Denver Law Review

Volume 79
Issue 4 *Symposium - Privacy*

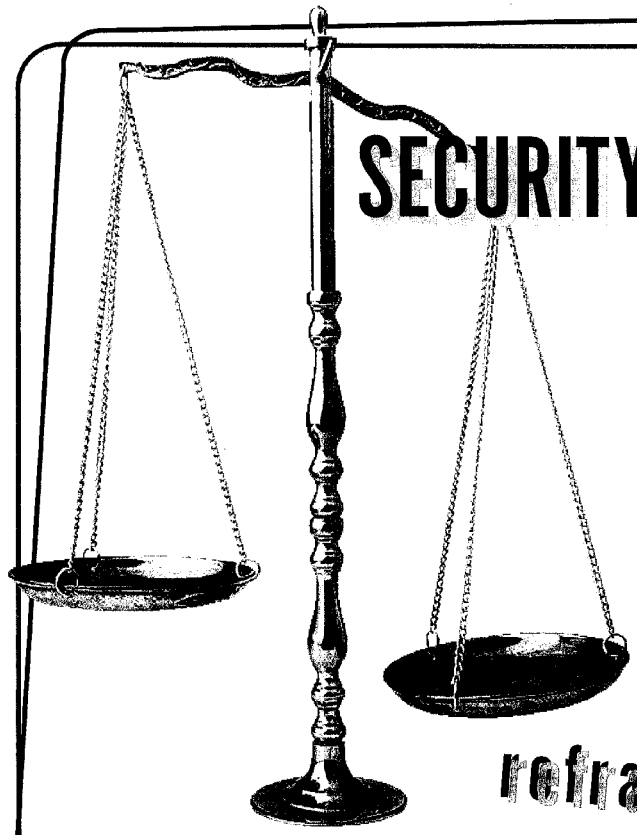
Article 4

January 2002

Security vs. Privacy

Shaun B. Spencer

Security vs. Privacy



SECURITY VS. PRIVACY

reframing the debate

By Shaun B. Spencer*

— "Freedom and fear are at war."**

This essay explores several dimensions of the debate between security and privacy that accompanies many anti-terrorism and law enforcement proposals.

The debate is often framed, either implicitly or explicitly, as a balancing of the tangible harms that a security proposal would prevent, against the intangible harms that an intrusion on privacy would cause. This approach presents the choice between, for example, the disastrous effects of a terrorist airline hijacking, and the relatively minor feeling of discomfort that might flow from presenting a national ID card before boarding. Given those limited choices, what right-thinking person would not choose the latter? This framework of balancing tangible against intangible harms is not merely a rhetorical strategy selected by the proponents of security measures. It is also a way of understanding the debate that flows naturally from the perception that privacy is a mere abstraction, a luxury with little concrete value.

This essay focuses on three ways in which the tangible-versus-intangible decision making framework both overvalues security and undervalues privacy. First, the framework is incomplete because it fails to account for the many unintended consequences that usually flow from security measures. The cumulative effect of those unintended consequences gradually erodes society's very conception of privacy. Yet the tangible-versus-intangible framework implicitly focuses on short-term benefits and consequences, necessarily excluding the long-term effects on privacy.

Second, the contextual specificity that characterizes the tangible-versus-intangible framework overemphasizes the harms on the tangible side of the scale. By embedding the choice between security and privacy in a concrete factual context (such as boarding a plane), the framework all but guarantees that people will decide to guard against the tangible harms.

Finally, the framework draws a false distinction between tangible breaches of security and intangible intrusions on privacy. In fact, the tangible results that

security proposals promise are often empirically suspect. Instead, security proposals serve largely intangible goals, such as allaying people's fears. In contrast, privacy intrusions can have quite tangible consequences that disrupt and inhibit social behavior.

I. UNINTENDED CONSEQUENCES AND THE EXPECTATION-DRIVEN CONCEPTION OF PRIVACY

The tangible-versus-intangible framework described above invariably understates the impact of any particular security measure on privacy. This is so for two related reasons. First, the framework fails to account for the many unintended consequences that inevitably accompany most privacy-intrusive security measures. Second, the framework ignores the fact that our conception of privacy is vulnerable to incremental encroachment not only by the initial security measure, but also by the unintended consequences that follow.[1] The tangible-versus-intangible framework, however, implicitly focuses on short-term benefits and consequences, and therefore excludes long-term effects on privacy.

A. Unintended Consequences

Unintended consequences come in several different forms. The first is secondary use, which occurs when information created or collected for one purpose is used for another, or when an information collection technique developed for one purpose is used for another.[2] One of the most widely acknowledged examples is the Social Security number (SSN). After Congress passed the Social Security Act, the newly-formed Social Security Board[3] had to find a way to track each worker's lifetime earnings, social security contributions, and benefits.[4] The Board assigned a number to each account, and assured citizens that the SSN was to be used solely to identify citizens' retirement accounts.[5] Yet in 1943, President Roosevelt ordered all federal agencies developing their own identification systems to use the SSN "exclusively."[6] Over the next five decades, the SSN's uses spread like wildfire, and by 1998 the Secretary of Health and Human Services acknowledged that the SSN was "in such extraordinarily wide use as to be a *de facto* personal identifier."[7] Today, someone who refuses to divulge her SSN will find it practically impossible to conduct everyday transactions.[8] This is not a peculiarly American phenomenon. Identifying numbers in Canada, Australia, the Netherlands, and Austria have all been put to widespread secondary uses.[9]

Secondary uses can flow to government as well as from it. For decades, direct marketers have collected vast stores of personal information about potential customers. Data profiling has become far more comprehensive with the rise of the Internet, which has put a great deal more personal information at profilers' disposal. Consumers, however, might be surprised to learn that businesses are not just sharing profiles with one another - they are sharing our profiles with law enforcement as well.[10] Sometimes law enforcement need not even ask for the information. Hosts of businesses reportedly opened their customer records to law enforcement agencies in the aftermath of September 11, often in violation of the privacy policies that they claimed they would honor when they collected the data.[11] Moreover, the USA Patriot Act[12] dramatically expanded the types of information about our Web surfing that any "governmental entity" - not merely law enforcement agencies - may monitor without a warrant.[13]

Consumers...might be surprised to learn that businesses are not just sharing profiles with one another - they are sharing our profiles with law enforcement as well

The second kind of unintended consequences are disclosures due to insufficient safeguards over personal information.[14] Any centralized database is vulnerable to hacking, even in such supposedly secure organizations as the Internal Revenue Service.[15] Accidental data disclosures have also become increasingly common. For example, credit agency Experian, drug manufacturer Eli Lilly & Co., and healthcare provider Kaiser Permanente, have all mistakenly divulged confidential information online.[16] Eli Lilly recently entered into a consent decree with the FTC concerning the accidental disclosure of the e-mail addresses of nearly 700 patients with mental illnesses, which Eli Lilly collected through its Prozac.com Web site.[17] Similarly, the House Energy and Commerce Committee recently took its Web site offline after discovering that an internal database concerning the Enron investigation "was left exposed to anyone with a Web browser."[18]

In addition to human error, there is the problem of human corruption. Centralized information is always at the mercy of dishonest or corrupt individuals willing to use it for their own personal or political gain. The abuses of J. Edgar Hoover and Richard Nixon are legendary.[19] But abuses of centralized databases and government surveillance are routine, rather than mere historical anomalies. Many security threat models predict that one percent of an organization's staff will always "be willing to sell or trade confidential information."[20] For example, in a five-year period, 127 employees of the California Department of Motor Vehicles were disciplined "for facilitating ID fraud."[21] Similarly, a Virginia notary public was recently convicted of "helping thousands of undocumented immigrants . . . illegally obtain Virginia

driver's licenses" and ID cards.[22] Until September 21, 2001, Virginia allowed applicants to prove residence with identity papers and a notarized affidavit.[23] *The Washington Post* reported that seven of the September 11 hijackers had obtained Virginia ID cards using that same loophole.[24]

A chilling General Accounting Office report details abuse of centralized crime databases by FBI and other law enforcement officers.[25] The National Crime Information Center ("NCIC") "is the nation's most extensive computerized criminal justice information system" consisting of a centralized database at FBI headquarters "and a coordinated network of federal and state criminal justice information systems."[26] "[I]nsiders pose the greatest threat to NCIC because they know the system and can misuse it by obtaining and selling information to unauthorized individuals, such as private investigators, or altering or deleting information in NCIC records."[27] The report found numerous incidents where insiders disclosed NCIC information to "unauthorized persons, such as private investigators, in exchange for money or other rewards."[28] In one case, a former Arizona law enforcement officer used NCIC information he obtained from three other officers to track down and murder his estranged girlfriend.[29] A Pennsylvania terminal operator used the NCIC to conduct background searches for her boyfriend - a drug dealer - who used the information to determine whether his new clients were undercover agents.[30] And in the tradition of Nixon's "dirty tricks," some local officials unlawfully used NCIC information to discredit political rivals.[31]

B. Incremental Encroachment and the Expectation-Driven Conception of Privacy

In any privacy-related debate, it is important to understand that privacy is generally defined by our own expectations.[32] Judicial privacy doctrines developed under the Fourth Amendment and in tort law define the scope of privacy by reference to whether an individual has a reasonable expectation of privacy in a particular context.[33] Even legislative action on privacy issues reflects social expectations of privacy. Given the variety of powerful interests that might be adversely affected by privacy-protective legislation, such legislation is extremely unlikely to pass unless it is supported by strong public perceptions of what is appropriately kept "private" in a given context.[34] Privacy, in short, is only as extensive as we believe it is.

This expectation-driven conception renders privacy vulnerable to incremental encroachment. Sweeping intrusions into the private sphere may fail because they conflict with firmly held expectations of privacy.[35] However, repeated moderate intrusions by governments and institutions capable of influencing social behavior can gradually erode expectations of privacy. The necessarily imprecise nature of group preferences means that we usually find a "gray area" where societal expectations are unsettled. The gradual erosion of privacy occurs through repeated incursions into this gray area.[36]

Thus, the effects of any single encroachment in fact reach much farther than the tangible-versus-intangible framework can acknowledge. The tangible-versus-intangible framework focuses too narrowly on the present, to the exclusion of the inevitable unintended consequences that will diminish privacy expectations far more than the initial security proposal. The framework commonly examines the extent to which a given proposal would intrude on our *current* expectations of privacy, and asks whether that intrusion is worth the promised security benefits.

To take just one example, proponents of a national ID card might suggest that limiting such a card to uses at borders and airports would have only minimal privacy implications, in part because people are already used to showing some form of ID when they travel.[37] But that view ignores the unintended consequences that would inevitably follow the creation of a card, even for initially limited purposes.[38] The urge to expand the uses of a biometric-based national ID - and the centralized database that would inevitably support it[39] - would be irresistible. A centralized database would facilitate the card's uses by government agencies responsible for welfare benefits, law enforcement, and medical data.[40] Businesses would push to use the national ID card, perhaps at first for credit and banking purposes, but eventually for as many purposes as the SSN and driver's license are currently used.[41]

Such plans are already underway. The American Association of Motor Vehicles Administrators ("AAMVA") recently proposed uniform national standards for all state-issued driver's licenses, which would encode a variety of information about each license holder, including a "biometric identifier."[42] Companies are already marketing scanners that can not only read, but also store, information from the AAMVA-standardized driver's license.[43] Scanners are being marketed to bars, restaurants, car dealerships, and convenience stores, and suggested for use by health clubs, personal trainers, and for the general retail market.[44] AAMVA itself has proposed sharing its model with banks, the travel industry, car rental agencies, insurance companies, and retailers.[45] Furthermore, as illustrated above, centralized databases are ripe for abuse from within and without, and increase dramatically the chance for accidental disclosures. As these uses and abuses accumulated in incremental steps, we would gradually come to expect less and less privacy in a variety of contexts - clearing the way for further encroachment. Each inch of ground that society yields in the private sphere renders the next inch more vulnerable. Yet the tangible-versus-intangible framework ignores these long-term effects by limiting its temporal focus to the present.

continued on page 554

continued from page 521

II. THE TANGIBLE, THE INTANGIBLE, AND THE PROBLEM OF CONTEXT

The tangible-versus-intangible framework also overvalues security because it embeds the choice between tangible and intangible in a specific factual context, such as the process of boarding an airplane - a context that is itself tangible. As explained below, framing the question in such a context inevitably leads people to guard against the more tangible harms.

In an age pervaded by cost-benefit analysis, there is an urge to reduce all policy decisions to a balance sheet. But we lack a single currency in which to measure the relative value of the privacy and security interests. Attempts to equate a "unit" of privacy to a "unit" of security, for example, are doomed to fail. As we attempt to choose between these two incommensurable goods,[46] we lack a simple, cost-benefit approach to the balancing.

Of course, the mere fact that two goods are incommensurable need not skew the calculus in one direction or the other; it simply makes the choice more difficult. Indeed, incommensurability characterizes most attempts to balance competing goods.[47] Despite our lack of a common "metric" in which to measure those goods, we find ways to make hard decisions.

What does skew the calculus, however, is the perception that breaches of security lead to tangible harms, while intrusions on privacy lead to intangible harms. Proponents of security measures can raise the specter of specific, all too tangible acts of violence. Failures of security can lead to concrete harms that have shaped our collective experience, such as the bombing of the Marine barracks in Beirut, the bombing of the American Airlines flight over Lockerbie, Timothy McVeigh's attack in Oklahoma City, and September 11.

Privacy, in contrast, is often considered a purely abstract value, one that we can sacrifice in a particular instance without risking any real, tangible harm.[48] Many who argue for the preservation of privacy stress its importance for purposes that are themselves abstract, such as personal autonomy,[49] personal and political identity,[50] and freedom of expression and association.[51] Moreover, privacy is a highly subjective concept, one that can vary from person to person.[52]

Comparing tangible and intangible consequences in the context of specific security proposals is likely to overstate the value of the tangible. As Julie Cohen observed in a related context, "Privacy, like other dignity-related goods, has inherently nonmonetizable dimensions. These dimensions may be lost or distorted beyond recognition in the translation to dollars and cents."[53] So a consumer making a decision about a transaction, with consequences defined in monetary terms, will find it difficult to translate the intangible, nonmonetizable dimensions of privacy into that decision making equation.[54] The specific context in which the consumer must decide constrains her decision making calculus.

A similar problem of context frustrates privacy advocates in the debate over privacy and security.[55] Debates over security proposals are often grounded in specific factual contexts in which the privacy implications appear innocuous, while a security breach could lead to grave harm. British Home Secretary David Blunkett colorfully contrasted the danger of terrorist attacks with abstract notions of privacy and liberty: "We can live in a world with airy-fairy civil liberties and believe the best in everybody and then they destroy us."[56] Oracle CEO Larry Ellison expressed a similar sentiment in testimony submitted to a congressional subcommittee considering national ID cards:

> Two hundred years ago, Thomas Jefferson warned us that our liberties were at risk unless we exercised 'eternal vigilance.' Jefferson lived in an age of aristocrats and monarchs. We live in a nuclear age with the threat of terrorists getting their hands on weapons with the capacity to destroy entire cities. Only by giving our intelligence and law enforcement agencies better tools and more latitude to pursue terrorists can we expect to save life and liberty together.[57]

Former National Security Agency general counsel Stewart Baker summed up this perspective:

> We as a people are willing to trade a little less privacy for a little more security. If using more intrusive technology is the only way to prevent horrible crimes, chances are that we'll decide to use the technology, then adjust our sense of what is private and what is not.[58]

Security proposals implicitly summon images of a horrible reprise to the World Trade Center and Pentagon attacks, as well as attacks using biological or nuclear weapons. Juxtaposed against those images are what some characterize as "airy-fairy" notions of privacy.[59] Though they do not explicitly deny that privacy has some value in the abstract, they urge people to sacrifice it in particular cases to prevent "real," tangible harms.[60] With the issue framed in such stark terms, one would be hard pressed to argue that, *in just this one case,* abstract privacy values should not yield to the need to prevent attacks by terrorists with biological and nuclear weapons.[61]

Furthermore, differences in the scale upon which security and privacy benefits are observable exaggerate our perception of privacy benefits as intangible and security benefits as tangible. The example of airport checkpoint searches helps illustrate this point. As I am frisked or scanned, I cannot possibly see the cumulative effect across society of implementing these types of uniform measures. I experience only my search and the searches of a few

continued on page 571

continued from page 554
people before and after me. A single individual cannot appreciate the full effect of widespread personal searches of everyday American travelers.

In contrast, the security benefits that appear to flow from the searches seem quite tangible. I board the plane with the knowledge that I pose no risk, and the belief that those around me pose no risk either, since they all endured the same scrutiny as I did. Then, after the flight goes smoothly, the safe landing reinforces the notion that security measures increase my safety. Of course, the many things that I failed to perceive are precisely the things that would undermine my confidence in security measures. For example, I may not have realized that the metal detector through which my fellow passengers and I passed had been inadvertently unplugged.[62] I may not have noticed one of my fellow passengers boarding the plane despite the fact that his driver's license did not match the name on his ticket.[63] Nor might I understand that such oversights are inevitable in passenger checks and baggage scans, because the "signal rate" - the frequency with which terrorists or impostors appear at the gate or weapons appear in the baggage - is so low.[64] Instead, I see only the safe result, which confirms my perception that security measures produce tangible benefits, or more specifically, that they avert tangible harms.

The distortion of individual perception in favor of security is obviously heightened in the wake of September 11. In today's climate, with physical and emotional scars from terrorist attacks still present on the landscape and in our lives, the perceived tangible benefits of security measures are magnified in the eyes of many. For that reason, we should not be surprised at the surface appeal of suggesting that we sacrifice "a little " privacy to preserve the tangible benefits of security. An important task for privacy advocates is to focus attention on how even seemingly limited intrusions on privacy can have consequences that reach far beyond the limited context in which they are proposed.

III. REVEALING THE TANGIBLE AS INTANGIBLE

Finally, I suggest that the tangible-versus-intangible framework is misleading. Measures alleged to yield tangible security benefits in fact serve many intangible purposes. Admittedly, in the wake of September 11, it is difficult to imagine a more tangible concern than the destructive effects of a terrorist attack. Many responses to these attacks, however, are not merely aimed at preventing such tangible harms. Instead, they serve in large measure to preserve merely the *perception* of security - the intangible notion that our government can, in fact, protect us from terrorism.

Jeffrey Rosen's investigation of Britain's experience with terrorism and video surveillance illustrates how security measures can serve predominantly intangible concerns.[65] In the wake of two IRA bombings in London's financial district, the government responded by installing surveillance cameras at the city's entry points.[66] Fear of terrorism continued, and the cameras - closed circuit TV, or "CCTV" - multiplied beyond anyone's expectations, both in London and throughout Britain.[67] Under Prime Minister John Major, the government devoted "more than three-quarters of its crime-prevention budget to encourage local authorities to install CCTV."[68] "[B]y 1998, 440 city centers" had surveillance camera networks.[69] Rosen's report estimates that "there are 2.5 million surveillance cameras in Britain," and that 300 different cameras photograph the average Briton every day.[70]

How many terrorists has Britain caught using this pervasive surveillance network? None.[71] "Although the cameras in Britain were initially justified as a way of combating terrorism, they soon came to serve a very different function. The cameras are designed not to produce arrests but to make people feel that they are being watched at all times."[72] And the people monitoring the cameras are most likely to focus on unconventional behavior in public, young men (especially if they are dark skinned), and attractive young women.[73] Cameras in London are most productive tracking "car thieves and traffic offenders. 'The technology here is geared up to terrorism,'" said London's press officer.[74] "'The fact that we're getting ordinary people - burglars stealing cars - as a result of it is sort of a bonus.'"[75] But there is no evidence that the cameras have prevented terrorism or other serious crime.[76]

The national ID card debate offers another timely illustration of the intangible nature of security concerns. Despite all best intentions, a national ID card will not prevent terrorism. Most countries have national ID cards or ID numbers,[77] and yet terrorism is a problem across the globe. September 11 hijacker Khalid Al-Midhar was on the INS's "watch list" of potential terrorists for nearly a year before the attacks, yet he boarded one of the hijacked flights using a ticket he bought in his own name.[78] Seven of the hijackers obtained fraudulent IDs from the State of Virginia.[79] Even more disturbingly, the INS recently notified a Florida flight school that it had approved student visas for Mohamet Atta and Marwan Alshehhi - six months *after* Atta and Alshehhi carried out the September 11 attacks, and in the midst of one of the most important and publicized law enforcement investigations in history.[80] Moreover, at Boston's Logan Airport, from which one of the September 11 flights originated, a man recently passed through two airport security checkpoints despite the fact that the name on his government-issued ID did not match the name on his ticket.[81]

Nonetheless, in the wake of the attacks, the American public threw its support behind a national ID card. Seventy percent of respondents to a Pew Research Center poll supported a "must carry" card - a card that the government would require us to carry on our person at all times and "show a police officer on request."[82] Perhaps most disturbingly, 49% of respondents to a CNN/USA Today/Gallup poll supported a

special national ID card that only Arab-Americans would be required to carry.[83]

Now, did the public suddenly review empirical evidence suggesting that national ID cards prevent terrorism? Certainly not. This was a reflexive response to the perception of vulnerability. The public needed to believe that there was something the government could do to prevent this type of attack. In the wake of September 11, fear and self-delusion are empowered to drive the debate over security proposals. Larry Ellison claims that people need not give up their privacy, only their "illusions" of privacy.[84] In the privacy-versus-security debate, however, privacy advocates often find themselves opposing efforts to preserve the mere illusion of security.

It is not enough, however, to point out the intangible nature of the security interest. That alone is unlikely to change the debate, precisely because people want, at some level, to believe that government can protect them against foreign threats. Government, too, has an essential interest in preserving this perception.

Accordingly, privacy advocates must also identify the tangible effects of preserving privacy against government intrusion. Speaking to a class at Harvard's John F. Kennedy School of Government in the fall of 2000, Simson Garfinkel said that privacy advocates need to show "where the bodies are buried."[85] I take him to mean that privacy advocates will make relatively little progress until they can show specific, tangible harms flowing from intrusions on privacy. His comment recognizes the tangible-versus-intangible perception that privacy advocates often confront.

Garfinkel's point finds support in the patchwork of privacy laws on the books today. In the few areas where we have found metaphorical "buried bodies," Congress has offered a healthy measure of privacy protection, albeit in the most narrow of circumstances. For example, Congress passed the Driver's Privacy Protection Act in the wake of the 1989 stalking and murder of actress Rebecca Schaeffer by a deranged fan who found her address through the department of motor vehicles.[86] Similarly, Congress passed the Video Privacy Protection Act after Judge Robert Bork's confirmation hearings, during which a *Washington Times* reporter shamelessly obtained copies of Judge Bork's video store rental records.[87]

Privacy advocates, then, must emphasize the tangible consequences of what some would dismiss as intangible aspects of privacy - those related to autonomy, to freedom of association and expression, and to personal and political identity. Joanna Malamud Smith notes that systematic deprivation of privacy by government is a hallmark of oppressive, totalitarian regimes.[88] Describing abuses in Nazi-occupied France, cold war East Germany, and the Soviet Union, Smith observes that:

> Constantly spying and then confronting people with what are often petty transgressions is a way of maintaining social control and unnerving and disempowering opposition . . . . [E]ven when one shakes real pursuers, it is often hard to rid oneself of the feeling of being watched - which is why surveillance is an extremely powerful way to control people.[89]

Smith quotes a memoir of a woman who lived under Stalinism: "'An existence like this leaves its mark. We all became slightly unbalanced mentally - not exactly ill, but not normal either: suspicious, mendacious, confused and inhibited in our speech . . . .'"[90] Such campaigns are nothing less than state-run terrorism.[91] Viewed from this perspective, privacy seems less an intangible abstraction than it does an instrumental value that produces tangible effects essential to a free citizenry.

Nor are deliberate assaults on privacy confined to totalitarian states. Smith also notes that the U.S. government has spied on dissenters such as Emma Goldman, the Wobblies, Malcolm X, and Martin Luther King, Jr.[92] Smith recounts the FBI's attempts to force King to commit suicide by sending him and his wife videotapes of King's sexual infidelities.[93] "Along with the videos, King received an anonymous letter. Knowing that he had attempted suicide as a twelve-year-old child, the writer, an FBI agent, encouraged King to end his life."[94] J. Edgar Hoover used the FBI's surveillance capabilities for his personal gain. One Hoover biographer tells the story of a magazine publisher who was planning an exposé on Hoover and the FBI.[95] "Hoover struck first, viciously. Favored newspaper contacts all over the country received a plain brown envelope with no return address. Inside was a packet of photographs showing the publisher's wife engaged in fellatio with her black chauffeur."[96] Thus, invasions of privacy empower the invader to control information and quell dissent.

IV. CONCLUSION

Today, police in Washington, D.C. are building a centralized network of surveillance cameras that will blanket the District of Columbia.[97] This unprecedented initiative operates within the cryptically named "Synchronized Operations Command Complex" (the "SOCC").[98] In the SOCC's Joint Operation Command Center, fifty workers monitor a wall of video screens hooked up to surveillance cameras.[99] The network already includes 200 cameras in public schools.[100] The SOCC will soon add another 200 in subways and parks.[101] It will also link the video from surveillance cameras that monitor intersections for drivers who run red lights, and from private cameras in banks, retail stores, hotels, and apartment buildings.[102] According to the director of the project, "I don't think there's really a limit on the

feeds it can take. We're trying to build . . . the capability to tap into not only video but databases and systems across the region."[103]

> A man living under a similar surveillance network in Britain observed: I am gay and I might want to kiss my boyfriend in Victoria Square at 2 in the morning. I would not kiss my boyfriend now. I am aware that it has altered the way I might behave. Something like that might be regarded as an offense against public decency.[104]

Despite this, the man maintains that "the benefits of the cameras outweighed the costs, because 'thousands of people *feel* safer.'"[105] As William Safire asks: "Is this the kind of world we want?"[106]

Policymakers are now deciding the fate of the D.C. video surveillance network, in addition to countless other security measures. If they accept uncritically the tangible-versus-intangible framework, their decision may be foreordained. The framework suggests a simple question: Which is more costly - the destruction from a terrorist attack on our capitol, or the discomfort that a commuter, tourist, or student might feel when passing innocently before a surveillance camera?

This essay has tried to illuminate what really lies on either side of the scale. First, the framework's short-term temporal focus necessarily excludes the future uses of such a surveillance network. Even today, the project is considering linking not only surveillance cameras, but also "databases and systems across the region."[107] The potential uses of centralized video surveillance and databases are unlimited, as are the long-term privacy intrusions of such expanded uses.

Second, the factual context in which the question is posed necessarily suggests the answer. We are left to imagine a known terrorist riding the Metro or walking across the Capitol Mall en route to his target. Even if one understands as a conceptual matter that the privacy consequences of pervasive surveillance will be widespread, it is difficult to measure such seemingly intangible harms against the prospect of another devastating terrorist attack. To accept the limited context in which the framework places the issue is to determine the outcome of the decision.

Finally, even if the surveillance system employed facial recognition technology that was 100% accurate - an extremely unlikely possibility[108] - it could not prevent terrorist attacks. Only two of the nineteen September 11 hijackers were on the terrorist watch list; the rest were unknown to intelligence or law enforcement officials before the attacks.[109] To catch even those two with facial recognition technology, the government would have needed not only their names, but also digital images of their faces. Like the pervasive surveillance network in Britain, centralized surveillance in D.C. would be better suited to making people *feel* safe rather than actually stopping terrorists.

So the question that policymakers must in fact decide is far more complex than the tangible-versus-intangible framework would suggest. The security side of the scale is much less substantial than many would suspect, because it is both empirically suspect and comprised in large part of mere *perceptions* of security. Similarly, the privacy side is weightier than the framework would admit, because it includes the long-term effects that unintended consequences will have on privacy, and because it considers the effect that security measures will have on the entire community, rather than on a single individual passing a checkpoint. Moreover, the privacy side of the scale holds far more than mere abstractions. Instead, intrusions on privacy can change behavior, control information, and deter political and cultural dissent. This more comprehensive way of approaching the security-versus-privacy debate makes decision-makers far more likely to protect privacy.

In an important address to the nation, President Bush warned, "Freedom and fear are at war."[110] In that context, Bush equated freedom with America, and fear with the Taliban and Al Qaeda. In the aftermath of September 11, however, privacy values are safeguarding our freedom, while some security proposals seek mainly to alleviate our fear. Freedom and fear are indeed at war. Let us not sacrifice the former by indulging the latter.

The author is a Climenko/Thayer Lecturer on Law at Harvard Law School. Before joining Harvard, he taught as an Adjunct Professor at Boston College Law School, and practiced in the litigation department of the Boston law firm Bingham Dana. The ideas in Part I of this essay are drawn substantially from the author's forthcoming article, Reasonable Expectations and the Erosion of Privacy, 39 SAN DIEGO L. REV. (forthcoming 2002). The author is grateful for the comments of Richard Sobel, and for the extensive contributions of Lawrence Friedman. The author also thanks Tanya Thiessen and the Denver University Law Review for organizing this important Symposium.