Public Affairs Quarterly
Volume 25, Number 2, April 2011

PRIVACY, SECURITY, AND GOVERNMENT SURVEILLANCE: WIKILEAKS AND THE NEW ACCOUNTABILITY

Adam D. Moore

In times of national crisis, citizens are often asked to trade liberty and privacy for security. And why not, it is argued, if we can obtain a fair amount of security for just a little privacy? The surveillance that enhances security need not be overly intrusive or life altering. It is not as if government agents need to physically search each and every suspect or those connected to a suspect. Advances in digital technology have made such surveillance relatively unobtrusive. Video monitoring, global positioning systems, airport body scanners, and biometric technologies, along with data surveillance, provide law enforcement officials with monitoring tools, without also unduly burdening those being watched.

Against this view are those who maintain that we should be worried about trading privacy for security. Criminals and terrorists, it is argued, are nowhere near as dangerous as governments.[1] There are too many examples for us to deny Lord Acton's dictum that "power tends to corrupt, and absolute power corrupts absolutely."[2] If information control yields power and total information awareness radically expands that power, then we have good reason to pause before trading privacy for security.

An indication of power is the ability to forcibly demand access to information about others while keeping one's own information secret. Governments, and corporations for that matter, are notoriously good at demanding access to information. A recent counter-movement to this trend is the emergence of online information-sharing sites dedicated to shining a spotlight on the backroom activities of government agencies and corporations. Sites like WikiLeaks promise to change the "accountability landscape" so to speak.

I have argued elsewhere that individuals have moral privacy rights that limit the surveillance activities of governments.[3] While not absolute, privacy rights shield individuals from the prying eyes and ears of neighbors, corporations, and the state. The question that I will consider in this article is one of balance—when are security

interests weighty enough to overbalance individual privacy rights? Before defending my own account, I will critique three rival views. One way to strike a balance between privacy and security is to let those in power decide. In most cases, these individuals seek public office for noble purposes—we should let them decide how best to protect privacy and security. I call this position "just trust us." A second view minimizes privacy interests by calling into doubt the activities privacy may shield. This view, called "nothing to hide," maintains that individuals should not worry about being monitored. Only those who are engaged in immoral and illegal activity should worry about government surveillance. Similar to "nothing to hide" is the view that "security trumps." This latter account holds that security interests are—by their nature—weightier than privacy claims. After offering a critique of these attempts at balancing, I will defend my own account. I will argue that by insisting on judicial discretion for issuing warrants, demonstrating probable cause for an intrusion, and allowing public oversight of the process and reasoning involved, we may promote both privacy and security. Finally, in the concluding section I will consider the WikiLeaks movement and its impact on accountability.

"Just Trust Us"—Trading Civil Rights for Security

Before considering the "just trust us" view, I would like to briefly address why we should consider privacy and security morally valuable. Privacy, defined as a right to control access to and uses of bodies, locations, and information, is necessary for human well-being or flourishing. Simply put, there is compelling evidence that individuals who lack this sort of control suffer physically and mentally.[4]

Security is also valuable. Whether derived from individual rights to self-defense or via a social contract, a legitimate function of any government is to protect the rights of its citizens. At the most basic level, security affords individuals control over their lives, projects, and property. To be secure at this level is to have sovereignty over a private domain—it is to be free from unjustified interference from other individuals, corporations, and governments. Security also protects groups, businesses, and corporations from unjustified interference with projects and property. Without this kind of control, businesses and corporations could not operate in a free market—not for long, anyway.

There is also national security to consider. Here, we are worried about the continued existence of a political union. Our institutions and markets need to be protected from foreign invasion, plagues, and terrorism. But again it seems that we value national security, not because some specific political union is valuable in itself, but because it is a necessary part of protecting individual rights. Armed services, intelligence agencies, police departments, public health institutions, and legal systems provide security for groups, businesses, and, at the most fundamental level, individuals. If correct, we have good reason to think that privacy and security are morally valuable.

Turning to the "just trust" account, a common view is that we should give the benefit of the doubt to those in power and assume that officials will not override individual rights without just cause. Public officials typically seek office to promote the public good and are generally well-meaning and sincere people—we should trust them to do what is right and fair. On this account, the balance of privacy and security should be determined by those in power, in reference to the issues at hand. If terrorists are using private e-mail accounts or chat rooms to plan attacks, then government officials may use Internet packet-sniffers to search for suspicious text.

Arguably, there are good reasons to distrust this method of establishing an appropriate balance between privacy and security. Justice Brandeis, dissenting in *Olmstead v. United States*, wrote: "Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."[5] Brandeis, like Lord Acton quoted in the opening, worries about human corruptibility and the incremental debasing of liberty and privacy. In a crisis, even the most noble among us are susceptible to favoritism, stubbornness, and suspect reasoning. While the cases noted below are based in US history and law, the point being made is more general.

Consider President Abraham Lincoln's situation at the start of the Civil War. Lincoln declared a state of emergency and suspended the legal rights of citizens in the Border States of Maryland, Kentucky, Missouri, and Tennessee. "In addition to using federal troops to intimidate state legislators and influence their decisions, Lincoln imprisoned 13,000 civilians and suspended the writ of habeas corpus so that no inquiry could be made into the validity of their detainment."[6] Lincoln also arrested nineteen members of the Maryland state legislature and encouraged civilians in Missouri to disperse gatherings of those who supported the Confederate cause. Additionally, the president established military tribunals that tried and punished civilians who offered aid and comfort to Southern sympathizers—thus denying these individuals the Constitutional guarantees of a public trial by an impartial jury.

The appropriate test, Lincoln argued, was whether the president should "risk . . . losing the Union that gave life to the Constitution because that charter denied him the necessary authority to preserve the Union."[7] Arguably, the notion of a president exercising "emergency powers" in a time of crisis based on his own subjective assessment of the issues at stake sets a bad precedent. But why, you may ask. Lincoln was not an "unthinking" man of zeal, and it could be argued that he adopted an appropriate policy—one that saved the Union.

First, it is not clear that suspending the writ of habeas corpus in the Border States was necessary to save the Union. Second, even if the states had split, it does not follow that we would have been thrown into a condition of worse security

compared to the history that actually happened. It is not as if the Union and the Confederate States would have reneged on protecting individual rights.[8] Third, even if Lincoln got it right, we should not feel good about it. Liberty and privacy rights were suspended based on the subjective evaluation of a politician—hardly a process that anyone would endorse ahead of time. Consider what could have happened if Lincoln had been severely depressed or if he had simply killed off individuals who advocated separation.

Several other cases also deserve mention. In February 1942, President Roosevelt authorized the internment of Japanese-Americans during World War II. Over one hundred thousand people of Japanese descent were rounded up and incarcerated. Several Japanese-Americans who protested the internment and several who tried to escape were shot and killed.[9] The passage of the Taft-Hartley Act in 1947 and the McCarran Act in 1950 provided justification for the "red scare" and the ensuing McCarthyism of the early 1950s.[10] Reaffirming the "clear and present danger" test established in *Schenk v. United States* (1919),[11] the Supreme Court maintained that "mere membership in the Communist Party was sufficient to justify government action."[12] Thus began one of the worst periods of government abuse.

From the late 1950s through the early 1970s, the FBI engaged in numerous operations designed to infiltrate, disrupt, and if possible eliminate groups that were deemed to be enemies of the American way of life. After a lengthy investigation of Counter Intelligence Program (COINTELPRO) operations, the Church Committee noted numerous abuses, including attempting to get individuals fired for their political beliefs, trying to destroy the marriages of intelligence targets, indiscriminately opening citizens' first-class mail, and warrantless break-ins.[13] A federal court, in *Socialist Workers Party v. Attorney General*,[14] found that "COINTELPRO was responsible for at least 204 burglaries by FBI agents, the use of 1,300 informants, the theft of 12,600 documents, 20,000 illegal wiretap days and 12,000 bug days."[15]

More recent cases come from abuses related to the USA PATRIOT Act and the terrorist attacks of 9/11—for example, Sami al-Hussayen's detainment for more than a year related to "providing expert advice and assistance" to terrorist organizations, the incarceration of numerous individuals without trial at Guantanamo Bay Naval Base, or the acts of rendition carried out by the CIA.[16] In each of these cases, in hindsight and after cool reflection, few would maintain that the balance between security and liberty or privacy was appropriately struck.

I would like to conclude this section by considering an interesting argument offered by James Stacey Taylor—one could view this as a new version of the "just trust us" argument.[17] Expanding on Taylor's example, suppose technology has advanced to the point where miniaturized robots roam everywhere, recording everything. Not only do they record everything you say or do from numerous angles, but they also record your very thoughts. This entire vast amount of in-

formation is uploaded to an ever-growing database. Taylor argues that "rather than opposing such an expansion of surveillance technology, its use should be encouraged—and not only in the public realm. Indeed, the State should place all of its citizens under surveillance at all times and in all places, including their offices, classrooms, shops—and even their bedrooms."[18] The mere existence of this database should not be worrisome and has clear benefits, among them unbiased access to the truth, better equality within the justice system between the rich and the poor, and deterrence. In brief, Taylor argues that once specific conditions are met, related to the accessing of information—those cases where the government is morally permitted to access information about individuals—then having more information available would be best, given that it is difficult to determine what information will be needed beforehand. The primary thrust of Taylor's argument is that the mere existence of such a database is value neutral.[19] The important questions are those surrounding access to this information.

Putting aside the supposed benefits of having such a system—in fact, there are numerous cases demonstrating how monitoring of this sort does not deter crime—I will present two general problems for Taylor's account.[20] First, if controlling access to our bodies and personal information is morally valuable and the loss of such control constitutes a health risk, then the notion that the mere existence of such a database is not morally problematic is suspect.[21] Furthermore, I am certain that such a tool would eventually be misused. Well-meaning government officials have been and will be tempted to set aside reasonable safeguards in times of emergency or crisis. For example, just think how such a database would have been used during the McCarthy era. From doctoring the information found in the database to changing the access requirements during a perceived crisis—"We have a moral obligation to stop those communists, homosexuals, Jews, or Muslims"—to how the rich or powerful might be spared such monitoring (think of the black-market anti-monitoring products that would be produced), the risks are hardly negligible.[22]

It is also interesting to consider how the "just trust us" view looks in light of the WikiLeaks movement. I doubt that any government or corporation would find such a view compelling if the tables were turned. These folks who seek to protect the citizens of different countries from governments and corporations run amok are well-meaning and upstanding individuals—we should just trust them to disclose what they think is important. Moreover, why should governments or corporations complain if they have nothing to hide?

The "Nothing to Hide" Argument

A counterpart to the "just trust us" view is the "nothing to hide" argument.[23] According to this argument we are to balance the potential for harm of data mining and the like with the security interests of detecting and preventing terrorist attacks.

I suppose we could weaken this further by merely referencing "security interests," which would include, but not be limited to, "terrorist attacks." The idea is that our security interests are almost always more weighty than the minimal costs of surveillance—privacy intrusions are a mere nuisance and are easily traded for increases in security. A formal version of the argument might go something like this:

> P1. When two fundamental interests conflict, we should adopt a balancing strategy, determine which interest is more compelling, and then sacrifice the lesser interest for the greater. If it is generally true that one sort of interest is more fundamental than another, then we are warranted in adopting specific policies that seek to trade the lesser interest for the greater interest.
>
> P2. In the conflict between privacy and security, it is almost always the case that security interests are weightier than privacy interests. The privacy intrusions related to data mining or National Security Agency (NSA) surveillance are not as weighty as our security interests in stopping terrorism, and so on—these sorts of privacy intrusions are more of a nuisance than a harm.
>
> C3. So it follows that we should sacrifice privacy in these cases and perhaps adopt policies that allow privacy intrusions for security reasons.

One could easily challenge Premise 2—there are numerous harms associated with allowing surveillance that are conveniently minimized or forgotten by the "nothing to hide" crowd. Daniel Solove notes that "privacy is threatened not by singular egregious acts but by a slow series of small, relatively minor acts, which gradually begin to add up."[24] Solove also points out, as I have already highlighted, that giving governments too much power undermines the mission of providing for security—the government itself becomes the threat to security. The point was put nicely by John Locke: "This is to think, that Men are so foolish, that they take care to avoid what Mischiefs may be done them by *Pole-Cats*, or *Foxes*, but are content, nay think it Safety, to be devoured by *Lions*."[25] It is also important to note the risk of mischief associated with criminals and terrorists compared to the kinds of mischief perpetrated by governments—even our government. In cases where there is a lack of accountability provisions and independent oversight, governments may pose the greater security risk.

Moreover, there is sensitive personal information that we each justifiably withhold from others, not because it points toward criminal activity, but because others simply have no right to access this information. Consider someone's sexual or medical history. Imagine someone visiting a library to learn about alternative lifestyles not accepted by the majority. Hiding one's curiosity about, for example, a gay lifestyle may be important in certain contexts. This is true of all sorts of personal information like religious preferences or political party affiliations.

Consider a slight variation of a "nothing to hide" argument related to what might be called physical privacy. Suppose there was a way to complete body cavity searches without harming the target or being more than a mere nuisance. Perhaps we search the targets after they have passed out drunk. Would anyone find

it plausible to maintain a "nothing to hide" view in this case? I think not—and the reason might be that we are more confident in upholding these rights and policies that protect these rights than we are of almost any cost-benefit analysis related to security. Whether rights are viewed as strategic rules that guide us to the best consequences, as Mill would argue, or understood as deontic constraints on consequentialist sorts of reasoning, we are more confident in them than in almost any "social good" calculation. I am not saying that rights are absolute—they are just presumptively weighty. This line of argument is an attack on the first premise of the "nothing to hide" position. Rights are resistant to straightforward cost-benefit or consequentialist sort of arguments. Here we are rejecting the view that privacy interests are the sorts of things that can be traded for security.

Another problem for the "nothing to hide" argument has to do with justice and the distribution of harms. The distribution aspect is highlighted when surveillance policies pick targets based on appearance, ethnicity, or religion. If the burden of surveillance policy and the corresponding harms fall on one portion of society, we may have a problem of justice.[26]

Finally, those who defend the "nothing to hide" view, balancers, rarely discuss the consequences of the surveillance policy they are promoting or whether an alternative might exist that better protects both privacy and security.[27] Consider, just for example, almost any predominately developed "isolationist" country—perhaps Switzerland. My guess is that these sorts of countries do not have much terrorist activity and likely do not have higher crime rates than the United States.[28] One way to obtain more security would be to change our selectively interventionist policies—in this way, security and privacy could be protected. Foreign policy can worsen or alleviate tensions between privacy and security.

The "Security Trumps" View

According to what might be called the "security trumps" view, whenever privacy and security conflict, security wins—that is, security is more important than privacy.[29] In the typical case, security protects fundamental rights, the most important of which is the right to life. Privacy may protect important interests, but these interests will never rise to the level of security of life and limb.

First, it is not clear why a "security trumps" view should be adopted over a "privacy trumps" view. Bodily privacy—the right to control access to and uses of one's body—seems at least as fundamental or intuitively weighty as security. In fact, one could argue that security only gets its value derivatively based on what it is protecting. On this view, security would be an instrumental value—something used to promote intrinsic values.

Second, given that we generally promote individual security by authorizing others, it would be advantageous to maintain certain checks against those who provide security. Privacy is one of these checks. The point is not that privacy is

absolute; rather, the point is that, before we set aside privacy for security, it would be prudent to put certain safeguards in place. Here we are rejecting the rule that security trumps in every case, independent of process or procedure. In fact, it seems odd to maintain that any increase in security should be preferred to any increase in privacy. Such a view would sanction massive violations of privacy for mere incremental and perhaps momentary gains in security. Also, given that security will be provided by others and power is likely a necessary part of providing security, we have strong prudential reasons to reject the "security trumps" view. If those who provide security were saints, then perhaps there would be little to worry about. The cases already presented are sufficient to show that we are not dealing with saints.[30]

Finally, it is false to claim that in every case, more privacy means less security or more security entails less privacy. Security arguments actually cut the other direction in some cases—it is only through enhanced privacy protections that we can obtain appropriate levels of security against industrial espionage, unwarranted invasions into private domains, and information warfare or terrorism. Consider how privacy protections enhance security when considering encryption standards for electronic communications and computer networks. Although the National Security Administration's position is that the widespread use of encryption software will allow criminals a sanctuary to exchange information necessary for the completion of illegal activities, consider how easily this security argument can be stood on its head. National security for government agencies, companies, and individuals actually *requires* strong encryption. Spies have admitted to "tapping in" and collecting valuable information on US companies—information that was then used to gain a competitive advantage.[31] A report from the Center for Strategic International Studies (CSIS) Task Force on Information Warfare and Security notes that "cyber terrorists could overload phone lines . . . disrupt air traffic control . . . scramble software used by major financial institutions, hospitals, and other emergency services . . . or sabotage the New York Stock Exchange."[32] Related to information war, it would seem that national security requires strong encryption and multi-level firewalls.

Balancing Privacy and Security While Maintaining Accountability

If I am correct, the views captured by "just trust us," "nothing to hide," and "security trumps" fail to establish a defensible process for balancing security, privacy, and liberty. In this section, having cleared aside these popular views, I will present my own account of how to strike an appropriate balance.

Consider the following case. Suppose that Fred gives Ginger, a mere acquaintance, his gun, in order to provide security—perhaps Ginger is a much better shot. Assuming that Ginger is like the rest of us, it would be irrational of Fred to agree

to a situation where Ginger could decide the best course of action independent of input, constraint, or consequences—it would be hard to believe that in this case Fred has *promoted* his security interests. This in part captures my argument against the views captured by "just trust us," "nothing to hide," and "security trumps." In furthering his own security interests, Fred would likely insist on several rules before employing Ginger as his protector. In general, there would be rules that provide a check on those with the power to provide security, rules that require a rational basis for overriding rights, and rules that allow for review of the adopted process as well as different protection policies that may provide better protection of rights.

Rules that provide a check on the power of security providers are necessary so that security is not also debased. These sorts of rules could include judicial review and public oversight of laws that promote some interests at the expense of others (WikiLeaks, discussed below, could provide an alternative way to check the power of security providers). By insisting on an objective independent authority, bias, prejudice, and clouded reasoning can be minimized. Oversight also ensures the accountability of the actors involved. Subjects could vote their protectors out of power or institute criminal sanctions against those who overstep the law. Public oversight, and the accountability it may promote, would require transparency.

As with rules that provide a check on power, there are rules that require a rational basis for rights balancing or trading. In cases where security is promoted at the expense of privacy, property, or liberty, we would require a rational basis for the rule. Probable cause is an example. If an agent of the government can demonstrate that a target committed, is committing, or will commit a crime, then an independent authority, like a judge, can issue a warrant or subpoena. Unlike the reading of tea leaves or the emotional judgments of a politician in a moment of crisis, a process like demonstrating probable cause before an impartial authority has a rational basis. There may be other sets of rules that achieve the same results—the point is not about this specific set; rather, the point is about what would be rational to endorse as a security enhancement.

With probable cause, a warrant issued from a judge, and sunlight provisions opening up the warrant and the procedure to public scrutiny, we can be confident that security concerns may be addressed with minimal impact on individual privacy. The requirement of probable cause puts the burden of proof in the appropriate place—invasions of private domains must be justified. The official seeking the warrant would highlight the security risks involved, along with the privacy interests at stake. Judicial oversight inserts an outside element into the process, providing a check on the enthusiasm of law enforcement officials. In any event, the question of when security should override privacy would not be left to the subjective judgment of one individual or a small group of individuals with similar interests. Finally, sunlight provisions provide public oversight of the entire process, including the reasons for the warrant and the judicial ruling. In

this way, at each step, public accountability is ensured. These sorts of provisions could be based in law and required or achieved via extra-legal instruments like WikiLeaks. Consider Table 1, which measures privacy interests across several dimensions.

Table 1 presents a rough guide for when privacy should give way to security—when should a warrant or subpoena be issued. First, if the subject has consented to the surveillance, then the magnitude, context, and security dimensions become irrelevant—such monitoring would be justified. Short of consent, if the magnitude is slight, the context was clearly "public," and the security threat high, the burden of proof for overriding privacy would be low. Sliding to the other extreme, if the magnitude of the invasion is profound, the context clearly "private," and the security threat low, then the burden for overriding privacy would be high. Finally, if there were a substantial security threat backed by clear and credible evidence, then independent of the magnitude, context, or consent, the burden for overriding privacy would be low. For example, if a police officer has good evidence that a murder will take place tomorrow afternoon at a suspect's home, then a warrant would be justified.

In addition, there will be justifiable exceptions to the rule of requiring probable cause and warrants. There may be instances when law enforcement officials need to act quickly and do not have the time to secure a warrant or provide an argument for probable cause—suppose a police officer hears a scuffle and someone

Table 1. **Privacy Interests across Four Dimensions**

	Magnitude of Invasion Duration, Extent, Means	
Slight		**Profound**
A onetime wiretap of a cell phone conversation		Total surveillance including data mining, electronic communications, physical movements
	Context	
Little Expectation of Privacy		**Reasonable Expectation**
The subject will be monitored in "public"—perhaps as he or she walks down the street		The subject will be monitored at his or her primary residence
	Consent	
Consented to Surveillance		**Evaded Surveillance**
The subject consents to the surveillance		The subject actively avoids surveillance
	Public Security	
Substantial Security Threat		**Little Security Threat**
Credible evidence that lives are at stake		The pacifist alliance plans to have a bake sale to raise funds

shouts for help. Provided that law enforcement officers act in "good faith" and can articulate reasonable grounds for entering private domains after the fact, they should be given some leeway in these cases. Perhaps internal and civilian oversight committees could review such cases to determine if appropriate action was pursued. Thus even in "emergency" situations where privacy is traded for security without a warrant or judicial oversight, we may insist on sunlight provisions and accountability.

Security concerns related to mass transportation or large public gatherings may also warrant an exception to the probable cause rule—individuals may be searched without evidence that they will commit a crime, in these cases. Nevertheless, there are at least two important controls that should be noted. First, individuals, in many instances, consent to these sorts of minimal intrusions. If you do not want to have your bag searched, then stay home and watch the ball game on television. Obviously, the more voluntary the activity, the more robust the consent would be, once given. In cases where the activity is less voluntary—flying on an airplane, for example—we insist on stronger justifications for more intrusive searches. Moreover, judicial and civilian oversight is still appropriate for establishing the correct balance between privacy and security in these cases. Few would sanction body cavity searches at airports for the minimal gains in security that could be obtained.

Assuming I am correct, it should be clear from the preceding just how far we have strayed from the baseline of probable cause, judicial oversight, and public accountability here in the United States. The USA PATRIOT Act allows covert searches and seizures with the target only being notified at some later time.[33] Targets suspected of violating the Computer Fraud and Abuse Act may be monitored without judicial oversight.[34] Foreign Intelligence Surveillance Act (FISA) courts, America's secret courts, have issued more than fourteen thousand applications for surveillance. "Of these applications, the Foreign Intelligence Surveillance Court (FISC) summarily approved without modification all but five, and it did not reject even one."[35] Foreign Intelligence Surveillance Court judges and magistrate judges have the authority to rule on these surveillance applications, although they have little power to reject them. "The FBI need not show 'probable cause' or any reason at all to believe that the target of the surveillance order is engaged in criminal activity. All the FBI needs to do is 'specify' that the records are 'sought for' an authorized investigation."[36] Note that, as long as this requirement is satisfied, the specification that the records are "sought for" an authorized investigation, US citizens are also covered. These courts meet in secret, and their proceedings are almost never published.

For the sake of argument, suppose that secret courts and gag orders are indeed necessary for certain cases dealing with sensitive matters related to national security. Why are there no sunlight provisions—ever? Here, the "nothing to hide" argument seems more forceful. Government agents providing security should be accountable to the American people.

Finally, over the past decade there has been an alarming decrease in applications for warrants and a sharp increase in the use of subpoenas.[37] Through the use of administrative subpoenas, the government gathers information necessary for the maintenance of the state. A critic of the proposed view of requiring probable cause, judicial oversight, and sunlight provisions may argue that these rules are too strong. Governments must be able to require disclosures from individuals and corporations for taxing purposes or for licensing without going before a judge.

Nevertheless, there is a vast difference between requiring citizens and corporations to file yearly tax returns and adopting policies that allow government agents almost unfettered access to information through the use of subpoenas. A required disclosure for tax information without showing probable cause seems reasonable—assuming that such information is accessed and used only by the IRS. Beyond such specific purposes and uses related to the administrative state, we should insist on probable cause, judicial oversight, and accountability. For example, if the tax records of a suspected criminal are relevant to an investigation, then the investigators should go before a judge, show probable cause, and if appropriate, acquire access.

Conclusion

As noted in the opening, the recent sharing of government information on sites such as WikiLeaks is forcing a new kind of accountability. One marker of power is the ability to demand information disclosures from others while keeping one's own information secret. As data mining and profiling have become the norm, many have become frustrated and alarmed with a perceived loss of power. Other entities, like governments and corporations, control vast amounts of information, including sensitive personal information about citizens, and use this information for their own ends. The average information target or citizen has little power to demand disclosures from governments and corporations and even less power to control the vast amounts of information being collected and stored. In terms of accountability to family, work, community, and the nation, individuals have felt increased pressure with the arrival of the digital age. For example, consider all the new devices used to monitor workplace activity in the private sector, and the corresponding changes in accountability. Information sharing sites, like WikiLeaks, have changed all of this. Now there is the possibility that the "new accountability" will be felt at all levels of government and business. Information that was once only heard in whispers at closed committee meetings is now being shouted from the mountaintop. Moreover, the shrill cry of "but you have no right to access this information" has an air of hypocrisy.

Critics of the WikiLeaks movement note that unleashing government secrets will lead to a body count. I would agree. It is only a matter of time before the disclosure of some state secret leads to an agent being discovered and killed. But

on the other hand, those of us who have been relatively powerless to control or demand information have lived with this threat for years. The cases of governments, corporations, and criminals using information obtained from various data banks to kill or control average citizens are too numerous to count. While I agree that "two wrongs don't make a right," I would stress what this phrase acknowledges. There are *two* wrongs. Perhaps with the leveling of the playing field, so to speak, we will find better ways to promote accountability and privacy.

To be clear, my current thinking about the WikiLeaks movement is that it is a necessary evil. If governments and corporations want to have privacy and security in sensitive information, then they would do well to offer these same protections to ordinary citizens. My fear is that what we will get are more domestic and international legal instruments designed to protect the current power structures. Those who can control and demand information while avoiding accountability by withholding secrets will write the rules to their advantage. If so, then I am solidly behind the WikiLeaks movement.

In this article I have argued that balancing tests that purport to justify invasions of privacy in the name of security often go awry and attempt to trade values that are difficult to measure. It has also been argued that, in trading privacy for security, we should insist on establishing probable cause, judicial oversight, and accountability. Probable cause sets the standard for when security interests override privacy rights. Judicial oversight, sensitive to case-specific facts like the context and magnitude of the proposed intrusion, introduce an "objective" agent into the process. Sunlight provisions allow for a public discussion of the merits of specific searches and seizures. All of this promotes accountability in that the reasons for a search and the actions of government officials are open to public scrutiny. A further benefit is that such policies engender trust and confidence in public officials.

A transparent society is not inevitable. Privacy at the personal level can be secured through custom and social pressure. Privacy related to big media, corporate interests, and the state can be guaranteed by law and also be grounded in customs and social practices. Justice Douglas, writing for the descent in *Osborn v. United States*, noted,

> The time may come when no one can be sure whether his words are being recorded for use at some future time; when everyone will fear that his most secret thoughts are no longer his own, but belong to the Government; when the most confidential and intimate conversations are always open to eager, prying ears. When that time comes, privacy, and with it liberty, will be gone. If a man's privacy can be invaded at will, who can say he is free? If his every word is taken down and evaluated, or if he is afraid every word may be, who can say he enjoys freedom of speech? If his every association is known and recorded, if the conversations with his associates are purloined, who can say he enjoys freedom of association? When such conditions obtain, our citizens

> will be afraid to utter any but the safest and most orthodox thoughts; afraid to associate with any but the most acceptable people. Freedom as the Constitution envisages it will have vanished.[38]

Douglas paints a grim picture, and we should heed his warning—we have good reason to resist traveling toward a watcher-based society. Transparency is not necessary for security. Striking an appropriate balance between privacy and security is difficult. Nevertheless, it has been argued that the best way to protect both of these important values is to insist on a probable cause requirement, judicial discretion, and public oversight.

University of Washington

NOTES

I would like to thank Bill Kline, James Stacey Taylor, Ken Himma, Dan Solove, and an anonymous referee for their comments and suggestions on earlier drafts of this paper.

1. Terrorists are nowhere near as dangerous as governments. "From 1980 to 2000, international terrorists killed 7,745 people according to the U.S. State Department. Yet, in the same decades, governments killed more than 10 million people in ethnic cleansing campaigns, mass executions. . . . In the 1990s, Americans were at far greater risk of being gunned down by local, state, and federal law enforcement agents than of being killed by international terrorists." James Bovard, *Terrorism and Tyranny: Trampling Freedom, Justice, and Peace to Rid the World of Evil* (New York: Palgrave Macmillan, 2003), p. 8.

2. Lord Acton, letter to Bishop Mandell Creighton (April 3, 1887), in *The Life and Letters of Mandell Creighton*, ed. Louise Creighton (New York: Longmans, Green, 1904), vol. 1, chap. 13.

3. Adam D. Moore, *Privacy Rights: Moral and Legal Foundations* (University Park, PA: Penn State University Press, 2010).

4. See Adam D. Moore, "Privacy: Its Meaning and Value," *American Philosophical Quarterly*, vol. 40, no. 3 (Fall 2003), pp. 215–227; and Moore, *Privacy Rights*, chap. 3. See also Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1968); Barry Schwartz, "The Social Psychology of Privacy," *American Journal of Sociology*, vol. 73, no. 6 (1968), pp. 741–752; and James Rachels, "Why Privacy Is Important," *Philosophy and Public Affairs*, vol. 4, no. 4 (1975), pp. 323–333.

5. *Olmstead v. United States*, 277 U.S. 438 (1928).

6. Jacob Lilly, "National Security at What Price?: A Look into Civil Liberty Concerns in the Information Age under the USA PATRIOT Act of 2001 and a Proposed Constitutional Test for Future Legislation," *Cornell Law Journal*, vol. 12 (2003), p. 451.

7. Ibid., citing Debora K. Kristensen, "Finding the Right Balance: American Civil Liberties in Time of War," *Advocate* (December 2001), p. 21.

8. I understand that African-Americans who remained in the Confederate States would

not have had their rights protected. But at the time, the outcome of the war was in doubt, and Lincoln could not have known that violating the liberty rights of those in the Border States would enhance long-term security for everyone, compared to the alternatives available.

9. *Korematsu v. United States*, 584 F. Supp. 1406 (N.D. Cal. 1984); *Hirabayashi v. United States*, 627 F. Supp. 1445 (W.D. Wash. 1986), affirmed in part and reversed in part, 828 F.2d 591 (9th Cir. 1987); *Yasui v. United States*, 83–151 BE (D. Or. 1984), remanded, 772 F.2d 1496 (9th Cir. 1985).

10. Taft-Hartley Act of 1947, Public Law 80–101, 61 Stat. 136 (1947); and the Internal Security (McCarran) Act of 1950, Public Law 81–831, 64 Stat. 987 (1950).

11. *Schenk v. United States*, 249 U.S. 47, 52 (1919). See *Dennis v. United States*, 341 U.S. 494 (1951).

12. Lilly, "National Security," p. 454.

13. US Senate, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong., 2d sess., 1976, bk. 2, pp. 6, 10–13.

14. *Socialist Workers Party v. Attorney General*, 642 F.Supp. 1357 (S.D.N.Y. 1986).

15. Laura W. Murphy, "ACLU Looks at Domestic Surveillance," ACLU Washington National Office, http://www.aclu.org/FreeSpeech/FreeSpeech.cfm?ID=9790&c=86 (accessed on January 8, 2010).

16. Ibid.

17. James Stacey Taylor, "In Praise of Big Brother," *Public Affairs Quarterly*, vol. 19, no. 3 (2005), pp. 227–246.

18. Ibid., p. 227.

19. One could cast Taylor's argument as a version of the old "guns don't kill people, people kill people" view. An important difference between these two positions is that almost everyone can own a gun while only a few will be able to access the database. Power in the gun case is more or less equalized—whereas power in the database access case is not.

20. See, for example, Michael McCahill and Clive Norris, "CCTV in London" (June 2002), Report to the European Commission Fifth Framework RTD, as part of *Urbaneye: On the Threshold to Urban Panopticon?*, Working Paper No. 6, Centre of Technology and Society at the Technical University of Berlin, pp. 1–30; p. 20, http://www.urbaneye.net/results/ue_wp6.pdf.

21. See Moore, *Privacy Rights*, chap. 3; and Moore, "Privacy: Its Meaning," pp. 215–227.

22. Other risks include regime change and hacking by other nations. Also, if this technology is available to the best of governments, it would also, sooner or later, be available to the worst of governments. I suppose the United States would then pursue a "nonproliferation" strategy so that our secrets could be kept safe while we had access to everyone else's.

23. For a more rigorous analysis of this argument, see Daniel Solove's "I've Got Nothing to Hide and Other Misunderstandings of Privacy," *San Diego Law Review*, vol. 44, no. 4 (2007), pp. 745–772.

24. Ibid., p. 769.

25. John Locke, *The Second Treatise of Government*, ed. C. B. Macpherson (Indianapolis, IN: Hackett, 1980), chap. 5, sec. 93.

26. See Jeremy Waldron, "Security and Liberty: The Image of Balance," *Journal of Political Philosophy*, vol. 11, no. 2 (2003), pp. 13–14.

27. Ibid.

28. See http://www.nationmaster.com/country/sz-switzerland/ter-terrorism.

29. For a defense of the "security trumps" view, see Ken Himma, "Privacy vs. Security: Why Privacy Is Not an Absolute Value or Right," *San Diego Law Review*, vol. 44, no. 4 (2007), p. 857.

30. Isaiah Berlin points to a different worry related to safety arguments and governmental paternalism: "Paternalism is despotic, not because it is more oppressive than naked, brutal unenlightened tyranny, nor merely because it ignores the transcendental reason embodied in me, but because it is an insult to my conception of myself as a human being, determined to make my own life in accordance with my own . . . purposes, and, above all, entitled to be recognized as such by others." Isaiah Berlin, "Two Concepts of Liberty," in *Isaiah Berlin: Liberty*, ed. Henry Hardy (Oxford, Eng.: Oxford University Press, 2002), p. 202.

31. Jonathan Wallace and Mark Mangan, *Sex, Laws, and Cyberspace* (New York: Henry Holt, 1997), p. 51.

32. Cited in Christopher Jones, "Averting an Electronic Waterloo," *Wired* (December 16, 1998), http://www.wired.com/politics/law/news/1998/12/16875. See also Eric Jensen, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense," *Stanford Journal of International Law*, vol. 38 (Summer 2002).

33. USA PATRIOT Act (U.S. H.R. 3162, Public Law 107–56), Title II, sec. 213.

34. Ibid., sec. 217.

35. ACLU Report, "Unpatriotic Acts: The FBI's Power to Rifle Through Your Records and Personal Belongings without Telling You" (July 2003), p. 3, http://www.aclu.org/national-security/unpatriotic-acts-fbis-power-rifle-through-your-records-and-personal-belongings-wit (accessed on January 8, 2010).

36. Ibid., p. 5.

37. For an analysis of subpoenas, see Christopher Slobogin, "Subpoenas and Privacy," *DePaul Law Review*, vol. 54 (2005), p. 805.

38. Supreme Court of the United States, 530 U.S. 1237; 120 S. Ct. 2676; 147 L. Ed. 2d 287; 2000 U.S. LEXIS 4126; 68 U.S.L.W. 3756, June 12, 2000, pp. 341–355.