to-incarceration.

tion in housing and hiring.[51] A criminal record could be sealed both locally and in online databases, say after seven years, if the person had not committed a new crime. A rehabilitated criminal's privacy could be returned to him when his deprivation of privacy would no longer be important for the public's safety and health.

Internet databases that rely on public records should be required to update as the public records update and be held accountable for mistakes in the database. Internet databases should make proper corrections in a timely fashion following a procedure similar to that of credit records and also provide mechanisms for filing a complaint if the online data is erroneous.[52]

All said and done, this article suggests that to the extent that communities are intact or can be activated and one can draw on informal social controls to enforce pro-social behavior, the role of the state and its coercive measures can be curtailed. This requires allowing some limitations on social privacy because communities can curb only the anti-social behavior that is visible to their members. Laws that shield individual privacy from members of their families and their communities should take into account this key observation, making appropriate adjustments.

IV. PUBLIC PRIVACY: REASONABLENESS UNPACKED

When communal processes fail or are inadequate, the state steps in—either on the side of privacy or the common good. The default position ought to be that privacy is vital for liberty, especially for political dissent, innovation, and the individualization which is essential for human flourishing. Yet the right to be secure is equally vital. Theoretically, a society could determine once and for all in its constitution the proper weight that should be accorded to each of these core values. However, neither rights nor security can be discussed in abstraction of the historical context, behind some kind of a veil of ignorance. Given the constant changes that societies face in their circumstances (e.g. the 2001 attacks on the American homeland), technological development (e.g. the

51. Kathryn Dugan, *New York Expands Employment-Related Protections for Individuals With a Criminal Conviction Record,* EMP. LAW MONITOR (Apr. 14, 2009), http://www.employmentlawmonitor.com/2009/04/articles/employment-policies-and-practi/new-york-expands-employmentrelated-protections-for-individuals-with-a-criminal-conviction-record/; Center for Community Alternatives, *Judicial Diversion: The Contract or Agreement Should Provide for Stealing,* CENTER FOR COMMUNITY ALTERNATIVES BLOG (Jun. 13, 2012), http://makingreformreality.blogspot.com/. For a review of New York's criminal record "sealing" rule, *see* George F. Carpinello, *Public Access to Court Records in New York: The Experience Under Uniform Rule 216.1 and the Rule's Future in a World of Electronic Filing*, 66 ALBANY L. REV. 1089 (2003).

52. Federal Trade Commission, *How to Dispute Credit Report Errors,* FED. TRADE COMM'N, http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre21.shtm.

rise of drones) and numerous other developments, the opposite is the case. Societies need to constantly re-triangulate the relationship between privacy and the common good.

In searching for criteria to judge whether the re-triangulation has to move the society's course in one direction or the other, a sociologist has great difficulties with the concept of the expectation of privacy. An individual's personal expectations of privacy are too weak to rely on. Those who relieve themselves in a swimming pool (if they are unaware of the urban legend) surely have a strong expectation of privacy; however, it is far from clear why this expectation of privacy should be respected. At the same time, those who speak in a sizeable political meeting may well not have an expectation of privacy; however, surely they should be protected from government surveillance under most circumstances to protect their privacy (among other reasons).[53]

With regard to society's expectation of privacy, a sociologist is keen to know which, if any, community will be polled to establish what this expectation is. The fact that judges seem free to assume they can rely on their sociological instincts as to what the community expects seems strange.[54] And sociologists would be quick to agree that the whole notion is circular. Mr. Katz has or does not have an expectation of privacy depending on what the court rules. All this has been said and much better by legal scholars.[55]

This in turn suggests the need for a macro Freudian-like analysis, which entails an examination of the subterranean forces that maintain this odd legal precept. Freud assumed that there are no accidents in personal life and behavior that seems abnormal or irrational serves some underlying cause. If such behavior is to be changed, this cause must be addressed. Freudian macro analysis suggests that the same is true for societal phenomena. Drug abuse, violent crime, and discrimination all

53. 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, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act,* 72 GEO. WASH. L. REV. 1557 (2004).

54. Morgan Cloud, *Symposium: Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendmen*t, 72 MISS. L.J. 5 (2002).

55. 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).

persist not because we are unaware of them or made no efforts to tackle them. They exist because we often address the symptoms rather than the root causes, make the wrong diagnoses of these subterranean causes, or do not have the needed resources or will/conviction to change them.

The expectation of privacy seems to persist in part because of the quest to move privacy from a protection of a space to that of a person. And to allow judges who seek to legalize a particular kind of search without warrants, to declare that there was no expectation of privacy and those judges who seek the opposite—to rule that there was.[56] Thus, four years after the Supreme Court ruled that the police had violated Katz's Fourth Amendment rights by bugging a pay phone without a warrant, the Court found that no warrant was needed to bug a phone conversation in a private home as long as one person approved of the wiretap.[57] This article suggests that both needs can be well served with the following criteria. The expectation of privacy as a legal precept is best allowed fading away through disuse and courts and policymakers' best look instead to the suggested criteria or some other such a set.[58]

A. Four Criteria For Re-Triangulation

In a previous exploration of privacy, this article tried to show that four criteria help form the framework for relevant public policies.[59] These are briefly revisited here and a contextual consideration is added. 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 terms "clear and present danger," despite the similarity, because they have a specific legal reference, not here followed.) 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.

56. Several legal scholars have written about the Supreme Court's movement away from *Katz v. United States* in its definition of what constitutes a "search." Peter Swire writes that current applications of the Fourth Amendment have "dramatically aided government surveillance" and suggests the Court work "collaboratively with the elected branches" to construct a more reasonable search and surveillance regime. *See* Peter P. Swire, *Katz is Dead. Long Live Katz,* 102 Mich. L. Rev. 904, 904-905 (2004).

57. Morgan Cloud, *Symposium: Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendmen*t, 72 Miss. L.J. 5 (2002).

58. Recently, some have suggested returning to a property-based conception of privacy in order to strengthen individual's power to control personal information in an increasingly digitized world. For a discussion on this topic *see* Pamela Samuelson, *A New Kind of Privacy: Regulating Uses of Personal Data in the Global Information Economy*, 87 Cal. L. Rev. 751 (1999) (book review); *see also* Jane B. Baron, *Property As control: The Case of Information*, 18 Mich. Telecomm. Tech. L. Rev. 367 (2012).

59. *See* Etzioni, *supra* note 1.

Hence the reluctance of the courts to reverse themselves and the criticism of elected officials who change their positions and are therefore depicted as "flip-floppers." Once tradition is breached, it is difficult to prevent it from unraveling, a phenomenon often referred to as the slippery slope. Changes, therefore, should not be undertaken unless there is strong evidence that either the common good or privacy has been significantly undermined. When the HIV/AIDS epidemic spread across the globe, killing more than two million people each year and infecting millions of others before medications were available that greatly ameliorated the disease and slowed its spread, it was such a condition.

The 2001 attacks on the American homeland—and the risk that they will be repeated and extended—fully qualify as such a well-documented and large-scale danger. To argue, as law professor Jonathan Turley did, "that all that happened was the destruction of two buildings and the killing of a number of people," may be a noble attempt to minimize the sense of threat to national security in order to protect rights, but lacks minimal sociological reality.[60] These attacks terrorized a nation by turning airplanes full of people into bombs, reaching into the heart of the national political, economic and communication centers, and threatening a nation that hereto felt secured by wide oceans. All this was through an attack carried out by a bunch of youngsters armed with no more than box cutters and a smaller budget than that of an indie movie. The notion that a larger number of people are killed by smoking, driving, and over eating disregards that these are the consequences of changes in behavior that were long established before their risks were understood; that they reflect in part people's choices; and are not imposed on the nation on a single morning, by foreigners. Both HIV and terrorist threats are deemed of an order that justified some new limitations on privacy. In contrast, the fears initially garnered by SARS in 2003 proved not to meet this criterion, nor did the killer bees that were said to swarm from Mexico in 1979.

Secondly, after determining that the common good needs shoring up, one best seek to establish *whether this goal can be achieved without introducing new limits on privacy*, by finding ways to advance the common good without violating 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. (Conversely, if privacy needs shoring up, one should look for ways to proceed that impose no "losses" to the common good. For instance, allowing the introduction of high power encryption

60. Jonathan Turley, *A Legal Perspective on Drone Strikes,* NATO Parliamentary Assembly, US Capitol, Jul 10, 2012.

for personal communications that include "trap doors" that enable authorities to read the messages, under approved conditions.)[61]

Thirdly, to the extent that privacy-curbing measures must be introduced, they should be *minimally intrusive*. 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.

In *United States v. Jones*, the Supreme Court used the duration of the surveillance as a criterion, holding that while short term monitoring might be tolerated, longer term monitoring should be banned.[62] A legal scholar scoffed at this criterion, suggesting that there is no magic point at which short turns to long. I suggest that the *scope* of intrusion is highly relevant because the more behavior and sensitive information is made visible, the greater the intrusion. The factors that determine scope include the duration of the surveillance as well as the range of information obtained and its sensitivity. Thus finding out the level of heat in a home entails extremely little intrusion compared to the surveillance of conversations, and finding the location of a car at a few points in time is much less revealing than tracking a person's cell phone location over long periods, and extremely less intrusive compared to a time in which already existing technology is used to monitor people's brain waves (if those are found out to truly reveal one's thoughts and feelings). Hence, this logic implies, an intrusion of the home that is limited in scope can be tolerated more readily than an expansive intrusion in a public space. Privacy, at least as here defined, is much more violated by prolonged tracking of public moves and eavesdropping than measuring the heat in one's kitchen.

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 infected individual about such exposure and the therapeutic and protective measures they ought

61. Philip Zimmerman, *Testimony of Philip R. Zimmermann to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation*, (Jun. 26, 1996), at http://www.philzimmermann.comEN/testimony/index.html.

62. United States v. Jones, 132 S.Ct. 945 (2012) (in his concurrence, Justice Alito wrote, "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy").

to next undertake, without disclosing the identity of the diagnosed person.

The application of these four balancing criteria helps to ensure that correctives to a society's course are both truly needed and not excessive. Granted, even when these criteria are applied, one cannot pinpoint with complete precision the proper or optimal course to follow. Societies have rather crude guidance mechanisms, and need to constantly readjust their course as they over-steer first in one direction and then in another.

One may suggest that the aforementioned four criteria provide for a social policy model and that the courts and legal scholars are concerned with what is constitutional.[63] For a sociologist this distinction is not sharply etched. The law is of course a very major tool of social policy. Surely, social policy should not be advanced if it violates the U.S. Constitution. And when the Constitution is interpreted in ways that lead to deeply troubling social policy, the nine wise persons entrusted with deciphering what is constitutional ought to, and surely do, revisit their previous interpretations of what is a living document. That is in effect what they did in overturning decisions made in cases such as *Korematsu v. United States* and *Plessy v. Ferguson*, and ought to do with *Citizen United*.[64]

A contextual consideration should be added. It might be called the "No Horse and Buggies Rule." It suggests that if those who endanger the public start using cars, one should not insist that the police continue to use only horses and buggies. The authorities should not be subject to technological lags compared to the criminals. A case in point concerns roving wiretaps.

Before 9/11, when the Foreign Intelligence Surveillance Court approved a warrant to tap a suspect's phone, that warrant was limited to a particular phone. This limitation reflected the days when most people had only one phone. After 9/11, taking into account that people use many communications devices, the PATRIOT Act revised this rule to allow the government to tap all the instruments of a given suspect in national security investigations.[65] Supporters point out that such wiretaps have long been allowed for other investigations (such as drug cases and racketeering) and argue that the measure simply updates federal law to a more technologically-advanced era.[66] Detractors, however, argue that

63. Orin S. Kerr, *Four Models of Fourth Amendment Protection,* 60 STANFORD L. REV. 503 (2007).

64. Korematsu v. United States*,* 323 U.S. 214 (1944); Plessy v. Ferguson, 163 U.S. 537 (1896); Citizens United v. Fed. Election Comm'n, 558 U.S. 50 (2010).

65. *The USA Patriot Act: Myth vs. Reality,* DEPT. JUSTICE, http://www.justice.gov / archive/ll/subs/add_myths.htm#s206.

66. *Id.*; Larry Abramson & Maria Godoy, *The Patriot Act: Key Controversies,* NPR (December 16, 2005), at http://www.npr.org/news/specials/patriotact/patriotactdeal.html.

such wiretaps violate the Fourth Amendment's requirement that a warrant "particularly describe the place to be searched" and could bring innocent people under the scope of a search (such as anyone who uses the same public library computer as the target of an investigation).[67]

Requiring the authorities to go to court and get a warrant for each instrument, for a person already proven to be a suspect and for whom there is probable cause to search his communications, simply makes the authorities lag too much behind those that threaten the common good, who are free to use all the new technologies the market brings up. It shall be seen later that there are ways to ensure that the authorities not abuse this and other such new powers.

Another case in point concerns national warrants. Historically, court-authorized warrants were local—that is, they specified the town or city in which the warrant could be administered. However, e-mails travel through several jurisdictions. Messages from one location are likely to be stored in another and some messages travel in disparate packets such that each travel their own route and must be collected in order to make sense. In response, the PATRIOT Act authorized what are in effect nationwide search warrants for electronic evidence.[68]

Even privacy advocates have not argued that this adaptation was unreasonable. The Electronic Frontier Foundation merely argued that this change in law allows the FBI to go "judge shopping"—that is, to seek out "only those judges least likely to say no" to a warrant request.[69] The Justice Department, for its part, notes that the "provision can only be used by courts with jurisdiction over the investigation," indicating that whatever "judge shopping" allegedly occurs can only happen within a range of judges already in a position to oversee the warrant requests.[70]

B. Within History

As already indicated, to proceed beyond the starting point that the community always faces multiple legitimate and not fully compatible concerns, one must ask whether there is a new threat to the common good (or to privacy)—that calls for recalibration of the prevailing balance between these two core values. This question cannot be answered abstractly, but must be examined within comparative and historical contexts. Thus, one may see a strong need for more privacy when considering political acts in China and in North Korea, but not necessa-

67. *USA Patriot Act*, Elec. Privacy Info. Center, http://epic.org/privacy/terrorism/usapatriot/.

68. *The USA Patriot Act: Myth vs. Reality, supra* note 65.

69. *Let the Sun Set on PATRIOT-Section 220: 'Nationwide Service of Search Warrants for Electronic Evidence,'* Elec. Frontier Found., http://w2.eff.org/patriot/sunset/220.php.

70. *The USA Patriot Act: Myth vs. Reality, supra* note 65.

rily when one deals with financial contributions to elections via the not-for-profit arms of super PACs in the contemporary U.S.[71]

In considering the present understanding of the right to privacy, historical context is particularly relevant. In the West, individual rights advocacy increased with the rise of new societal groups who had previously been oppressed by authoritarian monarchies and overbearing churches. The room for individual expression and variance of conduct (especially what was considered "deviance") was further suppressed by social pressures in the strong conformist small villages in which most people lived ("Salem" stands as an evocative symbol of this life). The rise of individualism, liberalism, and the concept of rights—especially the right to privacy—served to legitimate political action that sought to roll back the authoritarian rule that blanketed most people's lives in the Middle Ages in Europe. These same conditions can be found today in places such as North Korea and Saudi Arabia. In these polities the tilt against privacy clearly calls for the opposite re-triangulation, for curtailing the role of the state and moving the law and public policies to enhance individual rights, including privacy.

As of the 1960's, the moral order of the western societies has been undermined. However, no clear, new shared norms have emerged. In some cases the common good has been undermined by excessive attention to rights, particularly privacy. Those who bristle at this wording should revisit the case of hundreds of infants born with HIV, who could have been spared the ravages of AIDS but were not, and died, in order to protect the privacy of the mothers.[72]

Liberal democratic polities function best when they continually re-examine their laws and public policies and adjust them in response to changes in historical circumstances —to correct what was wrought by previous over-correction. This is necessary because societies have rather poor guidance systems and tend to over steer first in one direction and than in the other, stumbling like a drunken sailor through history. Thus, the Church and Pike Committees investigated abuses by the CIA, FBI and NSA in the mid 1970s, 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."[73] The Church Committee brought to light "Project Shamrock," a domestic surveillance program initiated under President Truman as part of a WWII censorship, which continued to operate into

71. For more discussion, see arguments for and against The Democracy Is Strengthened by Casting Light On Spending in Elections Act (DISCLOSE) Act.

72. Amitai Etzioni, *HIV Testing of Infants: Should Public Health Override Privacy?, in* THE LIMITS OF PRIVACY (1999) at 17-42.

73. *Post-Watergate Intelligence Investigations*. http://www.maryferrell.org/wiki/index.php/PostWatergate_Intelligence_Investigations.

the mid-1970s. The NSA monitored and collected communications sent by American citizens to international organizations.[74] The FBI was found to have engaged in "covert action designed to disrupt and discredit the activities of groups and individuals deemed a threat to the social order," such as the Southern Christian Leadership Conference and the anti-Vietnam War movement.[75]

In response to these reports, Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA) and created the Foreign Intelligence Surveillance Court, which is responsible for issuing warrants to permit domestic surveillance of American citizens by the U.S. government.[76] It led to a cultural change at the intelligence agencies by putting in place internal legal controls "requiring layers of attorneys to sign off on any possibly questionable activities."[77]

According to several reports, the reforms introduced in wake of the Church and Pike committees, and additional rules set by the agencies themselves, over-corrected the previous imbalance; they were one major reason that information available to some FBI agents and Bureaus was not transmitted in ways that could have prevented the 9/11 attacks. The 9/11 Commission Report found that the (sometimes incorrect) interpretation of FISA over the years created inter-agency intelligence sharing procedures that came to be known as "the wall" and the perception in the FBI, CIA and NSA that no intelligence information could be shared with other agencies and local police departments.[78]

After 9/11, the PATRIOT Act was enacted in a great rush and, according to its critics, curtailed 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.[79] The question that now must be faced is whether the American law and public policies currently tilt too far in one

74. *The Church Committee and FISA*, PBS (Oct. 26, 2007), http://www.pbs.org/moyers/journal/10262007/profile2.html.

75. U.S. Senate, 6 SELECT COMMITTEES TO STUDY GOVERNMENT OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, 94th Cong. (1976), http://archive.org/details/finalreportofsel06unit; For a comprehensive overview of the origins and developments of the Foreign Intelligence Surveillance Act, and suggestions on how its procedures could b reformed and oversight increased, *see* Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 G.W. L. REV. 1306 (2004).

76. The Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-1812 (2006).

77. Christopher Hayes, *Dealing With the Secret Government*, CBS NEWS (Aug. 27, 2009), at http://www.cbsnews.com/2100-215_162-5269340.html.

78. *The 9/11 Commission Report* (Washington: Government Printing Office, 2004) at 79.

79. 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).

direction or another, and in which direction they should be re-triangulated. This Article suggests next that not all-current developments call for the same adjustments.

C. GPS as a Police Tool

The police attached a GPS to the car of a suspected drug dealer. The Supreme Court, in the case *United States v. Jones,* unanimously ruled that this was a violation of his privacy. A liberal communitarian would point out that according to the first criteria, that of potential harm to the public, the data indicate that citizens do need to attend more to public safety. According to national statistics for 2010, fewer than half (47 percent) of violent crimes committed in this country are "cleared" (that is, suspects are arrested, charged, and turned over for prosecution) and only one out of five (18 percent) criminals who commit nonviolent crimes (such as burglary) are caught and tried. Second, there are obviously no voluntary ways to affect the same results. Third, the intrusion involved is fairly minimal. Reference is only to cars that travel in public spaces, in which they are already required to identify their owners (by displaying license plates) and are subject to police visual surveillance without warrants.

True, more than eyeballing is involved, because the device must be attached to the car. However the attachment is outside the vehicle (unlike a "spike mike" driven into the wall of a home, in the case *Silverman v. United States*)[80] and it reveals only the location of the car, not what is said or done in it. Moreover, tracking it can be turned off once the car enters a private space.[81] The scope of intrusion is limited and it should hence be allowed.

D. CCTV: Minimally Intrusive

Privacy advocates often suggest that whatever new measures the government introduces to enhance homeland security, public safety, or public health, are not effective.[82] However, when one demonstrates that the measures are reasonably effective, privacy advocates merely turn to other arguments to oppose them. Following the introduction of closed

80. Silverman v. United States, 365 U.S. 505 (1961).

81. Some argue that it is the fact that tracking cars reveals multiple locations over a long period of time (Jones' car was tracked for 28 days) that makes GPS an unacceptable invasion of privacy. *See* Christopher Slobogin, *Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 Duke J. of Const. L. & Pub. Pol'y 1 (2012).

82. In a debate between the head of the ACLU at the time, Nadin Strossen, and the author, Ms. Strossen was asked if she ever found any such measure she approved. Her first response was a curt "no." She then amended it to indicate that she could think of one, thickening the doors that separate the pilot cabin from that of the airline passengers.

circuit TV (CCTV) on a large scale, privacy advocates argued that CCTV did not produce any benefit to security and grossly violated privacy. Thus, Jeffery Rosen, who flew to London to study the matter, reported that while surveillance cameras were originally "justified as a way of combating terrorism, they soon came to serve a very different function."[83] Instead of catching terrorists and serious criminals, CCTV was more often used to target traffic offenders, car thieves, pickpockets, punks at the mall, and, when young male officers got bored, to zoom in on attractive women and "boyfriends and girlfriends making out in cars."[84]

Yet, CCTV has led to the arrest of terrorists, serious criminals, and contributed to significant decreases in crime rates in well-monitored areas. In Airdie, Scotland, "crimes of dishonesty," such as house and car break-ins, vehicle theft, and shoplifting, decreased by forty-eight percent after the installation of CCTVs.[85] In Newcastle, burglaries fell by fifty-six percent and criminal property damage by thirty-four percent in areas covered by CCTV.[86] A study that evaluated public surveillance systems in Washington, D.C., Baltimore and Chicago found that "in places where cameras were sufficiently concentrated and routinely monitored by trained staff, the impact on crime was significant and cost-beneficial, with no evidence of crime displacement."[87]

In the 1977 Oklahoma City Bombing, surveillance shows a Ryder truck parked near the federal building minutes before it exploded. Authorities were able to recover the truck's axel and trace it back to a body shop, whose owner identified Timothy McVeigh as the man who rented it.[88] In the trials that followed the July 7th, 2005 suicide bombings in the London transport system, the jury was shown CCTV footage that shows the defendants meeting with the suicide bombers and carrying out recon-

83. Jeffrey Rosen, *A Cautionary Tale for a New Age of Surveillance*, N.Y. TIMES (Oct. 7, 2001), http://www.nytimes.com/2001/10/07/magazine/07SURVEILLANCE.html?pagewanted=all.

84. *Id.*

85. Emma Short & Jason Ditton, *Does Closed Circuit Television Prevent Crime? An Evaluation of the Use of CCTV Surveillance in Airdie Town Centre,* (1998), http://www.scotland.gov.uk/Publications/1998/12/978abe73-d412-4ea3-86a7-e5acf24c8d7a.

86. *CCTV: Constant Cameras Track Violators,* 249 NAT. INST. JUST. J. 17 (2003).

87. Public surveillance technology such as Geographic Information Systems and improved cameras and systems are established as a capable crime preventer and investigative utility, and it is argued that the only reason why it isn't perceived as more successful is because the methods used for studying it limit the results obtained. *See* Nancy G. La Vigne, Samantha S. Lowry, Joshua Markman, & Allison Dwyer, *Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention,* URBAN INSTITUTE (2011), http://www.urban.org/publications/412403.html.

88. Steven Bryan, *Oklahoma City Bombing Facts and Figures*, YAHOO NEWS (Apr. 15, 2011), http://voices.yahoo.com/oklahoma-city-bombing-facts-figures8300355.html?Cat.

naissance missions.[89] CCTV footage captured the images of the 9/11 hijackers, allowing officials to identify them.[90] A day after the suicide bus bombing in Bulgaria that killed seven Israeli tourists, Bulgarian police were able to identify the suspected terrorists using images from CCTV footage.[91]

Considering the second criteria for limiting privacy, the availability of voluntary alternatives, it is clear that there is no way to accomplish these same goals through communal means. Indeed, when it was suggested in 2002 that members of the community should act as eyes and ears of the government, which would reduce the need for CCTVs, a storm of opposition from privacy advocates followed. The program, Operation Terrorism Information and Prevention System (TIPS), was eliminated from the Homeland Security Act, leaving turf to governmental surveillance.[92]

As long as CCTV equipment is aimed at specific public spaces, and the public is notified that it is being observed, its intrusiveness is limited. The physical intrusion of CCTV is minimal (for instance compared to stop and frisk and body scanners) and no less intrusiveness can be achieved as long as public spaces are to be surveyed by machines. All this changes if one merges the feed of many thousands of CCTVs in a city into one super-database, which allows law enforcement to track people day and night, a system now being tested in New York City.[93] This is especially true if the capacity of CCTV is expanded to include voice surveillance. The scope of intrusion becomes so omnipotent that such a system should be turned on only when the level of danger is very high, such as when authorities are searching for a known terrorist who is loose in a given city. In short, by the criteria established above, the limitations on privacy posed by localized CCTVs seem to qualify as reasonable.[94]

E. Screening Gates and Body Scanners: Voluntary

When screening gates were first introduced in 1972, the ACLU ar-

89. *Jury Sees 7/7 Bombing CCTV Images,* BBC (May 1, 2008), http://news.bbc.co.uk/2/hi/uk_news/7377649.stm.

90. *Video Shows 9/11 Hijackers' Security Check*, USA Today (Jul. 21, 2004), http://www.usatoday.com/news/washington/2004-07-21-attacks-surveillance-dulles_x.htm.

91. Phoebe Greenwood, *Bulgarian Police Release Images of Suicide Bombing Suspect*, Guardian (Jul. 19, 2012), http://www.guardian.co.uk/world/2012/jul/19/bulgaria-bombing-police-release-footage.

92. Nat Hentoff, *The Death of Operation TIPS*, The Village Voice (Dec. 17, 2002), http://www.villagevoice.com/2002-12-17/news/the-death-of-operation-tips/1/.

93. Joe Coscarelli, *The NYPD's Domain Awareness System Is Watching You*, N.Y. Mag. (Aug. 9, 2012), http://nymag.com/daily/intel/2012/08/nypd-domain-awareness-system-microsoft-is-watching-you.html.

94. Different issues may arise when the person being targeted by surveillance is considered suspicious. *See* Slobogin, *supra* note 81.

gued that they were ineffectual.[95] Actually, they stopped skyjacking. In the four years leading up to the implementation of universal airport screening in 1973 there were 109 (roughly twenty-seven per year) aircraft hijackings in the U.S. In 1973, there were two, and while there was an uptick in the early 1980's, there were no successful skyjackings from 1992-2000.[96]

These gates gained much more application after the 2001 attack on American homeland. After additional attempts were made to blow up airlines full of civilians in 2010, major American airports introduced backscatter and millimeter-wave sensing devices (popularly known as full body scanners) that check whether people hide forbidden objects under their clothes. Privacy advocates refer to them as "virtual strip-searches."[97]

The ACLU stated that "some experts have said explosives can be hidden by being molded against the human body, or in folds of skin, and British newspapers are reporting that government testing in the UK found that the technology comes up short in detecting plastic, chemicals and liquids."[98] Putting aside the question of whether these matters should be settled on the basis of what the notoriously unreliable British newspapers report, one notes that this argument about lack of effectiveness—the same type that the ACLU applies to nearly every security measure—does not answer the question of how much security the scanners add. And, if it turns out that they are quite effective, the privacy advocates merely turn to other arguments.

Most importantly, the body scanners are a voluntary measure. People are free to choose a pat-down rather than pass through the millimeter-wave machine, and even then about seventy percent of Americans say they prefer to be scanned. (The option of choosing a pat-down should not be considered unduly coercive, because random pat-downs were mandatory before the installation of body scanners—and even civil libertarians stopped arguing that there should be *no* scrutiny at all of those who are about to fly.)

Turning to the third criteria, the intrusiveness of the scanners is much smaller than often claimed. In order to illustrate how intrusive they are, privacy advocates display a rather graphic image obtained from a scanner (*see* left frame below). Yet, this image is not of an airline pas-

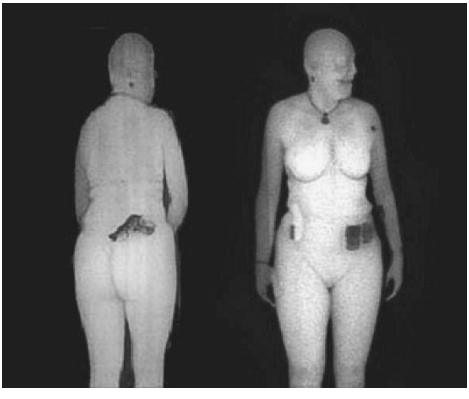
95. *Is Liberty Lost During Emergencies?* UNITED States Senate Republican Policy Committee Report, Nov. 7, 2011, http://rpc.senate.gov/releases/1999/cv110701.htm#N_6_.

96. *Id.*

97. *ACLU Backgrounder on Body Scanners and "Virtual Strip Searches"*, ACLU (Jan. 8, 2010), http://www.aclu.org/technology-and-liberty/aclu-backgrounder-body-scanners-and-virtual-strip-searches.

98. *Id.*

senger but of a TSA employee who volunteered to test the machine. The actual images are much less graphic. See on the right side.



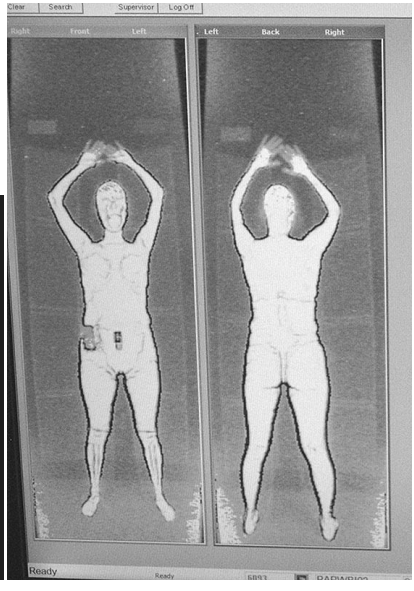


Image used by the ACLU[99] Actual image seen of passengers by TSA agents[100]

Moreover, the images of passengers that actually appear on TSA screens are much less revealing, because the scanners are equipped with two kinds of privacy filters.[101] One conceals the genitals and the other the face. (What's more, new scanner software replaces the realistic images of the passengers who are being scanned with a cartoon of a generic, clothed body, and marks areas that should be checked further.[102] This software is currently being tested.) Further preserving privacy, TSA staffers who view the images are in a separate room and are unaware of the identity of the passenger who is screened.[103]

---

99. *"See Through" Body Scanners,* ACLU (Jun. 3, 2008), http://www.aclu.org/technology-and-liberty/see-through-body-scanners.

100. *Airport security full body scanners: up close and personal,* THE BAY AREA TRAVELER (Jun. 15, 2010), http://thebat-sf.com/2010/06/15/airport-body-scanners-up-close-and-personal/.

101. *Frequently Asked Questions: Advanced Imaging Technology,* TSA, http://www.tsa.gov/approach/tech/ait/faqs.shtm.

102. David G. Savage, *The Fight Against Full-body Scanners at Airports,* L.A. TIMES (Jan. 13, 2010), http://articles.latimes.com/2010/jan/13/nation/la-na-terror-privacy13-2010jan13.

103. *You asked for it. . .You got it, Millimeter Wave images*, TSA BLOG (May 9, 2008), http://blog.tsa.gov/2008/05/you-asked-for-ityou-got-it-millimeter.html.

Finally, the Electronic Privacy Information Center (EPIC), in its critique of scanners, states that new security measures "present privacy and security risks to air travelers because they might create data files directly linked to the identity of air travelers. These files, if retained, could provide the basis for a database of air traveler profiles."[104] *The New Republic*'s Jeffrey Rosen argues that "the greatest privacy concern is that the images may later leak."[105] Other privacy advocates hold that the radiation involved may harm one's health. Yet these hypothetical concerns pale in comparison to the possibility that terrorists might bring down another airplane, or worse.

In short, screen gates in general and full body scanners in particular seem to qualify as effective new tools of homeland security if judged by the communitarian criteria set out. The use of these security measures is in the public's interest, poses very limited harm, contributes to security, has a limited scope of intrusion, and is in part voluntary.

F. Drones: Excessive Intrusion

The domestic use of drones, also known as "unmanned aerial vehicles" (UAVs) by law enforcement agencies "passes" the first and second criteria but faces very serious challenges on the basis of the third one. Drones are an effective response to the new security challenges posed by 9/11 and well serve public safety and other common good purposes. For instance, in North Dakota a drone was used for surveillance purposes to assist in the arrest of a man engaged in an armed standoff with police after he refused to return six cows that had wandered on to his ranch to their rightful owner. The drone flew over the property (in public, navigable airspace) to make sure the man was still present and unarmed prior to the launching of the arrest raid.[106] There are clearly no other voluntary measures that could provide anything that approaches the level of surveillance drones provide.

However, drones fail to meet the third criteria because they are much more intrusive than other means that enhance public safety. At first it may seem that the main reason for the preceding statement is that drones can readily survey spaces hereto considered private or semi-private such as one's backyard, roof tops, verandas, and space greatly removed from public thoroughfares. Drones differ from other security

104. *Whole Body Imaging Technology and Body Scanners ("Backscatter" X-Ray and Millimeter Wave Screening),* Elect. Privacy Info. Center, http://epic.org/privacy/airtravel/backscatter/.

105. Jeffrey Rosen, *Nude Awakening: The Dangerous Naked Machines,* The New Republic (Jan. 29, 2010), http://www.tnr.com/article/politics/nude-awakening?page=0,1.

106. Jason Koebler, *Court Upholds Domestic Drone Use in Arrest of American Citizen*, U.S. News (Aug. 2, 2012), http://www.usnews.com/news/articles/2012/08/02/court-upholds-domestic-drone-use-in-arrest-of-american-citizen.

cameras in that they do not only monitor public spaces, but "can see any area visible from the air," including private residences.[107] However, the same can be said about planes and helicopters. And the U.S. Supreme Court has held that individuals may be surveyed by manned aircraft without a warrant because any person could (theoretically) observe anything in the open from the "public navigable airspace."[108] However, the Supreme Court also ruled in 2001 that "the use of a device that is not in 'general public use' is a search even if it does not physically invade the home."[109] Because most people do not utilize UAVs on a regular basis, the use of drones or UAVs to collect information without a warrant may therefore qualify as an unlawful search.[110]

Privacy advocates are also concerned that drones may soon be equipped with video or infrared cameras, heat sensors, GPS, sensors that detect movement, automated license plate readers[111] and even with technology to intercept wireless communications, all of which would greatly exceed the minimal intrusion condition.[112] Further, it may be possible to equip drones with facial recognition technology linked to catalogs of identification information such as the FBI Next Generation Identification database, which would give the government or private corporations new powers to track individuals.[113] However, the same is true about manned flying machines and even blimps.

The main intrusiveness of drones arises from two other factors. First and foremost, unlike piloted aviations systems, which can briefly pass or linger above any one space, drones can readily provide surveillance for many hours, continuously. Indeed, there are no technical difficulties in using them to provide non-stop surveillance. This is a very major quantitative leap from the use of piloted aviation systems. Also, drones, unlike UAVs, are as a rule invisible and often inaudible to those subject to their scrutiny. That means that individuals must assume that they may be under surveillance at all times, without notification or warning (the kind

107. Ryan Calo & John Villasenor, *Ten Myths About Drones*, HUFFINGTON POST (May 22, 2012), http://www.huffingtonpost.com/ryan-calo/drones-myths_b_1537040.html.

108. Benjamin Wittes & John Villasenor, *Regulating Domestic Drones on a Deadline*, WASH. POST (Apr. 19, 2012), http://www.washingtonpost.com/opinions/faa-regulation-of-drones-will-challenge-our-privacy-expectations/2012/04/19/gIQA9IH8TT_story.html; *see* California v. Ciraolo, 476 U.S. 207 (1986); *see* Florida v. Riley, 488 U.S. 455 (1989).

109. *Kyllo*, 533 U.S. at 27.

110. *Unmanned Aerial Vehicles (UAVs) and Drones*, ELEC. PRIVACY INFO. CENTER, http://epic.org/privacy/drones/.

111. *Open Letter to Michael P. Huerta (U.S. Federal Aviation Administration),* ELEC. PRIVACY INFO. CENTER (Feb. 24, 2012), http://epic.org/privacy/drones/FAA-553e-Petition-03-08-12.pdf.

112. M. Ryan Calo, *The Drone as a Privacy Catalyst*, 64 STANFORD L. REV. 29 (2012).

113. *Open Letter to Michael P. Huerta*, *supra* note 111.

CCTV provides) in all places but inside one's home or workplace (but only as long as the shades are drawn and the shutters closed).

These observations suggest that drones be banned from routine security use and their use limited to exceptional cases, such as finding missing people, watching for natural disasters, and when there are firm indications that there is a major security threat (e.g. when the national alert level is raised) or probable cause demonstrated in a court of law. Congressman Landry (R-LA) has introduced an amendment to the National Defense Authorization Act that prohibits the introduction into court evidence collected by drones without a warrant.[114] The amendment passed, and since then, additional bills stipulating the same have been introduced in both houses of Congress.[115] Government officials claim that they would obtain a warrant before utilizing UAVs to survey residents of the United States.[116] These steps seem to be moving in the direction that a liberal communitarian analysis favors.[117] In short, although drones can rather effectively serve a major common good, and there are no voluntary substitutes, their intrusion is so exceptionally high that their employment should be limited to situations in which there is a particularly strong and urgent public need, or where each application is first subject to a review by a court.

G. Medical Information: More Privacy Needed

The same criteria that were used to justify granting more leeway to the common good and limiting privacy in most of the cases above—lead to the opposite conclusion in the case of medical privacy. Health and medical records deserve special protection not only because they contain the most intimate details of an individual's self, but because in the hands of the wrong people (e.g. potential employers), such information can lead to unfair discrimination and have significant financial consequences. In the past, gross violations of privacy in this realm—some of which were perfectly legal at the time—were all too common. Important steps have since been taken to strengthen privacy protections. But in the face of technological advances that have transformed the way health records

114. *Amendment to the Rules Committee Print of H.R. 4310*, 112th Cong., 2nd Sess., at http://www.rules.house.gov/amendments/LANDRY_097_xml51512090055055.pdf.

115. *See* Preserving Freedom from Unwanted Surveillance Act of 2012, H.R. 5925, 112th Cong. (2012); Preserving Freedom from Unwanted Surveillance Act of 2012, S.R. 3287, 112th Cong. (2012).

116. Darrell Preston, *Drones Take To American Skies On Police, Search Missions,* Bloomberg (May 31, 2012), http://www.bloomberg.com/news/2012-05-31/drones-take-to-american-skies-on-police-search-missions.html.

117. *See* Calo, *supra* note 112. This discussion points to the possibility of unmanned drones being used domestically, and how this new development in security may catalyze a dramatic modernization of privacy law.

are stored and shared, government and industry officials must be vigilant in maintaining up-to-date security and health employees trained to properly use new technologies.

Before 2003, major violations of the most intimate and sensitive kind of privacy, that of information about one's medical conditions, were surprisingly common—with no benefits for the common good. Some involved the unauthorized use of medical information. A database created by the state of Maryland in 1993 to keep the medical records of all its residents for cost containment purposes was illegally sold by state employees to representatives of health maintenance organizations (HMOs). In Florida, a state health department worker using state computers compiled a list of 4,000 people with HIV and forwarded it to two newspapers.[118] When a woman from New York was running for Congress in 1992, someone obtained hospital records that detailed her attempted suicide and leaked it to the press.[119]

Often legal, before 2003, but equally damaging to medical privacy was a systematic flow of medical information from the health insurance and management corporations to other parties, including employers, marketers, and the press. For example, thirty-five percent of Fortune 500 corporations drew on personal health information, stored in their self-insurance divisions, in making employment decisions.[120] A 1996 study by Harvard and Stanford found 206 cases of genetic discrimination against asymptomatic individuals who suffered loss of employment, loss of insurance coverage, or ineligibility for insurance based on their potential for disease gleaned from personal genetic tests.[121]

Much of such use of personal medical information became illegal in 2003 when the Standards for Privacy of Individually Identifiable Health Information (also know as the "Privacy Rule") were implemented as part of the federal Health Insurance Portability and Accountability Act (HIPAA), which passed in 1996. The rule regulates the use and dissemination of Protected Health Information (PHI) and limits the circumstances when such information can be disclosed without patient

118. Doug Stanley & Craig S. Palosky, *HIV Tracked on Unauthorized Lists*, TAMPA TRIB., Oct. 3, 1996, at 1.

119. Christine Gorman, *Who's Looking at Your Files?* Tim *HIV Tracked on Unauthorized Lists,* May 6, 1996, reprinted in Robert Emmet Long, ed., RIGHTS TO PRIVACY (New York: H. W. Wilson Co., 1997), 81-84.

120. U.S. Congress, OFFICE OF TECH. ASSESSMENT, OTA-BP-BA-67, MEDICAL MONITORING AND SCREENING IN THE WORKPLACE: RESULTS OF A SURVEY (1991); David F. Linowes, A *Research Survey of Privacy in the Workplace* (Apr. 1996) (unpublished paper, on file with the University at Urbana-Champaign).

121. E. Virginia Lapham, Chahira Kozma, & Joan O. Weiss, *Genetic Discrimination: Perspectives of Consumers,* 274 SCI. 621, 624 (1996).

authorization.[122] Some additional steps in this direction are included in the American Recovery and Reinvestment Act of 2009. The law further limits the sale and use of medical records for marketing and fundraising, and grants individuals the ability to track accidental or purposeful disclosures of their records by requiring doctors to keep "audit trails."[123]

There are reasons to further extend these protections. Too many health care facilities do not adequately protect their data banks. The Chicago Tribune reported in April 2012 that since 2009, "400 large health care breaches affecting at least 500 people and more than 50,000 smaller breaches have been reported to the federal government." Five million people were affected when a computer was stolen at TRICARE, a health program for members of the military, and 250,000 individuals in Illinois have had their private health data exposed between 2009 and 2012.[124] Because it is often difficult to trace the source of online information leakage, policy researchers recommend a "traitor-tracing scheme. . .that facilitates digital forensics following the illegal copying and redistribution of digital media data."[125] Stronger enforcement is also needed. In the four years after the implantation of the Privacy Rule, 350 complaints were filed, of which only four were prosecuted by the Department of Justice and as of June 2012 only fifteen cases of HIPAA violations have led to court settlements, penalties, or criminal convictions.[126]

The 2009 Affordable Care Act also requires "Health Information Exchanges" (HEIs) that allow health care providers to share medical records electronically which they will do by partnering with private companies like Microsoft and General Electric. One software security expert raises the concern that a national network such as this would be vulnerable to attacks that compromise privacy and worries about Microsoft having "a near-monopoly controlling the overwhelming majority of sys-

122. *Summary of the HIPAA Privacy Rule,* U.S. DEP'T OF HEALTH HUM. SERV., http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html; Alexandra Podrid, *HIPAA—Exceptions Providing Law Enforcement Officials and Social Service Providers Access to Protected Health Information*, 16 NAT'L CENTER FOR PROSECUTION OF CHILD ABUSE 4 (2003).

123. *HIPAA Privacy & Security Audit Program*, U.S. DEP'T OF HEALTH HUM. SERV., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html.

124. Deborah L. Shelton*, Health Records Lost, Stolen or Revealed Online,* CHI. TRIB. (Apr. 23, 2012) http://articles.chicagotribune.com/2012-04-23/news/ct-met-health-data-breaches-20120423_1_breaches-health-privacy-health-care.

125. Azadeh Nematzadeh & L. Jean Camp, *Threat Analysis of Online Health System,* PROCEEDINGS OF THE 3RD INTERNATIONAL CONFERENCE ON PERVASIVE TECHNOLOGIES RELATED TO ASSISTIVE ENVIRONMENTS, 31 (2010), at http://dl.acm.org/citation.cfm?id=1839294.1839331.

126. Doreen Z. McQuarrie, *HIPPA Criminal Prosecutions: Few and Far Between*, U. HOUSTON L. CENT. (2007), http://www.law.uh.edu/healthlaw/perspectives/2007/(DM)HIPAACrimCharges.pd; *HIPAA Convictions/Fines/Settlements,* HIPAA Security and Privacy, at http://www.hipaasecurityandprivacy.com/p/convictions-fines.html.

tems."[127] Other experts say concerns are overblown, but agree that HEIs do indeed increase security risks and that "[t]he key is to build them right, with appropriate security and privacy controls, standards and policies, from the very beginning."[128] States are required to join an exchange by 2014, so it is pivotal that rushing to meet that deadline does not sacrifice investing in the strengthened security technology and worker training needed to prevent large-scale breaches of privacy.[129]

In sum, to determine what constitutes reasonable law and public policy, considering whether privacy or common good concerns are to be privileged, would benefit if four criteria are employed: the scope of the threats to the common good, whether these can be satisfied by voluntary measures, whether the proposed intrusion is minimal, and whether attention is paid to mitigating the side effects. Such continuous reevaluation of the nation's legal positions and public policies is needed because societies at any given time tend to over-steer in one direction or the other. Currently, the American system seems to require corrections that do not all point in the same direction. In some areas new technologies call for granting more weight to the common good, in others—to privacy protection.

V. THE SURVEILLANCE OF SURVEILLANCE, A CYBERNETIC PERSPECTIVE

Societies are cybernetic systems in the sense that they have overlays that guide the layers of action, somewhat like nerves are used to guide muscles.[130] When these overlays are too weak, they allow for actions that damage both rights and the common good such as wide spread corruption, crime, and abuse. When they are overwhelming, they tend to retard action, suppress innovation, and slow adaptation to historical changes. Hence, in addition to seeking the proper course of action—for instance, between maximum privacy and maximum security—societies need to find the proper balance between action and guidance (which include not merely consensus building, elections, and policy making but also oversight and accountability). In liberal democracies guidance tends to be deficient, hence it is the focus of the following discussion. It is es-

127. Taylor Amerding, *Health exchange privacy concerns overblown, experts say,* CSO (Aug. 16, 2012), http://www.csoonline.com/article/713846/health-exchange-privacy-concerns-overblown-experts-say.

128. *Id.*

129. *See* Gina Stevens, CONG. RESEARCH SERV., R41756, PRIVACY PROTECTIONS FOR PERSONAL INFORMATION ONLINE (2011). The differences between new privacy and security health risks to online health systems are defined, and a traitor-tracing solution is offered to counter the risks in order to ensure that electronic health records become a viable option for databases.

130. *See* AMITAI ETZIONI, THE FREE SOCIETY (1971).

sential because there is an inverse relation between commanding sufficient guidance and limiting the latitude one can grant to state's action. The more the government action is properly supervised, the more the government is accountable and can be trusted—the more one can assume that whatever additional powers it is granted will be use only for legitimated purposes—the more communitarian triangulation can tilt in favor of the common good.

The issue is illustrated by considering the use of the E-Z Pass. These passes can be employed and a very high measure of privacy can still be maintained—if immediately after the tollbooth computer establishes that the toll has been paid, the date and time information about the car's passage through the gate is erased. The extreme opposite situation arises if this information is added to a person's dossier, remains there without time limits, and is accessible to authorities and perhaps even others, such as divorce lawyers and the media.

Assume next that the authorities announce that the E-Z pass computers are programmed to maximize privacy. Such an assurance obviously does not suffice, because one cannot assume that the government will heed the policy it announces. The essence of the American political system is based on the idea that the public may trust the government but also receive verification that this trust is not misplaced. There have been many instances of abuse—from Nixon's enemies list and use of the IRS to harass his opponents to J. Edgar Hoover spying on Martin Luther King, Jr.—to confirm the public refusal to blindly trust the government. This deep sense is addressed through America's system of checks and balances, the free press, Congressional oversight, the introduction of the Offices of the Inspector General, and reports by the Government Accountability Office, among others.

One major way to further enhance accountability is to employ new technologies for this purpose. One key example is a wider use of audit trails, a computer program which keeps records of who has stored information, which in turn allows one to determine whether that person was authorized to access it.[131] Yet despite all these mechanisms, the public's trust in the government is quite low.[132] Additional steps are called for to both ensure that accountability is high enough and that the public will be able to better trust its government. This requires enlisting modes of oversight that draw not on the government but the public, somewhat like

131. *Audit Program Protocol*, U.S. DEP'T OF HEALTH HUM. SERV., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html.

132. Rick Newman, *Trust in Government and Other Institutions Hits New Lows*, U.S. NEWS (Jun. 20, 2012) http://www.usnews.com/news/blogs/rick-newman/2012/06/20/trust-in-government-and-other-institutions-hits-new-lows.

civilian review board of police departments.[133]

One way to enhance accountability through public involvement is to form an independent privacy review board. One such board, the Privacy and Civil Liberties Oversight Board, was proposed by the 9/11 Commission (itself a model of a review board) and established as part of the Intelligence Reform and Terrorism Prevention Act of 2004.[134] The board was to be composed of distinguished private citizens selected by the President, with a Chairman and Vice Chairman to be confirmed by the Senate.[135] Critics of the board maintained that it "appeared to be a presidential appendage, devoid of the capability to exercise independent judgment and assessment or to provide impartial findings and recommendations."[136] The board's former Vice Chairman, Alan Charles Raul, has disputed that allegation, pointing to a report the board issued that was highly critical of the FBI.[137] Nonetheless, the 110th Congress moved the board outside of the White House and established it as an independent agency.[138] The Senate did not confirm any of President Bush's replacement nominees.[139] In December of 2011, Obama nominated five board members, four of whom were confirmed by the Senate on August 2, 2012.[140] No action was taken in confirmation of David Medine, who is nominated for chairman of the board, and without whom the board will not be able to hire staff or possibly begin work.[141] Given the current high level of distrust in the government, there seems to be a strong case for

133. In a green paper the Department of Commerce advocated for the creation of a Privacy Policy Office to complement the work of the Federal Trade Commission in constructing privacy policy. Privacy advocates argued this would undermine the work of the FTC, but Peter Swire supports the idea, or a comparable office house in the Executive Office of the President, as it would provide "a more effective structure for the administration to weigh privacy concerns with other competing policy goals and values." *See* Peter P. Swire, *Why the Federal Government Should Have a Privacy Policy Office,* CENTER AM. PROGRESS (2011).

134. THE WHITE HOUSE, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD (2004), *available at* http://georgewbush-whitehouse.archives.gov/privacyboard/.

135. *Id*.

136. Garrett Hatch, CONG. RESEARCH SERV., RL34385, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD: NEW INDEPENDENT AGENCY STATUS (2009).

137. Alan Charles Raul, *Privacy and Civil Liberties: Where's the Watchdog?*, WASH. POST (Oct. 23, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/10/22/AR2009102203802.html.

138. Garrett Hatch, CONG. RESEARCH SERV., RL34385, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD: NEW INDEPENDENT AGENCY STATUS (2009), at 5.

139. *Id.* at 8.

140. U.S. SENATE COMMITTEE ON THE JUDICIARY, NOMINATIONS: PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *available at* http://www.judiciary.senate.gov/nominations/112thCongressExecutiveNominations/PrivacyAndCivilLibertiesOversightBoard.cfm.

141. Mark Rockwell, *Senate Confirms Privacy Oversight Board Nominees, but Leaves Out Chairman,* GSN (Aug. 6, 2012), http://www.gsnmagazine.com/node/26931?c=federal_agencies_legislative.

moving forward quickly with his confirmation and reactivating the board's work.

This or some other such board, whose staff and members have security clearances, could help reassure the public by issuing annual reviews that would report whether various new security measures (a) were abused and (b) were effective.[142] A good place to start would be to review the cases brought before the FISA court and determine whether it is too lax or too strict. And the board could inform the public whether those who have access to the output of massive computerized searches use them for legitimate purposes and what measures are taken to further minimize abuse when it is uncovered.

The way in which such reviews could serve the public is illustrated by a Washington Post investigation of President Bush's claim in defense of the expanded surveillance powers granted to law enforcement and intelligence agencies by the PATRIOT Act that "federal terrorism investigations have resulted in charges against more than 400 suspects, and more than half of those charged have been convicted."[143] The Washington Post reviewed that claim and concluded "the numbers are misleading at best."[144] Its analysis found that "39 people—not 200, as officials have implied—were convicted of crimes related to terrorism or national security."[145] And among all those charged as a result of terrorism investigations in the three years following the September 11th attacks, the *Post* found "no demonstrated connection to terrorism or terrorist groups for 180 of them."[146] Moreover, "a large number of people appear to have been swept into U.S. counterterrorism investigations by chance—through anonymous tips, suspicious circumstances or bad luck—and have remained classified as terrorism defendants years after being cleared of connections to extremist groups."[147] In response to Bush's defense, Lisa Graves of the ACLU stated, "[t]he real problem is that these record searches take place behind closed doors and are kept secret

142. The American Bar Association makes similar suggestions. *See* AMERICAN BAR ASSOCIATION, STANDARDS OF GOVERNING TECHNOLOGICALLY-ASSISTED PHYSICAL SURVEILLANCE 11 (1999) ("The legislature should provide accountability for the provisions governing access to and storage and disclosure of records maintained by institutional third parties via appropriate criminal, civil, and/or evidentiary sanctions, and appropriate periodic review and public reporting").

143. Dan Eggen & Julie Tate, *U.S. Campaign Produces Few Convictions on Terrorism Charges*, WASH. POST (Jun. 12, 2005), http://www.washingtonpost.com/wpdyn/content/article/2005/06/11/AR2005061100381.html.

144. *Id.*

145. *Id.*

146. *Id*.

147. *Id.*

forever."[148]

There was much in the report to support those who distrust the government and to raise serious doubts about whether the new powers accorded the government are justified. In contrast, if such a review had shown that most of these cases involved terrorists setting out to commit major acts of violence, the public would have leaned in the opposite direction. An established civilian review board charged with overseeing whom the government is collecting information about, with what cause and by what means, could play a similarly useful function. Clearly such a board could not look into every single one of the thousands of investigations conducted on U.S. citizens by law enforcement and intelligence agencies. But it could look at a random sample, of say, 200 cases, and determine if the majority involved individuals that actually presented a security risk. Such information would assure the public that the privacy sacrificed to heightened surveillance was worth the benefit of increased national security—or conversely expose that the government had overreached and upset the proper balance between privacy and the common good.

In short, the more extensive and effective accountability is provided, within the context of liberal democratic societies, whose guidance and oversight methods tend to be deficient—the more latitude could be granted to the government, without fearing that privacy would be wantonly violated or that that it would be limited without significant security gains. Furthermore, such mechanisms could help ensure that security measures would be minimally intrusive and their side effects would be mitigated.

VI. EROSION OF PUBLIC/PRIVATE BOUNDARIES

The discussion so far has followed a very strongly established tradition in Western legal thought and normative deliberations that draws a sharp line between the public and the private realms. This line is most evident in discussions of individual rights, which are rights against the government, seeking to curb its power and to protect the person from the state. Thus, the right to privacy is first and foremost a right against the government, as revealed in historical cases such as grievances raised against the Quartering Acts, which required the colonies to provide housing for British soldiers. One finds the same focus on protection from the government in the reproductive rights cases that are at the foundation of the federal, constitutional right to privacy in the U.S.

The Privacy Act of 1974 limits the right of the government to collect personal data but not that of the private sector. Many of the issues typically raised by privacy advocates concern surveillance, data banks,

148. *Patriot Act Works, Bush Claims,* WIRED (Jun. 9, 2005) http://www.wired.com/politics/law/news/2005/06/67807.

tracking, and other forms of search, focus first and foremost on the government. Although individuals do enjoy some legal protections against corporations and each other, these are often less clearly delineated and even less enforced. Thus, one's right to privacy against corporations at the work place, is much less clear than the right to protection from government surveillance, and varies from state to state. The same holds regarding protections from the media and peeping toms.

Over the last decade or so though, the boundaries between the private and public realms have been greatly diminished, both in general and in matters concerning privacy in particular. Currently, private corporations keep detailed dossiers on hundreds of millions of Americans, including not just what they purchase, but also tracking what Internet users read, visit, eat and drink, who users call, email and date, and much else. Other dossiers are kept on crimes a person has committed, divorces and political leanings, financial contributions, as well as interest in topics such as religion, the Bible, gambling and adult entertainment.[149] One may assume that given that the government is banned from collecting such information about Americans and building dossiers on innocent people, it could not use private agents to accomplish that which the government is banned from doing itself. However, this is far from clear, as one sees in matters other than privacy.

As far as privacy is concerned, the issue is moot. Even if the government does not contract private corporations to collect and process personal data of the kinds the government is prohibited from collecting and banking, the corporations can and do collect and accumulate such data and make it available to the government on their own. Given that the government is a large and reliable client, shaping the data in ways that they will serve the government's needs is much in the self interest of these corporations. Hence, according to Daniel Solove, "the government has been increasingly contracting with businesses to acquire databases of personal information."[150] ChoicePoint, a major private sector commercial data broker, has thirty-five contracts with government agencies, including the FBI, Drug Enforcement Administration, and IRS. A 2011 FBI manual authorizes agents to search for private citizens in commer-

149. In 2005 one data aggregation company, Choicepoint, had records on over 220 million people. *See They're Watching You*, BUS. WK. (Jan. 24, 2005), http://www.businessweek.com/magazine/content/05_04/b3917056_mz005.htm; *see also* Ryan Singel, *Newly Declassified Files Detail Massive FBI Data-Mining Project,* WIRED (Sept. 23, 2009), http://www.wired.com/threatlevel/2009/09/fbi-nsac/; and Ryan Singel, *Privacy and Consumer Profiling*, ELEC. PRIVACY INFO. CENTER, http://epic.org/privacy/profiling/.

150. DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (NYU Press 2004) at 169.

cial databases without prior authorization or notification.[151] One may well hold that some of the usages of private databases by the government serve legitimate purposes, even if they are loaded with extensive dossiers on most adult Americans, rather than being restricted to those for which there is some evidence or reason to suspect that they are violating the law. However, one must still note that from here on, whether such databanks are in the FBI headquarters or in some corporate office matters little. At most, they are just a click—and a payment—away.

It follows that if privacy is to be better protected, these protections will have to cover both the private and the public sector. This may seem obvious but it also entails a very major rethinking of the age-old dichotomy between the public and private realms. Steps in this direction include a slew of laws that limit the violation of privacy by private actors in one specific area or another. These include consumer credit reports, education records, bank records, video rental records, motor vehicle records, health information, children's online information, and customer financial information.[152] This patchwork of laws can be viewed as based on a rationale that treats differently three main areas—private information gleaned from public records (e.g. house ownership), relatively sensitive information (especially medical and financial), and information that is, in effect, deemed less sensitive (most consumer choices).[153]

Public records, therefore, are open for dissemination online because this information was not private in the first place; less sensitive information is considered in need of little protection because no or little harm is inflicted when it is used by third parties; and sensitive information is protected. And to the extent that one finds that some area is not well protected, the argument runs, Congress should add another "patch" to cover this area. However, because evidence shows that insensitive information can be used to determine sensitive information, laws are needed that not only ban the use of sensitive information but also ban indirect access to protected areas.[154]

---

151. Charlie Savage, *FBI Agents Get Leeway to Push Privacy Bounds*, N.Y. TIMES, Jun. 13, 2011, at A1.

152. Gina Stevens, CONG. RESEARCH SERV., R41756, PRIVACY PROTECTIONS FOR PERSONAL INFORMATION ONLINE (2011).

153. A similar approach is taken by the American Bar Association. *See* American Bar Association, STANDARDS OF LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS (2012).

154. 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. Peter Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization,* 57 UCLA L. REV. 1701 (2010); *see also* Marcia Stepanek, *Weblining*, BUS. WK. (Apr. 3, 2000), http://www.businessweek.com/

For example, in the case of Health Information Exchanges, there are concerns that the data that is entered into HEIs—though it is to be encrypted—could easily be "de-anonymized." In 2006, AOL released the search records—stripped of "personal identifiers"—of over 600,000 people. An investigation by the New York Times demonstrated that extremely intimate information—including names and faces—could be gleaned from purportedly anonymous data. A breach of an HIE could have much more serious consequences than it being revealed that one AOL user—Thelma Arnold—searched "school supplies for Iraq children," "safest place to live" and "the best season to visit Italy."[155] For this reason, privacy advocate and lawyer Grayson Barber suggests that it should be made a crime to "re-indentify" medical records.[156] That is, the wall that separates more sensitive and less sensitive information is shored up as well. (Granted, the debate about what is sensitive and what is not would continue.) That is, the law would ban private and public agents, corporations and the government, from using information on what one purchases (and other such "less" sensitive information) to divine one's medical condition (and other such "more" sensitive information).

VII. IN CONCLUSION

Privacy is a core value. It is essential for political dissent, innovation, and individuation. The default position of the law and public policy should be that privacy must be well protected. However, society is called upon to attend to multiple values, and these do come into conflict with privacy. The question hence arises which value ought to yield? Note that framing the examination of privacy in this liberal communitarian way differs from those who view privacy as a right, and leave it to others to prove that any exceptions ought to be made, under which this right will yield, and set very high the bar such proof must clear. Liberal communitarianism does not privilege the common good or privacy, and makes a strong commitment to both the starting points for its deliberations.

The key question, which core value must yield under what conditions, cannot be addressed abstractly and summarily, by pointing to the high value of privacy—or to that of security or of some other common good. The question must be addressed within the given historical context in which a particular society finds itself. In this context the first issue is how to enable informal social controls to maintain the moral order,

---

2000/00_14/b3675027.htm; Jennifer Golbeck, Christina Robles & Karen Turner, *Predicting Personality with Social Media,* CHI EXTENDED ABSTRACTS (2011).

155. Micheal Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES (Aug. 9, 2006), http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all.

156. Grayson Barber, *Electronic Health Records and the End of Anonymity*, 198 N.J. L. J. 227 (2009).

which in turns serves to minimize the coercive role of the state. This often requires allowing a high level of visibility of personal conduct to other members of the community, i.e. limiting social privacy. To put it in popular terms, there are and there ought to be few protections against gossip. It takes a village to prevent a crime.

To the extent that the state must be involved, four criteria have been laid out to help sort out whether a particular society, in a particular period, has compelling public needs that require a re-triangulation of the relations between privacy and the common good. Given that societies often over-steer in one direction or the other, and their circumstances change—such redirection is frequently needed. If the new needs cannot be served by voluntary means—preference is best given to the least intrusive interventions by the state. And attention should be given to mitigating the side effects of such interventions.

To the extent that government agents are held accountable, and oversight over their action is adequate, they can be granted more powers and leeway. The more surveillance is itself under surveillance, the more surveillance a society can tolerate. However, when one cannot rely on the government itself to provide sufficient oversight, new public bodies are needed.

The traditional distinction between the public and the private realm is losing much of its value. One must increase privacy protections against private agents, because—aside from violating privacy on their own, often without any gain to anyone but to themselves—they also share the information they garner, including very comprehensive dossiers, with the government. Hence all agents should be prohibited from collecting sensitive information—*and from using insensitive information to ferret out that which is more sensitive*—unless there is compelling public interest, the intrusion is minimized and the side effects are mitigated, in both the private and the public realms. This last requirement entails a major departure from prevailing legal traditions and public policy that in liberal democracies restrain the state but poorly regulate the private sector.