

Epilogue: An Escape from Fear

By the time you read this, North America and Europe may have been shaken by new waves of terrorist attacks. In the aftermath of the traumatic events, nothing in this book offers any reason to expect that the public will demand laws and technologies that protect liberty and security at the same time. On the contrary, everything we know about the vulnerabilities of the Naked Crowd suggests that new fears will be accompanied by new claims that everything has changed and that we can no longer afford to defend the American values – such as privacy or freedom – that we had taken for granted in calmer times. Refusing to evaluate whether or not these new laws and technologies in fact increase security, the public may willingly acquiesce in the destruction of privacy without getting anything tangible in return. Even if the actual threats are limited and contained, the fears they engender may be exaggerated and corrosive. It's not hard to imagine a mentality of permanent crisis on the part of the public, leading to the steady encroachment of technologies of surveillance and profiling that have no discernable impact in preventing terrorism. And the ineffectiveness of the technologies, perhaps, will provoke further calls for their proliferation.

In light of what we know about the psychology of the Naked Crowd, this scenario may materialize; perhaps it is more likely than not to do so. But each of the relevant actors – the technologists, the lawmakers, the courts, and the public – might be persuaded to strike a more reasonable balance between liberty and security, if each were addressed in terms they could

understand and accept. In this Epilogue, I'd like to review a range of more optimistic scenarios that could save America and other Western democracies from the paralyzing fear that is our greatest enemy. In particular, I'd like to evaluate four different models for protecting liberty and security: the transparency model, the control use model, the judicial oversight model, and the political oversight model. Although each has proved useful in different democracies at different times, I want to argue that political oversight provides the most promising path for America in the twenty-first century.

The transparency model is associated with the author David Brin. In *The Transparent Society*, Brin argues that the proliferation of cameras and surveillance devices is inevitable, unstoppable, and largely beneficial. Instead of trying in vain to resist the spread of cameras and databases with ineffective laws and regulations, Brin insists, we should focus instead on ensuring that everyone can view each others' cameras so that "average citizens share, along with the mighty, the right to access these universal monitors."¹ Brin imagines the wonderful benefits of a metropolis in which every citizen can "use his or her wristwatch television to call up images from any camera in town."² In the middle of the night, he enthuses, pedestrians could dial up street cameras to ensure that assailants aren't lurking around the corner; and suitors who are running late can peer benignly at restaurants across town to make sure that their dates haven't left in a huff. Brin insists that police officers will act more responsibly in arresting criminals if they are sure that citizens are scrutinizing their conduct at all times. The danger, he says, isn't that surveillance technology will be used by too many people but too few. He sings the praises of "wearables" – tiny computers that combine the attributes of a portable camcorder, cell phone, laptop and pager,

and have been used by small bands of “sousveillance” activists in San Francisco and Los Angeles to film the public activities of shopkeepers, ordinary citizens, and the police. He doesn’t quail at the idea that the government might dispatch tiny gnat cameras to swarm through the air and spy on citizens, because he is confident that citizens can develop antignat cameras to expose the robotic intruders and force the government to obtain warrants instead.³ He embraces the possibility of profiling citizens on the basis of their proclivities and behavior, suggesting that a “glass house” effect can protect us from the worst abuses. He praises the benefits of a national I.D. card and integrated databases, but insists that citizens should demand new levels of “transparency, accountability and outright nakedness on the part of government officials” in exchange. “Create a true inspector general of the United States,” he told me. “Draft citizen juries with the power to walk in through any door and badger even the C.I.A. director with questions. Rename the White House the Glass House. Each time the government has asked for new powers, we’ve said, ‘Fine. Show me yours first. Strip.’”

Brin is an engaging provocateur, and he usefully calls our attention to the ways that technologies of transparency can promote democratic accountability. Many surveillance technologies that seem to threaten liberty and privacy when the government refuses to make them transparent seem more reasonable when citizens can confirm that they are being deployed in precisely the ways that the government promises. Consider the example of the e-mail search program originally known as Carnivore. Carnivore is a search engine that allows the government, when it is searching for a particular e-mail, to sift through all of the messages that have been sent and received by a particular Internet Service Provider. When the search engine finds the suspicious

message, it sets off an alert. If Carnivore operates in the way the government suggests, it might be viewed as a perfectly reasonable search, along the model of the Blob Machine, since it focuses with laser-like precision on guilty information and reveals no innocent information to any human being. By contrast, if Carnivore were seized by rogue government agents, it might be deployed to sift through innocent as well as suspicious e-mails, which looks more like the kind of fishing expedition that the framers of the Fourth Amendment meant to prohibit. The way for independent third parties to ensure that Carnivore is being operated reasonably, rather than unreasonably, is for the government to reveal the source code for Carnivore. But the government has refused to reveal the source code, claiming unconvincingly that it would compromise the security of the system. By emphasizing the importance of open sourcing for surveillance technologies in general, Brin reminds us that transparency may help to promote liberty without threatening security.

But although Brin usefully emphasizes the importance of technologies of accountability, he exaggerates the benefits of living in a transparent society and seriously underestimates the costs. On the benefits side, he uncritically cites studies from two British cities – Glasgow and King’s Lynn – purporting to show a connection between the installation of CCTV cameras and a drop in crime.⁴ Both studies were excluded as methodologically unreliable by the British Home Office’s comprehensive review of the empirical evidence about the effectiveness of CCTV, on the grounds that they did not include crime data for control areas.⁵ The Home Office’s comprehensive review, as I mentioned in the Chapter One, found no convincing evidence of a connection between the spread of CCTV and the decline of violent crime, and a negligible effect

on crime in public transportation systems or city centers. Throughout Brin's book, one finds similar technopositivistic enthusiasm about the possibility of security benefits for surveillance technologies without a careful evaluation of the empirical evidence.

At the same time, Brin is far too glib about the costs of living in a transparent society. "In the twenty-first century, we have to follow the advice of the journalist who said: Live your life as if today's mistake may wind up on page 23," he told me. "In such a world, we're all going to have to become more tolerant of each other's small mistakes and to try harder not to make big ones." But Brin is too optimistic about "our" ability to tolerate the mistakes of those we have never met; and his optimism is based on the conflation of information with knowledge. Neighbors in a small town can (sometimes) tolerate each others' weakness because they know each other whole and in context. By contrast those who have never met each other face to face can have information about each other but they can never really know each other. As a result, in a world of short attention spans, small mistakes come to define people rather than being a basis for tolerance and understanding.

Brin concludes his book with a sunny vision of the Omnipicon as a global village, with kindly citizens looking over the shoulders of their virtual neighbors to ensure the mutual safety of all. "Busybodies will gossip but you'll know *their* secrets – and you'll be able to leave your doors unlocked. Your bedroom will be protected from snoops by electronic guardians, but most of all by the fact that voyeurs and snoops will fear being caught Better to know our neighbors (in their multitudes) than to live a fiction of splendid, lonely isolation."⁶

Brin's vision is romantic but unconvincing. True knowledge takes place only gradually: it is a slow, gradual process of mutual revelation. "Real friendship is a slow grower; and never thrives, unless ingrafted upon a stock of known and reciprocal merit,"⁷ wrote Lord Chesterfield. But we can't possibly take the time to know and be known by millions of virtual neighbors whom we will never meet. We can only reveal snippets of ourselves, and can only have access to snippets of others; and we risk constantly being judged out of context and confusing the part for the whole. When surveillance technologies that judge people out of context are deployed by government rather than by fellow citizens, furthermore, the dangers of mistaken identification become far more acute. If wrongly identified by a digital database or profiling system, people can lose jobs, be denied access to airports, federal buildings, and health insurance, and be arrested or blackmailed. And although Brin is optimistic about the possibility that citizens might choose technologies like the Blob Machine that protect security while also protecting privacy, he is ultimately too much of a populist to think in a cool eyed fashion about how to promote the adoption of these technologies if citizens prove indifferent to them. "We may vote as people to tell the watchers: 'make your cameras just acute enough to catch the bad guys,'" he says. But he has nothing to say about what happens when we vote to install cameras that inhibit the innocent without catching the guilty. For this reason, it seems useful to remember Brin's lessons about the virtues of transparency in government while resisting his enthusiasm about the virtues of living in glass houses.

The second model for balancing liberty and security might be called the control use model. One of its advocates, William Stuntz, argues that the executive should be given expanded

surveillance authority but only if it is prohibited from using any evidence that the surveillance reveals to prosecute low level crimes, as opposed to murder or terrorism. Stuntz's insight is powerful, and he reminds us of the dangerous possibility that general data searches, justified in the name of fighting serious crimes, may quickly become excuses for fishing expeditions that yield evidence of relatively trivial crimes. But there are obvious objections to the control use model. Many citizens see nothing wrong with using broad surveillance authority to collect evidence of trivial as well as serious crimes. And as the prosecution of Al Capone demonstrates, there are clearly benefits to using convictions for low level crimes, such as tax evasion, to imprison suspects whom the police know to have committed far more dangerous crimes, but can't quite prove the more serious charges. Before and after 9/11, federal officials have used versions of the Al Capone strategy to prosecute those whom they suspect as terrorists without having proof beyond reasonable doubt.

In a case from 1991, for example, the State of Missouri charged Zein Hassan Isa, a naturalized U.S. citizen born in Palestine, with the murder of his daughter. Isa had been targeted as a suspected agent of the Palestinian Liberation Organization, and the government obtained a foreign intelligence surveillance warrant to tap his home. While he was being covertly tapped, Isa became enraged at finding his daughter at home with a boyfriend, an lapse of virtue that he claimed dishonored his family. Within earshot of the microphones, he took a knife and stabbed her to death. "Quiet, little one!" he exclaimed in Arabic as his wife held the daughter down by the hair. "Die quickly, my daughter, die!"⁸ When the State of Missouri tried to introduce the foreign intelligence surveillance tapes as part of Isa's prosecution for murder, Isa objected that

his Fourth Amendments rights had been violated on the grounds that the tapes concerned a “private domestic matter” that was not relevant to the foreign intelligence investigation that had authorized the original wiretap. But a federal court rejected his argument, noting that the Foreign Intelligence Surveillance act allows the retention and sharing of information that is “evidence of a crime” and contains no requirement that the crime be related to foreign intelligence.⁹ The court noted other cases where suspected agents of foreign powers had been indicted for credit card fraud.¹⁰ Therefore, the court refused to suppress the evidence.

The court’s conclusion seems correct on several levels: murder is too serious a crime to overlook, and the Foreign Intelligence Surveillance court had already found probable cause to believe that Isa was an agent of a foreign power; for this reason, indicting him for a crime not directly related to terrorism might have helped to prevent him from committing acts of terror. (There was also a dispute about whether he had killed the daughter to conceal his terrorist plans.) The Foreign Intelligence Court of Review made a similar argument in upholding the Bush administration’s effort to tear down the rigid wall that separates foreign intelligence surveillance from criminal prosecution. In efforts to prevent terrorism, the Court recognized, criminal prosecution and intelligence gathering may converge: arresting and prosecuting terrorists may be the best way of preventing them from carrying out their violent schemes.¹¹ Similarly, ordinary crimes may be intertwined with foreign intelligence crimes: as the Court noted, if a group of terrorists committed bank robberies to finance the manufacture of bombs, evidence of the bank robbery should be treated as evidence of the terrorist act.¹² For this reason, the Court rejected the argument that the government can engage in sweeping foreign intelligence surveillance without a

judicial warrant only when its “primary purpose” is intelligence gathering rather than law enforcement, and it also emphasized that the government should be free to prosecute suspected terrorists for lower level crimes that are discovered in the course of the surveillance. At the same time, the Court emphasized that foreign intelligence surveillance shouldn’t be used as a pretext or excuse to investigate ordinary crimes that are completely unrelated to terrorists acts. When criminal prosecution is the sole purpose of an investigation, therefore, the government must obtain an ordinary criminal warrant.

All this suggests that broad forms of what Roger Clarke calls “personal dataveillance” should be permissible when the government has probable cause to believe that a particular individual is especially dangerous. And once the government plausibly believes that an individual is dangerous, it should be able to resort to the Al Capone Strategy, prosecuting him for lower level crimes unrelated to terrorism as a way of getting him off the streets. By contrast, when the government engages in “mass dataveillance,” without cause to suspect particular individuals of particular crimes, the situation looks very different. If the government were able to use the Al Capone strategy here, and prosecute people for crimes unrelated to terrorism when they pose no special dangers to society at large, many citizens might feel as if they were living in a police state. For this reason, mass dataveillance could be permitted as a tool of risk prediction, as opposed to criminal investigation, only when there are limitations imposed on how the government can use evidence of ordinary crimes unrelated to terrorism. A model here might be the German wiretap law, which allows intelligence authorities to use wiretaps for domestic surveillance only when there is factual basis to suspect that one of a list of crimes involving a

threat to national security has been or is about to be committed. The German law says that evidence obtained through wiretapping can only be used in the investigation and prosecution of the specified national security crimes or certain other serious crimes; if the intelligence officers find evidence of low level crimes, they may not share it with law enforcement officers or introduce it in court.¹³ Although legal limitations on the use of evidence obtained by mass dataveillance are worth exploring, they may be difficult to sustain in practice for the reasons I discussed in Chapter Three: in America, the political pressure to expand the list of crimes for which wiretaps could be justified has proved too overwhelming to resist.

A third model for balancing liberty and security focuses on judicial oversight. I've argued that it would be foolish to expect that judges will (or should) take positions about privacy that vary dramatically from what the public demands. Conceptions of what kinds of searches are reasonable and unreasonable under the Constitution depend crucially on public conceptions of reasonableness, and because judges have shown little willingness to cast themselves as crusaders for privacy in the past, there is little reason to count on them to pave the way in the immediate future.

Over the long term, it's possible that some kind of constitutional restraints on dataveillance and electronic monitoring of citizens might evolve. Social changes, after all, move slowly through the courts: nearly two decades elapsed between the time that the California Supreme Court first invalidated an anti-miscegenation law in 1948 and the time the Supreme Court struck down all state laws prohibiting interracial marriage in 1967.¹⁴ (It took Alabama voters another three

decades before they repealed the last such law in 2000).¹⁵ Along the same lines, it took the Supreme Court nearly 40 years from 1928, when it held that wiretapping wasn't a search because it didn't involve a physical trespass, to 1967, when it changed its mind and held that wiretapping is an unreasonable search because the Fourth Amendment protects "people, not places."¹⁶

Although the transformation may be similarly slow in coming, it's not impossible to imagine that the Supreme Court might gradually abandon its circular focus on subjective expectations of privacy and come to recognize, as Justice Harlan did, that the analysis of unreasonable searches in an electronic age must "transcend the search for subjective expectations or legal attributions of assumption of risk."¹⁷ In Harlan's view, the question of whether a particular search is unreasonable must be answered "by assessing the nature of a particular practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the conduct as a technique of law enforcement." He concluded that "[t]he impact of the practice of third-party bugging, must, I think, be considered such as to undermine that confidence and sense of security in dealing with one another that is characteristic of individual relationships between citizens in a free society."¹⁸

Harlan was in dissent, and his views have never attracted a Supreme Court majority. But Canada's privacy commissioner challenged the use of video surveillance on similar grounds, claiming that ubiquitous video monitoring, like ubiquitous hidden microphones, inhibits the spontaneity that can only flourish if individuals are secure in the knowledge that their daily interactions in a free society aren't being routinely being recorded or observed by the state. At the privacy commissioners' request, Gérard La Forest, the former justice of the Canadian

Supreme Court, wrote an eloquent advisory opinion expressing his own view that generalized surveillance, whether recorded or not, violated “the right to be secure against unreasonable search or seizure” guaranteed by the Section 8 of the Canadian Charter. Mirroring Harlan’s reasoning, he insisted that the constitutional test shouldn’t be whether a particular surveillance technology is in widespread use, but whether it is “inconsistent with the aims of a free and open society.” In his view, dragnet video surveillance in public places, could not pass this test, because it was more consistent with a police state than a free society. “We may not have a reasonable expectation that the police will *never* observe our activities in public spaces, either incidentally or as part of a targeted investigation,” he wrote. “But surely it is reasonable to expect that they will not *always* do so.”¹⁹ Unlike surveillance which is targeted at particular suspects, in other words, La Forest concluded that ubiquitous video surveillance in public is unreasonable because it inhibits the innocent and guilty alike.

There is, however, an unsettling element of subjectivity in asking judges to make a value judgment about whether or not a particular surveillance technology is consistent “with the aims of a free and open society.”²⁰ In my view, this inquiry gives courts too much discretion to decide what kind of freedom from surveillance they think an open society requires. In examining a new technology of dataveillance, courts might instead be persuaded to follow the lead suggested by Harlan himself, examining the “extent of its impact on the individual’s sense of security balanced against the utility of the conduct as a technique of law enforcement.”²¹ This cost-benefit analysis could ask the kind of question courts have traditionally asked in deciding whether or not to permit a search without a warrant or individualized suspicion, examining the

invasiveness of the search; the amount of discretion entrusted to the police officers; the necessity of the search; and its likely effectiveness. These questions are consistent with the ones that the Supreme Court generally asks in deciding whether to allow searches without warrants, where it has forbidden the use of road blocks as a means of ordinary crime control, but noted that “the Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack or to catch a dangerous criminal who is likely to flee by way of a particular route.”²²

A cost-benefit analysis along these lines might suggest that the most invasive forms of mass dataveillance are unreasonable and ineffective when deployed for general law enforcement purposes rather than being targeted at terrorism. In evaluating the constitutionality of Canada’s proposal to create a database of the travel information of airline passengers that would be available to any state agency for any reason, Justice La Forest objected that “information about one’s movements and travel activities should not as a general rule be made available to the state without case,” and that when people are forced to reveal information about their movements, they reasonably expect the state not to “record, compile, or maintain this information for general law enforcement purposes.”²³ Evidence that general data searches of passenger information have not been proven to be effective in identifying terrorists would add weight to the analysis. But in order to perform a well-informed cost-benefit analysis of a particular security technology, the public, courts and other reviewing bodies would need access to empirical data about its effectiveness, as they currently have access to wiretap reports. In this sense, transparency, privacy, and security are mutually reinforcing.

A difficulty with the cost-benefit analysis suggested by Justices Harlan and La Forest is that it might recreate some of the circularity of the current judicial doctrines for regulating privacy, allowing privacy interests to recede as technology becomes more effective. For this reason, some European countries have given judges a more aggressive role in deciding on behalf of society how much privacy the government may reasonably invade. The German constitution, for example, establishes a principle of proportionality (*Verhältnismässigkeit*) which authorizes German judges to balance, in each case, a defendant's privacy interests against the strength of the suspicion and the seriousness of the offense. Invoking this doctrine, German courts have held that a greater intrusion will not be permitted when a less intrusive method would be sufficient.²⁴ The German federal constitutional court has invoked the proportionality principle to hold that taking spinal fluid from a suspect to decide whether or not he was insane was disproportionately invasive given the misdemeanor charge he faced.²⁵ Unlike American courts during the Clinton impeachment, a German court also refused to admit a private diary turned over to the police by the wife of a defendant's paramour in a case involving perjury. Although the diary might have been admitted if it contained evidence of felonies or international espionage, the court held, in this case the gravity of the invasion outweighed the low level nature of the suspected crime.²⁶

Even more ambitiously, Article 8 of the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, an international convention adopted in 1950, declares that "everyone has the right to respect for his private and family life, his home and his correspondence." It goes on to say that "there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic

society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.” Article 8 has been interpreted by the European Court of Human Rights to require national legislatures to adopt laws protecting data privacy; the European Court has also used it to require a kind of heightened judicial scrutiny for government actions that invade privacy, authorizing judges to strike down laws and technologies if there is an alternative that is more respectful of privacy and at least as effective in protecting security. The Court has held that the main object of Article 8 is to protect the individual against arbitrary actions by public authorities that are out of proportion to the threat at hand;²⁷ and using these abstract tests, it has held that monitoring and surveillance of people in public as well as private places may invade the sanctity of private life “once any systematic or permanent record comes into existence of such material from the public domain.”²⁸ Invoking the same principle, the Court has invalidated listening devices recording the voices of suspects in a police station and in their cells; and it has also ruled against the Romanian Intelligence service for releasing information about a citizen’s political activities that had been collected by the secret police. Because Romanian law provided no safeguards for gathering and archiving personal data about systems, the Court concluded that it conferred arbitrary discretion on public authorities.²⁹

It’s possible to imagine a similar kind of heightened judicial scrutiny for privacy in America, in which American judges could combine the judicial activism that enjoys bipartisan support in cases involving free speech with broad, European-style protections against privacy invasions that are disproportionate to the threats at hand. A judicial doctrine that strictly scrutinized all laws

and technologies infringing on privacy might adopt as its model the four part test proposed by George Radwanski, the privacy commissioner of Canada, to help courts and legislators evaluate the appropriateness of surveillance proposals. Any such law or technology, he argues, must be (1) demonstrably necessary to address a particular need or problem, (2) likely to be effective in addressing the problem, (3) proportional to the importance of the problem or the expected security benefit, and (4) there must be no less privacy-intrusive way of achieving the same result.³⁰ In Radwanski's view, the kind of mass dataveillance that is being considered in Canada and the U.S. can't be justified in light of these four principles because there is little evidence they are effective in predicting terrorist behavior or identifying known terrorists, because their costs to the privacy of innocent citizens far outweigh their security benefits, and because human intelligence would be more effective in keeping terrorists off airplanes. After concluding that a particular technology is unreasonable – that costs to privacy and equality outweigh the benefits to security – judges applying heightened scrutiny might give legislators and technologists a chance to redesign the technology in ways (like the Blob Machine or the Dutch PrivaCams) that strike a better balance. In evaluating invasive surveillance technologies such as wiretapping, courts have required that they be implemented in ways that minimize the detection of private activity unrelated to the objectives of the search. Using privacy enhancing technologies, it wouldn't be impossible to design data searches and video surveillance that minimized the recording and storage of personally identifiable information.

Although the judicial control model may make sense in other countries, I am not persuaded by it, and I don't believe that American judges will or should cast themselves in the role of saviors in

attempting to balance liberty and security. The history of American judicial activism in hotly contested areas where the country is divided and there are strong passions on both sides should be a cautionary tale. The abortion wars are only the most dramatic example of how judges who presume to enforce privacy rights with shadowy support in the text and history of the Constitution may provoke political backlashes that harm the cause of privacy more than they help it. Moreover, the victims of mass dataveillance are not vulnerable or unpopular minority groups, but all citizens whose personal data is unreasonably scanned and exposed to the state. For this reason, privacy advocates should be able to make their case in the political arena, and to the degree that the political branches are unresponsive, their indifference will reflect the zero-risk mentality of public opinion in general rather than prejudice or antipathy to particular groups. The excesses of the crowd are the Achilles' heel of democracy to which there is and should be no judicial remedy.

In my view, the most promising of the four models for balancing liberty and security is the last one, which I'll call the political oversight model. This model holds that Congress is better suited than the courts to strike a reasonable balance between liberty and security for many reasons. Judges tend to be reactive and slow moving, meaning that their decisions often lag behind technology, while Congress can pass laws proactively, as it did when it regulated e-mail privacy as early as 1986. Congress can legislate with flexibility and nuance, tailoring its regulations more closely to the particular challenges raised by particular technologies, while judges tend to prefer bright lines and abstract principles. As I argued in Chapter Four, the most important advances for privacy regulation since 9/11 have been congressional rather than judicial – from

the repudiation of the Total Information Awareness Program to the regulation of the Carnivore e-mail surveillance program to the sunset provisions for the most invasive provisions in the U.S.A. Patriot Act.

The great political challenge for the future is how Congress can be persuaded to create oversight mechanisms that balance liberty and security in a thoughtful way. One model, more in the European than the American tradition, is the office of the Privacy Commissioner of Canada, which has been a vigorous advocate for the enforcement of privacy laws. The office was created by the Canadian parliament in the 1980s to defend fair information practices; and the commissioner today has broad and independent powers to investigate privacy complaints, to conduct audits on state agencies, and to refer cases to court. After 9/11, George Radwanski, the current privacy commissioner, criticized the Canadian government's proposals for data surveillance on a broad scale. In particular, the government proposed to require commercial air carriers to provide passenger information to the Canadian intelligence service and the police, creating a database that could then be searched not only to find suspected terrorists but also to identify anybody wanted on any warrant for any offense punishable by five years or more in jail. Radwanski argued that the database might be justified if passenger information were used only to stop terrorist activity before it occurs. But the same intrusion was unacceptable, he insisted, when the information is used to search for ordinary criminals and to force all travelers to identify themselves to the police.³¹ Radwanski also criticized a related proposal – similar to the CAPPs profiling system being developed in the United States – that would give the Canadian Customs agency the authority to collect passenger information on every air traveler entering Canada. The

information would include the names, citizenship, and nationality of the travelers; their flights and destinations; their travel documents; and the form of payment. The Canadian intelligence agency has announced that it will retain the information in an extensive national database for six years, and that the database will be accessible to other government agencies not only for fighting terrorism but also for tracking pedophiles, money launderers, tax evaders, and perhaps even frequent travelers to Thailand.³² As in the U.S., the Canadian Customs agency plans to perform intelligence analysis on the passenger information to identify behavior patterns that might anticipate future threats, and also to use the database to solve crimes after they have occurred.

Radwanski said he was willing to accept the creation of a six year national security database if it were limited to preventing and investigating acts of terrorism, but he objected vigorously to the number of government agencies who have access to the information and the unlimited number of secondary uses to which the data can be put. He used all the persuasive powers of his office — including privately lobbying the customs agency, denouncing the profiling scheme in the media, and investigating a formal complaint that it violated Canada's privacy act. He also argued that it couldn't be justified in light of the four principles he had proposed for evaluating the reasonableness of security technologies – necessity, effectiveness, proportionality, and the absence of less intrusive alternatives. In his view, mass datavallance can't be justified in light of these four principles because there is little evidence it is effective in predicting terrorist behavior or identifying known terrorists, because its costs to the privacy of innocent citizens far outweigh its security benefits, and because human intelligence would be more effective in keeping terrorists off airplanes.

Given the relative success of the Canadian privacy commissioner in acting as a public advocate for privacy, a similar office might, in theory, help to balance liberty and security in the United States. Privacy advocates have long sought such an office, ever since the Senate recommended the creation of a federal privacy commission in 1974, but the proposal was tabled thanks to opposition by the Ford administration. “I do not favor the establishment of a separate Commission or broad bureaucracy empowered to define privacy in its own terms and to second guess citizens and agencies,” Ford declared.³³ As Ford’s statement suggests, Americans are more suspicious than Canadians of expert administrative bodies, which they perceive to be elitist and bureaucratic. Canada, by contrast, has been described as a “pleasantly authoritarian” culture, with far greater trust in government and willingness to defer to experts. Nevertheless, if Congress delegated the functions of a privacy agency to a special oversight committee, rather than a broad new bureaucracy, some of the libertarian concerns of those who are concerned about privacy but are suspicious of government might be mollified.

Conceptions of privacy, liberty, and equality vary dramatically among different Western democracies, and each country’s legislative response to the challenge of balancing liberty and security should reflect its unique political culture. A distinctively American response, therefore, might emphasize the importance of congressional resistance to the executive’s attempts to expand its own power. As Marc Rotenberg of the Electronic Privacy Information Center has argued, one way to understand the challenge of balancing liberty and security after 9/11 is the model of checks and balances in the U.S. Constitution. That means that if Congress grants the president new authority to engage in foreign intelligence surveillance, it should also create new

means of congressional oversight, or if the Department of Homeland Security proposes a trusted traveler program, it should be subject to open government standards.

Rather than creating a new federal agency, in the model of the Environmental Protection Agency or the Food and Drug Administration, Congress could authorize an existing congressional committee to review the effectiveness of new surveillance methods, balancing their costs to privacy against their benefits to security, and making recommendations about whether or not they are justified. The oversight committee could also collect data about the effectiveness of particular architectures of data mining and profiling, which it could compare with data about the effectiveness of the best available alternatives. Although Congress hasn't yet been moved to impose this kind of oversight, for the reasons I discussed in Chapter Four, there is a long tradition in America of legislative checks on new forms of surveillance, and over time, meaningful oversight is more likely to come from Congress than the courts.

The attempt by privacy groups to seek political accountability through transparency and coalition building strikes me as the most promising way of balancing liberty and security in the American political system. But the liberties threatened by dataveillance and other security technologies should not be defined exclusively in terms of privacy. In a comprehensive survey of federal laws protecting privacy, published in the 1990s, Priscilla Regan found that communications, information, and workplace privacy issues were on Congress's agenda for years, or even decades, before legislation finally emerged. "In these three cases, the initial policy issue was defined as one of 'privacy,'" she writes. "But in each case, protecting privacy involved

costs to fairly defined interests – government agencies, law enforcement and intelligence officials and employers. These interests were therefore concerned about redefining the issue from the idea of privacy to another idea, such as efficiency, crime control, or honesty and productivity in the workplace.”³⁴ Regan concludes that “privacy as an idea has not had a powerful influence on policy making,”³⁵ because its abstract and amorphous nature made it easy for more concrete interests to capture the attention of Congress: when presented with a choice between privacy in general and a more specific value, like crime control, Congress has tended to choose security.

Also, by framing the policy debates in terms of individual rights – in particular, the right of individuals to control information about themselves – policy advocates have invited a focus on cloying personal anecdotes of privacy victims who can make the case that their own privacy has been violated. Members of the public tend to perceive these stories as the missteps of a few unlucky bumblerers and aren’t convinced that they might suffer a similar fate. When individuals conclude that they themselves are not immediately at risk, they are perfectly happy to sacrifice privacy in the long term for an (illusory) promise of security in the short term.³⁶ Regan found that when the legislative debates were redefined as a battle that pitched security against more specific interests than privacy, Congress was willing to strike a reasonable balance. “In the case of information privacy, fair information principles replaced privacy in policy discourse; in communication privacy, industry competitiveness replaced privacy; and in psychological privacy, employment opportunities replaced privacy,”³⁷ Regan concluded. Once privacy advocates made alliances with other groups who could make the case for legislation in terms of

the public good, rather than individual rights, they were more successful. Thus, when it came to protecting e-mail privacy in 1986, industry groups were persuaded to rally around the bill after they came to believe that their own business interests were at stake.

If history is any guide, therefore, the most effective way of persuading Congress to strike a reasonable balance between liberty and security is not to focus exclusively on the ways that dataveillance threatens privacy. Instead, Congress might also be urged to focus on the threat to less amorphous and more empirically measurable values, such as equality. I've argued throughout this book that dataveillance threatens to make it harder for individuals to redefine themselves; it is a technology of classification and exclusion that attempts to put people in different boxes, predicting their behavior in the future based on their behavior in the past. In this sense, it changes not merely the way that citizens relate to one another as individuals but the way that the state relates to them as a group: instead of treating all citizens as presumptively equal, the government is now treating some as more trustworthy and valuable than others. After groups of individuals are routinely discriminated against at airports, in applying for jobs, or in trying to enter federal buildings, it's not hard to imagine that the resulting uproar (and lawsuits) could galvanize Congress into regulating technologies of dataveillance. But even before particular scandals emerge, the language of equality may have enough political resonance to form the basis of an effective and broad-based coalition for reform.

Political oversight seems more promising in America than judicial fiat; but in any democracy, the future of the balance between liberty and security will depend crucially on the attitudes of the

public itself. This has been a book about the vulnerabilities of the Naked Crowd, and although I've not been optimistic about the ability of the public to make calm judgments about liberty when it feels under siege, the picture is not entirely bleak. There are strong social pressures to embrace ineffective, feel-good technologies of security in the immediate wake of an attack; but the public is often able to reach a more considered judgment after the initial fears have faded, more information becomes available, and a sufficiently vocal minority begins to raise questions about the costs and benefit of the technology in question. Immediately after 9/11, more than 6 in 10 Americans agreed that the average person would have to give up civil liberties to fight terrorism. By June, 2002, however, the number had fallen to 46 percent.³⁸ Along the same lines, recall the shift in public opinion about national identification cards. A poll conducted the week after the 9/11 attack found that 70 percent of the respondents supported the idea of a national ID card that would have to be shown to officials on demand. Six months later, however, another poll found that only 26 percent of Americans backed the proposal, while 41 percent opposed it.³⁹ The shift reflected growing concern that government agencies would use the information for reasons that had nothing to do with terrorism; the public was also moved by the arguments of privacy advocates that the system would be ineffective in identifying determined terrorists, many of whom had obtained valid ID in the past. The shift in public attitudes toward ID cards is consistent with studies of group psychology which have found that people are less susceptible to group pressure when they have more information about a topic and are therefore more confident about their opinions. In the face of a unified majority, many individuals will take the group's view despite empirical evidence to the contrary. But when vocal minorities present a contrary view, people are more likely to act independently. And as the television pictures of burning

buildings faded from memory, so did the demand for unrealistic precautions. This is why it's important to be cautious about constructing, in the heat of passion, vast architectures of surveillance and identification that will linger long after fears have subsided and the immediate danger has passed.

If the public is to have a chance of resisting the temptations of crippling fear, it will have to be addressed in ways that promote trust rather than undermining it. Psychologists of fear have found that the most effective risk communication takes account of the limitations and peculiarities of the public mind. Imagine the dirty bomb scenario that I discussed in Chapter Two: how could the relatively low risks of contamination be conveyed to the public in a way that would avoid a mass panic? There is no point in presenting dry statistics about the relatively low risk of being contaminated by radiation for those not in the immediate area of contamination: studies of risk communication have found that telling people that the annual risk of living next to a nuclear power plant is equivalent to the risk of riding an extra three miles in a car fails to calm them down: because people have difficulty comparing unrelated risks, they tend to become confused and angry instead.⁴⁰ Merely being presented with evidence about the low risk of contamination may have the perverse effect of increasing public fears of being contaminated: when people are briefed about the low risks of radiation exposure from electric and magnetic fields, they tend to become more concerned rather than less, because they remember the scary pictures of radiation rather than the reassuring numbers that accompany them.⁴¹ More effective risk communication tends to compare different forms of radiation risk: When traces of radiation from Chernobyl reached the U.S., for example, the E.P.A. noted that exposures in the U.S. were

a tiny fraction of the exposure from chest X-rays; and this seemed to reassure U.S. citizens. By contrast similar comparisons in Europe failed to alleviate high public anxiety that had little relation to the actual threats, because the media and the public didn't trust the sources of information.⁴²

By all accounts, trust is the most important factor in avoiding mass panic: the public has to trust the credibility of official sources of information in order to believe them. People accept the risks of X-rays and prescription drugs because they trust the medical profession, but they are fearful of nuclear power because they don't trust the managers of nuclear power plants.⁴³ In order to inspire trust, government officials and media outlets have to convey the facts as accurately as they can, avoid spin, and candidly confess the limits of their knowledge rather than pretending to be more technically competent than they are. Israel has used this model since the 1960s: by and large, citizens trust that the government gives them truthful information, however bad the news is, within the limits of what is possible to convey without compromising the country's security. Unfortunately, in the United States, where citizens are instinctively distrustful of government, this kind of candor is hard to come by: at the height of the anthrax scare, the director of Homeland Security broke most of these rules of risk communication: speculating on the basis of incomplete knowledge, giving unhelpful risk comparisons to unrelated threats (being infected by anthrax was less than the risk of auto accidents, he said), and feigning a knowledge of the facts he didn't possess. At the same time, he failed to convey a crucial piece of information: many people didn't realize that they had to be exposed to anthrax in order to be at risk.⁴⁴

In the case of radiological danger, the possibilities of a public backlash against incompetent and dissembling officials are much greater. People have trouble understanding the risks of radiological weapons because of a basic confusion between radiation and radioactivity. A study of people's understanding of the risks of radon in their homes found that the E.P.A., to its credit, had tried to convey accurate information, but homeowners were confused because they thought, reasonably but incorrectly, that if their house had radon in it, it was permanently contaminated. To be disabused of this confusion, the E.P.A. would have had to explain that although a small amount of rapidly decaying radon can do damage, once the influx has been stopped, there is no danger. But because citizens are reluctant to absorb scientific information relating to technologies that it fears, this sort of message would likely be lost in the media din.

I've described a hypothetical set of events that would have to transpire in order to avoid fear and panic in the face of future terrorist attacks. But it's hard to be optimistic that all of these pieces of the puzzle will fall into place. "In a risk society there is a new moral climate of politics, one marked by a push-and-pull between accusations of scaremongering on the one hand and of cover-ups on the other," Anthony Giddens writes. "A good deal of political decision-making is now about managing risks – risks which do not originate in the political sphere, yet have to be politically managed. If anyone – government official, scientific expert or lay person – takes any given risk seriously, he or she must announce it. It must be widely publicized, because people must be persuaded that the risk is real – a fuss must be made about it. However if a fuss is indeed created and the risk turns out to be minimal, those involved will be accused of scare-mongering."⁴⁵ We saw this dynamic with the color coded terrorism alerts that the Department of

Homeland Security issued to calibrate the threats of violence on a daily basis. During the first two years after the 9/11 attack, none of the predicted threats materialized, but the political pressure to show that the government was serious about protecting the public from terrorism remained so great that the alerts continued. As amplified by the cable TV media, they created much more fear than they assuaged, and created a kind of public fatigue that made it less likely that the government and the television spokesmen would be trusted when a serious threat finally materialized.

There are many ways that trust is destroyed in a political culture that is skeptical of authority in all its forms. As Paul Slovic has discussed, the fact that individuals give more weight and attention to negative events means that the media will do so as well: scientific studies showing increased risk for death and disease get far more attention than studies with less gloomy conclusions.⁴⁶ Special interest groups have an incentive to use their own experts to sow mistrust among the public in order to influence policy debates. And a general mistrust of government, which can be healthy in checking executive excesses, means that experts of any stripe will be greeted with skepticism. At the end of his study of public opinion, Walter Lippmann called earnestly for the creation of an administrative cadre of experts who would sort through information about science and foreign affairs that was too complicated to be digested by an easily distracted public. Today, a similar proposal would be even less plausible than it was when Lippman wrote in the 1920s: no expert can command deference by virtue of his position; and even the experts, dependent on the public for status and recognition, have the same incentive to exaggerate risks and pander to public fears as the political branches. All this is to say that even if

the executive branch, the media, and the scientific community didn't have their own reasons to fan the public's fears rather than assuaging them, it's hardly clear that when trustworthy figures arise during times of crisis, the public will be inclined to trust them for long.

It should be obvious, by this point, that fear itself is indeed our most intractable enemy – as Roosevelt called it “nameless, unreasoning, unjustified terror which paralyzes needed efforts to convert retreat into advance.”⁴⁷ We are now experiencing the peculiar weaknesses of a society ruled by public opinion – the narcissistic individualism that is the enemy of individuality; the technological egalitarianism that is at odds with genuine equality; and the unrealistic zero risk mentality that selfishly demands complete insulation from remote dangers that are, by definition, impossible to eliminate. To overcome the weaknesses of the Naked Crowd, we will have to learn to live with our own anxieties and fears, rather than unrealistically demanding their eradication. And in this regard, our success in overcoming our fears may depend crucially on bold and farseeing political leadership, of the kind that Rudolph Guiliani, the former Mayor of New York City, offered in the wake of the 9/11 attacks. The greatest leaders of democracies in earlier wars did not pander to public fears; instead, they challenged citizens to transcend their self-involved anxieties and to embrace ideals of liberty larger than themselves. It is hard to imagine Franklin Roosevelt instituting a color-coded system of terrorist threat levels. The great war time leaders encouraged citizens to see themselves as part of a larger struggle, rather than encouraging them to focus obsessively on their own vulnerabilities. Without enlightened political leadership that has the courage to challenge the public's emotionalism, rather than encouraging it at every turn, democracies may not find the inner resources to stay calm in the face of an uncertain future.

A model for the kind of leadership we need might, perhaps, be found in Lincoln's address to the Young Men's Lyceum of Springfield, Illinois.⁴⁸ In the speech, delivered in 1838, Lincoln argued that the greatest danger facing America comes not from some "transatlantic military giant" such as European or Asian or African invaders. If the danger is to reach our shores, Lincoln argued, "it must spring up amongst us; it cannot come from abroad. If destruction be our lot we must ourselves be its author and finisher." The danger that Lincoln feared most was mob rule – "the increasing disregard for law which pervades the country — the growing disposition to substitute the wild and furious passions in lieu of the sober judgment of courts, and the worse than savage mobs for the executive ministers of justice." He noted the wave of mob violence that was sweeping the country from New England to Louisiana – the lynching of gamblers, the burning of African Americans, the shooting of newspaper editors, and the execution of suspected murders. In the midst of a nation seized by the "mobocratic spirit," Lincoln worried that a dictator may rise up among the people, resolved to destroy our constitutional liberties in order to satisfy his own ambition. To fortify against this danger, Lincoln urged his audience to be guided by reason – "cold, calculating, unimpassioned reason" – rather than the passion that "has helped us, but can do so no more." He concluded by challenging his audience to revere the laws and the Constitution in the face of its anxieties and fears. "Let every American, every lover of liberty, every well-wisher to his posterity swear by the blood of the Revolution never to violate in the least particular the laws of the country, and never to tolerate their violation by others." Instead of flattering the crowd, Lincoln challenged the members of his audience to transcend their baser impulses and embrace an ideal larger than themselves, the ideal of constitutional liberty itself.

The threats that menace us today are different, but the means of resisting them are similar, and must be found within our selves and in the best aspects of the American character. No Western democracy that has confronted terrorism during the last decades of the twentieth century was transformed beyond recognition by the experience; instead, each society became more like itself. Britain chose to wire itself with surveillance cameras and to embrace technologies of classification that took the place of a caste system that had begun to fray. Israel chose to become more fatalistic at the same time that it became more defiant. Germany chose to resurrect the use of informers but continued to place restrictions on the secret police. France relaxed its restrictions on state information gathering but maintained its restrictions on the press that prohibit the disclosure of embarrassing private information about political leaders and celebrities. And so forth. Nations do not re-invent themselves in times of stress; they reveal essential aspects of their character.

America, in this regard, faces a choice. We can choose, in the face of anxiety and fear, to express the weaknesses of the American self – the hyper-individualism that is the enemy of individuality and the crude egalitarianism that is the enemy of equality. We can demand unrealistic levels of personal insurance against remote risks and blame the national government when catastrophes nevertheless arise. Or we can make a different choice. Americans were not always afraid of risk and reluctant to take responsibility for their own fate. The pioneers who settled the open frontier embraced external threats as challenges to be overcome rather than risks to be litigated. Above all, they were pragmatists, and insisted on empirical evidence before choosing one technology of security or another. They did not embrace snake oil simply because it made them feel safe;

instead, they preferred to be safe.

These strengths of the American character – pragmatism, courage, individuality, and self-possession – can be tapped today as readily as our weakness. We have it within our power to overcome the paralyzing fears that threaten our liberties. The supreme question that faces us is whether we are ready and willing to save ourselves, rather than demanding salvation from judges or technologists or other illusory protectors. We can in short, strike a decent balance between freedom and security, as long as we are willing to find that balance in ourselves. Are we?

Acknowledgments

This book is an attempt to respond to a challenge posed by my friend and teacher Lawrence Lessig, whose influence and criticisms have been, as always, definitive. It's always a pleasure to work with Jonathan Karp of Random House, who once again provided invaluable support, candid advice, and constructive guidance from beginning to end. Tim Bartlett of Oxford University Press suggested that I write about liberty and security at a time when I thought I was writing about another topic; uncorked by this suggestion, the argument soon emerged. Chapters One and Three expand on essays that first appeared in the New York Times Magazine, and I'm indebted to Adam Moss, Gerry Marzorati, and Paul Tough, for ideal editorial experiences. At The New Republic, Martin Peretz, Peter Beinart and Leon Wieseltier have offered a vibrant home for more than a decade. I'm grateful to Dean Michael Young and my colleagues at the George Washington University Law School for providing the privacy and freedom that makes writing possible, as well as for criticisms of the manuscript that emerged at a faculty Works in Progress workshop. In 2002 and 2003, students in my privacy and security seminar contributed their suggestions and creative ideas. Neal Katyal, Cass Sunstein, Christine Rosen, Marc Rotenberg, Eugene Volokh, and Benjamin Wittes read the manuscript and generously improved the arguments, especially those with which they disagreed. Lydia Wills was a dedicated agent and Elise Schwartz, Ken Kilgour, and Murray Scheel were wonderful research assistants. I'm very grateful for their help.

Epilogue: An Escape from Fear

1. David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Reading: Perseus, 1998), p. 9.
2. *Ibid.*, p. 4.
3. *Ibid.*, p. 282.
4. *Ibid.*, p. 5.
5. Brandon C. Welsh and David P. Farrington, *Crime Prevention Effects of Closed Circuit Television: A Systematic Review*, Home Office Research Study 252, August, 2002, pp. 10-11, available at <<http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf>>.
6. Brin, *The Transparent Society*, pp. 334-35
7. *Lord Chesterfield's Letters* (Oxford: Oxford Univ. Press, 1998), p. 54.
8. Rogers Worthington, "A Family Tragedy or Terrorists' Scheme?" *The Chicago Tribune*, June 13, 1993, p. C21.
9. *United States v. Zein Hassan Isa*, 923 F.2d 1300, 1304 (1991).
10. *Id.* at 1305, *citing* *United States v. Hawamda*, No. 89-56-A, slip op. (E.D. Va., April 17, 1989); *see also* *United States v. Pelton*, 835 F.2d 1067, 1075-76 (4th Cir. 1987); *United States v. Cavanagh*, 807 F.2d 787, 790-91 (9th Cir. 1987); *United States v. Badia*, 827 F.2d 1458, 1464 (11th Cir. 1987); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984); *United States v. Belfield*, 692 F.2d 141, 147-49 (D.C. Cir. 1982).
11. *In Re: Sealed Case*, 310 F.3d 717, 724 (Foreign Int. 2002).

12. *Ibid.* at 736.

13. Craig M. Bradley, *The Exclusionary Rule in Germany*, 96 HARV. L. REV. 1032, 1054-55 (1983).

14. See *Perez v. Sharp*, 32 Cal. 2d 711 (1948) and *Loving v. Virginia*, 388 U.S. 1 (1967).

15. Herma Hill Kay, *From the Second Sex to the Joint Venture: An Overview of Women's Rights and Family Law in the United States During the Twentieth Century*, 88 CAL. L. REV. 2017, 2037 & n.117 (2000), citing Somini Sengupta, "Marry at Will," *The New York Times*, November 12, 2000, p. WR2.

16. See *Olmstead v. United States*, 277 U.S. 438 (1928) and *Katz v. United States*, 389 U.S. 347, 351 (1967).

17. *United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

18. *Ibid.* at 796-97.

19. Opinion by Justice Gérard V. La Forest on Video Surveillance, April 5, 2002, available at <http://www.privcom.gc.ca/media/nr-c/opinion_020410_e.asp>.

20. *Id.* See also Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974).

21. *United States v. White*, 401 U.S. at 786 (Harlan, J., dissenting.)

22. *City of Indianapolis v. Edmond*, 531 U.S. 32, 44 (2000).

23. Re: Opinion – CCRA Passenger Name Record, Opinion by retired Supreme Court Justice Hon. Gérard V. La Forest, November 19, 2002, available at <http://www.privcom.gc.ca/media/nr-c/opinion_021122_lf_e.asp>.

24. Craig M. Bradley, *The Exclusionary Rule in Germany*, 96 HARV. L. REV. at 1041.

25. *Ibid.*, n.43, citing *Judgment of June 10, 1963*, BVerfG, 16 BVerfG 194.

26. *Ibid.* at 1042-43, n.48 citing *The Diary Case*, Judgment of February 21, 1964, BGH, 19 BGHSt 325.

27. John Wadham, *Human Rights and Privacy – The Balance* (March 2000), reprinted in Daniel J. Solove and Marc Rotenberg, *Information Privacy Law* (New York: Aspen, 2003), p. 693.

28. P.G. & J.H. v. United Kingdom, E.C.H.R., 9/25/2001, reprinted in Solove and Rotenberg, *Information Privacy Law*, p. 698.

29. *Rotaru v. Romania*, E.C.H.R., 5/4/2000, reprinted in Solove and Rotenberg, *Information Privacy Law*, p. 706.

30. See, e.g., George Radwanski, Testimony regarding Bill C-36, the Anti-Terrorism Act, to the House of Commons Standing Committee on Justice and Human Rights (October 23, 2001), available at <http://www.privcom.gc.ca/speech/02_05_a_011024_e.asp>.

31. See Letter from George Radwanski to Minister Lawrence MacAulay, the Solicitor General (May 17, 2002), available at <www.privcom.gc.ca/media/an/ac_020517_e.asp>.

32. See Fact Sheet, Canada Customs and Revenue Agency, "Advance Passenger Information/Passenger Name Record (API/PNR)" (October, 2002), available at <www.ccradrc.gc.ca/newsroom/factsheets/2002/oct/api-e.html>.

33. Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill: Univ. of North Carolina Press, 1995), p. 80.

34. *Ibid.*, p. 175.

35. *Ibid.*, p. 177.

36. *Ibid.*, p. 178.

37. *Ibid.*

38. See Amitai Etzioni and Deidre Mead, The State of Society- A Rush to Pre-9/11, available at <http://www.gwu.edu/~ccps/The_State_of_Society.html>.

39. Julia Scheeres, "Support for ID Cards Waning," *Wired.com*, March 13, 2002, available at <<http://www.wired.com/news/print/0,1294,51000,00.html>>.

40. Paul Slovic, "Perception of Risk from Radiation," in Paul Slovic, *The Perception of Risk*, p. 271.

41. *Ibid.*, p. 268.

42. *Ibid.*, p. 272.

43. *Ibid.*, p. 269.

44. Baruch Fischhoff, "Assessing and Communicating the Risks of Terrorism," Remarks delivered at the 27th Annual AAAS Colloquium on Science and Technology Policy, April 11-12, 2002.

45. Anthony Giddens and Christopher Pierson, *Conversations with Anthony Giddens: Making Sense of Modernity* (Stanford: Stanford Univ. Press, 1998), p.212.

46. Paul Slovic, "Perceived Risk, Trust and Democracy" in Slovic, *The Perception of Risk*, pp. 324-25.

47. Franklin D. Roosevelt, First Inaugural Address, March 4, 1933, reprinted in *The Public Papers and Addresses of Franklin D. Roosevelt*, Samuel I. Rosenman, ed. (New York: Random

House, 1938), p. 11.

48. John G. Nicolay and John Hay, eds., *Complete Works of Abraham Lincoln* (New York: Lamb Publishing Company, 1904), vol. 1, pp. 35-50.