THE NAKED CROWD
RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE

BY JEFFREY ROSEN

For Christine

What marriage may be in the case of two persons of cultivated faculties, identical in opinions and purposes, between whom there exists that best kind of equality, similarity of powers and capacities with reciprocal superiority in them – so that each can enjoy the luxury of looking up to the other, and can have alternately the pleasure of leading and of being led in the path of development – I will not attempt to describe.

John Stuart Mill, *The Subjection of Women*

Contents

Prologue: The Naked Crowd

Chapter One: A Cautionary Tale

Chapter Two: The Psychology of Fear

Chapter Three: The Silver Bullet

Chapter Four: The Path of the Law

Chapter Five: Identity Crisis

Epilogue: An Escape from Fear

Acknowledgments

Prologue: The Naked Crowd

After the terrorist attacks of September 11, 2001, officials at the Orlando International Airport began testing a remarkable new security device. Let's call it the Naked Machine, for that's more or less what it is. A kind of electronic strip search, the Naked Machine uses microwaves and millimeter waves to bounce off the human body. In addition to exposing any guns or other weapons that are concealed by clothing, the Naked Machine also produces a three dimensional naked image of everyone it scrutinizes.[1] Unlike the crude metal detectors used at airports today, the Naked Machine can detect ceramic and plastic as well as metal, allowing airport monitors to distinguish between lethal explosives and harmless nail clippers. The technologists who invented the Naked Machine hope that it will be deployed in the future not only at airports but also in schools, at public monuments, in federal buildings, and in prisons. Before we enter any vulnerable public space, the Naked Machine could strip us bare and confirm that we have nothing to hide.

The Naked Machine is a technology that promises a high degree of security, but it demands a correspondingly high sacrifice of liberty and privacy, requiring all travelers to expose themselves nakedly, even though they raise no particular suspicions and pose no particular threats. Many people feel that this is a small

price to pay in an age of terror: what's a moment or two of embarrassment if terrorists are thwarted as a result? But the Naked Machine doesn't have to be designed in a way that protects security at the cost of invading privacy. With a simple programming shift, researchers at the Pacific Northwest National Laboratory in Washington State have built a prototype of a redesigned Naked Machine that extracts the images of concealed objects and projects them on to a sexless mannequin.[2] The lurking image of the naked body is then scrambled into an unrecognizable and nondescript blob. (For most of us, this is an act of mercy.) This redesigned version of the Naked Machine – let's call it the Blob Machine – guarantees exactly the same amount of security without invading liberty or privacy. Unlike the Naked Machine, the Blob Machine is a silver bullet technology that promises dramatic benefits without obvious costs; if it were deployed at airports, or perhaps even on subways and buses, the most scrupulous defenders of liberty and privacy could greet it with gratitude and relief.

For those who care about preserving both liberty and security, the choice between the Blob Machine and the Naked Machine might seem to be easy. But in presenting a hypothetical choice between the Naked Machine and the Blob Machine to groups of students and adults since 9/11, I've been struck by a surprising pattern: there are always some people who say they would prefer, at the airport, to go through the Naked Machine rather than the Blob Machine, even if the lines for each were equally long. When asked why, the people who choose the

Naked Machine over the Blob Machine give a range of responses. Some say they are already searched so thoroughly at airports that they have abandoned all hope of privacy and don't mind the additional intrusion of being seen naked. Others say they're not embarrassed to be naked in front of strangers, adding that those who have nothing to hide should have nothing to fear. (A few are unapologetic exhibitionists.) Still others are concerned that the Blob Machine would be less accurate in identifying weapons than the Naked Machine, and would prefer not to take chances. And in each group, there are some people who say they are so afraid of terrorism on airplanes that they would do anything possible to make themselves feel better, even if they understand, on some level, that their reaction is based on emotions rather than evidence. They describe a willingness to be electronically stripped by the Naked Machine as a ritualistic demonstration of their own purity and trustworthiness in much the same way that the religiously devout describe rituals of faith. They don't care, in other words, whether or not the Naked Machine makes them safer than the Blob Machine because they are more concerned about feeling safe than being safe.

In their willingness to choose a technology that threatens privacy without bringing more security, the people who prefer the Naked Machine to the Blob Machine are representative of an important strain in public opinion as a whole. It has become a cliche to say that everything changed after 9/11; but the cliche, on so many levels, is wrong. Before and after 9/11, when presented with images of

remote but terrifying events, groups of people tend to be moved by emotions rather than arguments, and this leads them to act in ways that sociologists and psychologists have associated with the behavior of crowds. The crowd tends to personalize risk and exaggerate the probability of its recurrence. It demands high levels of security while assigning less weight to more abstract values like liberty and privacy. Like the fearful people who prefer the Naked Machine, the public is sometimes more concerned about feeling safe than being safe. And it has little patience for evaluating the complicated choices that are necessary to ensure that laws and technologies are designed in ways that protect liberty and security at the same time.

This book began as an attempt to respond to a challenge posed by my friend Lawrence Lessig, who teaches at Stanford Law School and is the most creative and provocative philosopher of cyberspace. We were participating in a panel discussion about technologies of security, and I expressed skepticism about the proliferation of surveillance cameras in Britain, arguing that they posed grave threats to privacy even though the British government's own studies had found that they resulted in no measurable decrease in terrorism or crime.[3] Lessig politely but firmly called me a Luddite. These technologies will proliferate whether we like it or not, he said, and he encouraged me to think about ways of designing the technologies and constructing legal regulations in ways that might protect liberty and security at the same time. In the course of trying to answer Lessig's

challenge, I've become convinced that it is indeed possible, in theory, to design technologies and laws that protect both liberty and security. Unlike civil libertarians such as Alan Dershowitz[4] and Stephen Brill,[5] who, in the wake of 9/11, uncritically embraced technologies such as national ID cards without acknowledging the complicated range of choices they pose, I've been persuaded that there are well designed and badly designed architectures of identification, surveillance, and data mining, and the decision to accept or resist them should be guided by the details of the design and the values that constrain the designers.

As the response to the Naked Machine shows, however, it's also hard to be optimistic, in an anxious age, that Western democracies will, in fact, adopt these well designed laws and technologies, rather than settling for poorly designed alternatives. In the pages that follow, I will explore the reasons why the public may not demand laws and technologies that protect liberty and security, and why the legislatures may not require them, the courts may not refine them, and the technologists may not supply them on their own. I will examine the social as well as technological reasons why the risk-averse democracies of the West continue to demand ever increasing levels of surveillance and exposure in a search for an illusory and emotional feeling of security. The result is peculiar ordeal of living in the Naked Crowd, whose vulnerabilities and anxieties I will attempt to describe. In the Epilogue, I will try to imagine scenarios that might encourage the adoption of well designed laws and technologies, and to evaluate models that those laws

and technologies might follow. But my primary goal is to describe the challenge, rather than presuming to suggest that there are easy solutions: in societies ruled by public opinion, the excesses of public opinion can't be easily overcome.

In focusing on the emotionalism of some of the public responses to fears of terror, I don't mean in any way to deny or minimize the gravity of the new threats we face. At the beginning of the twenty-first century, the dangers of terrorists attacks on the Western democracies are clear, present, and deadly serious, and the need for effective responses to these dangers should be our highest priority of national security. My concern, however, is that the technologies and laws demanded by a fearful public often have no connection to the practical realities of the threats that we face. We run the risk, therefore, of constructing vast but ineffective architectures of surveillance and identification that threaten the liberty and privacy of innocent citizens without protecting us from terrorism. And although individuals should be free, in a pluralistic society, to trade liberty and privacy for higher levels of security, it's hard to defend government polices that require the surrender of liberty and privacy without bringing demonstrable security benefits. These feel-good laws and technologies may also distract the government from the focused intelligence gathering that has proven to be the most successful response to terrorism in the past.

This is a book about the anxieties of the Naked Crowd in an age of terror; and in

this sense, it is also a book about our anxieties about identity at the beginning of the twenty-first-century. Now that we can no longer rely on the traditional markers of identity – such as clothes or family or religion – to make judgments about whether or not strangers in the crowd pose risks to our security, fearful citizens are turning instead to technologies of identification and risk management. The interest after 9/11 in surveillance cameras, data profiling systems at airports, integrated databases of personal information, and biometric identification systems is a sign of our fears and confusion about whom to trust. But the question of whether trust is possible in a society of strangers is not unique to 9/11: it has been an enduring social challenge of the modern era. As traditional communities, social hierarchies, and natural systems of surveillance broke down in the twentieth century, the question of trust became especially acute.[6] Many of the surveillance technologies that arose in the private sector in the second half of the twentieth century were designed to verify personal identity and to distinguish between trustworthy and untrustworthy consumers. In short, the search for technologies that predict future behavior and put people in convenient categories predated our fears of terrorism; as we will see, many of the same risk profiling technologies that were used before 9/11 to classify and monitor customers on Amazon.com were deployed after 9/11 to classify and monitor potential terrorists.

The sociologist Anthony Giddens has described modernity as a "risk culture,"[7] in which individuals, no longer able to rely on traditional sources of identity such as

tradition and family and religion, must define themselves each day from an infinite variety of lifestyle choices. In an individualistic society, the effort to calculate risk becomes an obsessive preoccupation, not because individuals face more life-threatening dangers than in the past – in the age of antibiotics, we face fewer – but because the need to anticipate the future becomes especially pressing in a world where fewer aspects of our lives follow a predestined course. In an increasingly uncertain world, in which the status of individuals is constantly shifting, people find it increasingly difficult to live on what Giddens calls "automatic pilot."[8] Public discourse becomes addicted to predicting the future: as the proliferation of pundits, risk profilers, and futurologists suggest, people are desperate for guidance about how to plot their life choices from a bewildering variety of options. The constant calculation of future risks becomes a psychological crutch and a market imperative: witness the wave of books with "Future" in the title, from *Future Shock* to *The Future of Work* (or Freedom or Ideas, or what have you.) "A significant part of expert thinking and public discourse today is made up of *risk profiling* – analysis of what, in the current state of knowledge and in current conditions, is the distribution of risks in given milieu of action," Giddens writes. "Since what is 'current' in each of these respects is constantly subject to change, such profiles have to be chronically revised and updated."[9] In this sense, America's preoccupation with risk transcends the particular (and undeniably real) threats we now face. Previous ages have been menaced by catastrophes, plagues, and dangerous fanatics. Instead, our current

preoccupation with risks reflects the peculiar malleability of modern identity: an effort to anticipate risks is a self defense mechanism in a world where we are forced increasingly to make judgments about the trustworthiness of those we will never meet face to face.

In addition to embracing technologies of identification that purport to tell them whom to trust, citizens also face increasing pressure to expose personal information, in order to prove that they have nothing to hide. Crowds react to individuals in the same emotional terms that they react to remote threats; and as individuals on the Internet are increasingly exposed to vast audiences of strangers, many find it hard to resist the temptation voluntarily to strip themselves bare in the hope of attracting the attention and winning the trust of a virtual audience of strangers. Celebrities have long been familiar with the public pressure to reveal personal information: the illusion of familiarity that celebrity creates leads to growing demands that celebrities open up their personal lives, in order to sustain a sense of emotional connection with their unseen audience. In the age of the Internet, private citizens are experiencing similar pressure to expose themselves in the manner of celebrities. In the Naked Crowd, citizens who resist the overwhelming social pressure to reveal personal information to prove their trustworthiness are suspected of being potential terrorists, elitists, or worst of all, nobodies.

The sociologist Thomas Mathiesen has contrasted Michel Foucault's Panopticon – a surveillance house in which the few watched the many – with what he called the "Synopticon" created by modern television, in which the many watch the few.[10] But in the age of the Internet, we are experiencing something that might be called the "Omnipticon" in which the many are watching the many, even though no one knows precisely who is watching or being watched at any given time. The technology now exists to bring about the fulfillment of a particular kind of dystopia, where no aspects of life are immune from the relentless scrutiny of public opinion, and where the public's lack of tolerance for individuality and eccentricity results in a suffocating and pervasive social conformity. "At present individuals are lost in the crowd," John Stuart Mill wrote in the nineteenth century. "In politics it is almost a triviality to say that public opinion now rules the world." Mill was equally concerned that public opinion would infiltrate the "moral and social relations of private life," as "inhabitants of distant places," increasingly brought into "personal contact" by "improvements in the means of communication," would increasingly "read the same things, listen to the same things, see the same things, go to the same places, have their hopes and fears directed to the same objects, have the same rights and liberties, and the same means of asserting them."[11]

In the twenty-first century, changes in politics and technology have dramatically exacerbated the tyranny of public opinion. As traditional authorities continue to

decline, and public opinion becomes the only judgment that can command respect and deference, more and more aspects of our public and private lives become infiltrated by the logic of polls, evaluations, focus groups, and democratic accountability. Teachers are evaluated by their students and C.E.O.s by their employees. Buyers and sellers evaluate each other on eBay and Amazon, and the telephone company asks customers to assess and rank even the most mundane interactions with sales representatives as a reminder that every opinion matters and must be counted. As technologies make it possible for more and more aspects of our lives to be observed by strangers, it also ensures that more and more aspects of our lives will be evaluated by strangers. In the past, it was only unusually interesting people – celebrities, crime victims, or politicians – who had to worry about the face they presented to large and unseen audiences. But in the age of the Omnipticon, no individual is immune from the pitiless and unblinking gaze of the crowd, and all of us are susceptible to its fickle emotions – including anxiety, jealousy, and fear.

The excesses of the Naked Crowd were brought into sharp relief by the terrorist attacks of 9/11; but they are hardly a new phenomenon. In *The Crowd*, a classic nineteenth century study of the popular mind, Gustave Le Bon argued that impulsiveness, irritability, and absence of critical spirit are "the special characteristic of crowds."[12] As a result, he concluded, the sentiments of crowds tend to be simplistic, exaggerated, and overconfident. Crowds are moved by

images rather than arguments, he wrote, and the images most likely to impress a crowd are the most dramatic and therefore the least typical – great crimes, for example, or great miracles or disasters. But because crowds are incapable of reasoning, they have trouble distinguishing improbable events, which tend to be the most memorable, from mundane events, which are more likely to repeat themselves. "A hundred petty crimes or petty accidents will not strike the imagination of crowds in the least, whereas a single great crime or a single great accident will profoundly impress them, even though the results be infinitely less disastrous than those of the hundred small accidents put together," Le Bon observed.[13] For example, a flu epidemic which killed 5,000 people in Paris made little impression on the popular imagination, because it was reported only in dry statistics that emerged week by week in the newspapers, while a visually memorable accident, such as the fall of the Eiffel Tower, would have made an immense impression, even if it had killed fewer people. For all these reasons, Le Bon concluded, individuals act and feel very differently in crowds than when they are isolated from each other, and are especially susceptible to irrational and contagious epidemics of fear.

Le Bon, it must be said, was a sexist and racist (and not only by our own more exacting standards); and his politically incorrect generalizations have not always withstood the test of time. "Crowds are everywhere distinguished by feminine characteristics, but Latin crowds are the most feminine of all,"[14] he wrote.

Nevertheless, his insights about the tendency of crowds to be moved by images and emotions rather than arguments and analysis were confirmed during the twentieth century by more empirical behavioral economists and social psychologists, who resist calling the public irrational, but emphasize its "quasi-rationality"[15] or "bounded rationality"[16] in evaluating remote but frightening risks. These scholars have found that people are vulnerable to systematic errors and biases in judgment; as a result, they have difficulty appraising the probability of especially frightening threats because of their tendency to make judgments about risk based on emotional intuitions about whether something is good or bad, rather than a dispassionate calculation of costs and benefits. Groups of people also tend to fixate on the hazards that catch their attention, which means those that are easiest to imagine and recall. A single memorable image – of the World Trade Center collapsing, for example – will crowd out less visually dramatic risks in the public mind, and will lead people wrongly to imagine that they are more likely to be victims of terrorism than mundane risks, like heart disease. Although mental shortcuts can work relatively well in some circumstances[17], they can also create anxiety and panic that is disproportionate to the threat at hand.

Because people fear risks that produce memorable images above all, the psychology of fear is driven inextricably by images of terror transmitted by the media. In this sense, the growth of the Internet and 24/7 cable TV stations have exacerbated the biases and errors of judgment to which the public is vulnerable.

After World War I, in his classic study of Public Opinion, Walter Lippmann pointed to the growth of motion pictures and newspapers, which created an increasing gap between the simplistic images in people's heads and the complicated reality of the remote threats that confronted American democracy. "The only feeling that anyone can have about an event he does not experience is the feeling aroused by his mental image of that event,"[18] Lippmann recognized, and as Americans increasingly faced threats far removed from their personal experience, the images that engaged them were likely to come from movies, radio, and newspapers. This created a new problem for democracy – "the problem which arises because the pictures inside people's heads do not automatically correspond with the world outside."[19]

In absorbing images from movies and newspapers, Lippmann worried, people were too impatient to make reliable judgments about complicated threats involving war and foreign affairs. "The truth about distant or complex matters is not self-evident, and the machinery for assembling information is technical and expensive," he wrote.[20] Besides, citizens in a modern democracy are not very good at absorbing complicated information from the media: because of our short attention spans, we tend to simplify and generalize, reducing unfamiliar people and events to crude and easily intelligible stereotypes. Instead of imaginatively projecting ourselves into events that are remote from our daily experience, we selfishly try to relate these events to our own parochial concerns. "In almost every

story that catches our attention we become a character and act out the role with pantomime of our own," Lippmann wrote. Instead of taking our "personal problems as partial samples of the greater environment," we instead reconfigure "stories of the greater environment as a mimic enlargement of [our] private life."[21] As a result, "self-centered" public opinion is likely to exaggerate the individual risk posed by remote events and to undervalue common interests such as liberty or privacy.

Since Lippmann wrote, the gap between the "pictures in our heads" and the reality of the threats that menace us has expanded dramatically because of the exponential growth of new media. In *The Image*, written at the beginning of the 1960s, Daniel Boorstin explored the way the "Graphic Revolution"[22] – by which he meant the explosion of television as well as movies, newspapers, and magazines – had transformed the way Americans related to political leaders and to public affairs in general. The need to fill empty space on television and in magazines brought with it irresistible demands for the manufacturing of "pseudo-events" – that is, events created for the sole purpose of producing memorable images that could then be reported and consumed. Pseudo-events were distinctive, vivid, and easier to grasp than reality itself: whether they were believable and memorable was more important than whether they were true.

In the 1990s, the rise of the Internet and 24/7 cable news stations expanded the

amount of empty air time and dramatically exacerbated the demand for pseudo-events that would catch the public's attention in an increasingly fractured and competitive market place. Stations like Fox News and CNN converted themselves into twenty-four hour purveyors of alarm, with shrieking banners running like stock tickers along the bottom of the screen, exaggerating the latest threat in the most lurid terms. ("Chilling chatter" read the banners on the first anniversary of 9/11, as the government reported intercepted messages from terrorists purportedly planning a new attack abroad.) These stations had a commercial incentive to exaggerate the risks posed by low probability, randomly distributed threats, in order to convey the impression that everyone was at risk and therefore catch the attention of an easily distracted audience. But there are tangible effects to this brazen fear mongering: when the Office of Homeland Security put the nation on a Code Orange alert for an imminent terrorist attack, there was a run at malls across America on duct tape and plastic sheeting, as people rushed to insulate their houses against a hypothetical chemical attack that never materialized.

The vicious cycle at this point should be clear. The public fixates on low probability but highly terrifying risks because of dramatic images it absorbs from television and the Internet, which in turn have an incentive further to exaggerate the horror of the same remote risks in the hope of sustaining the attention of the public. This cycle fuels a demand for draconian and symbolic but often poorly designed laws and technologies of surveillance and exposure to eliminate the

risks that are, by their nature, difficult to reduce. The demand for these ineffective and invasive laws and technologies is made even worse by the fact that the public tends to conceive of risks as an all or nothing affair: they mistakenly believe that a hazard is either dangerous or safe without recognizing the possibility of a middle ground. Many people embrace what W. Kip Viscusi of Harvard Law School has called a "zero risk" mentality, naively believing that it is possible to eliminate risks that can never be entirely eliminated.[23] This only increases the demand for showy safety rituals that are designed more to commemorate the last dramatic threat than to anticipate the next one.

It's possible, as the Blob Machine shows, to design laws and technologies that protect liberty and security, striking a more effective balance between exposure and concealment. But it's also hard to be optimistic that these laws and technologies will actually be adopted. The choices among them are complicated and the crowd's attention span is short. Moreover, there is no obvious political constituency for a reasonable balance between liberty and security. Our civic debate is polarized between technopositivists who greet every proposed expansion in surveillance power with uncritical enthusiasm, and Luddites, who are fighting a doomed battle to resist technologies that will proliferate whether we like them or not. And rather than trying to ensure that these laws and technologies are designed well rather than poorly, even the self-styled pragmatists in the debate allow their judgment to be distorted by hyperbole and fear. "It stands to reason

that our civil liberties will be curtailed" after September 11, wrote Judge Richard Posner soon after the attacks. "They should be curtailed, to the extent that the benefits in greater security outweigh the costs in reduced liberty. All that can reasonably be asked of the responsible legislative and judicial officials is that they weigh the costs as carefully as the benefits."[24] But this careful weighing of costs and benefits is precisely what legislators and judges have proved, in times of crisis, to be incapable of sustaining.

Why should we care about the emotionalism of the Naked Crowd? If citizens want to strip themselves naked at the airport because the ritual makes them feel better without making them safer than a less intrusive alternative, why should any one else object? Of course, individual citizens should be free to surrender their own privacy in exchange for a feeling of security, as long as their choices are not imposed on anyone else. But when the government adopts vast technologies of surveillance and classification, Western democracies may be slowly transformed in ways that we are only beginning to understand. It may be worth imagining some of the social and individual costs of badly designed technologies and laws, in order to frame the debate about how to design them better.

As the government collects and stores more and more personal information about citizens in what Daniel Solove has called "digital dossiers,"[25] there is, first of all, the danger of the Googelization of identity – a phenomenon that could allow

government agents to single out any individual from the crowd and reconstruct his or her movements, purchases, reading habits, and even private conversations for any period of time. Google, of course, is the Internet search engine that allows any citizen to punch in the name of any other citizen and instantly retrieve information about him or her that has appeared in cyberspace. It is one of the many technologies of identification that help us to acquire information about strangers and new acquaintances in deciding whom to trust, a substitute for more traditional ways of assessing someone's reputation, such as gossip or face to face judgments about character. Because Google retrieves isolated bits of personal information, a Google search inevitably runs the risk of confusing information for knowledge and judging us out of context.

After being set up on a blind date, for example, a friend of mine ran a Google search and discovered that her prospective partner had been described in an article for an online magazine as one of the 10 worst dates of all time; the article included intimate details about his sexual equipment and performance that she was unable to banish from her mind during their first -- and only -- dinner. These are the sort of details, of course, that friends often exchange in informal gossip networks. The difference now is that the most intimate personal information is often recorded indelibly and can be retrieved with chilling efficiency by strangers around the globe.

As the government begins to use Google-like technologies of data mining and data profiling to judge people out of context, the consequences can be far more severe than embarrassment. Roger Clarke has used the term “Dataveillance” to refer to the "systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons."[26] Clarke distinguishes between “personal dataveillance” of previously identified individuals and the “mass dataveillance” of groups of people. Personal dataveillance tends to be used for investigation and mass dataveillance for risk prediction; and both technologies present distinct costs and benefits. Personal dataveillance – designed to collect information about individuals who have been identified in advance as suspicious – can be usefully deployed to catch the most serious criminals or to prevent the most serious crimes. In the fall of 2002, for example, the suburbs of Washington, D.C. were terrorized by a sniper who killed several people before being caught by the police. Although the risk of being killed by the sniper was far lower than the risk of being killed in a car accident, the crime was so visible, and the TV images it produced were so dramatic, that hundreds of otherwise rational citizens could be seen sprinting hysterically from their cars to the mall in a zig zag pattern, to avoid what they imagined were the sniper’s cross hairs. The sniper turned out to be an unemployed man who was traveling with a teenage Jamaican accomplice, and he was caught, in the end, because he boasted to a priest about having committed a murder in Alabama. Based on this human tip, the police were able to engage in a form of personal

dataveillance, connecting a fingerprint found at the Alabama crime scene with one stored in an immigration and naturalization service database. They were then able to identify the sniper's accomplice and to track down his license plate number. This combination of old fashioned police work and cross-referencing of criminal databases made fools of the criminal profilers and "forensic psychologists"[27] who filled weeks of air time predicting that the sniper was an angry white man in his thirties who drove a white van. But the sharing of information about serious crimes among several government agencies was a defensible use of database technology: it allowed the identification of a serious criminal with no tangible threat to the privacy of innocent citizens.

When applied by the state on a broad scale, however, personal dataveillance can run the risk of judging people out of context, leading to arrests based on mistaken identity. For example, an F.B.I.. watch list widely circulated to private employers was riddled with inaccuracies, misspellings, and people who had been wrongly identified as terrorists. Many of these innocent victims were repeatedly stopped at the airport, and found it very difficult to clear their names once they had been tagged as suspicious in computer databases.[28] Other troubling cases in America after 9/11 involved immigrants who were arrested and detained for months based on snippets of circumstantial evidence suggesting that they fit a terrorist profile but later turned out not to be terrorists. A man named Hady Hassan Omar was arrested on September 12 and detained for 73 days after he bought a one-way

airline ticket on the same Kinko's computer used by one of the 9/11 hijackers. An Egyptian named Osama Elfar was locked up for more than two months because he had attended a Florida flight school and worked as a mechanic for an airline in St. Louis. A gas station attendant from Pakistan was denied bail in Miami after being arrested because he stood in line to renew a driver's license a few minutes ahead of Mohammad Atta. An Egyptian student named Abdallah Higazy, who had been staying in a hotel near the World Trade Center on 9/11, was put in solitary confinement after F.B.I. agents accused him of using a ground-to-air radio to transmit information to the terrorists. Only after another guest showed up to claim the radio were the charges dropped. Although these immigrants eventually had a chance to prove they weren't terrorists, many were later deported for having committed low level crimes that had nothing to do with terrorism. Of the 130 Pakistani seized after 9/11, 110 were convicted of immigration violations, and 22 were convicted of robbery, credit card fraud, or drug possession. None was linked to the 9/11 attacks. This pattern of misidentifying people as serious criminals and then punishing them for low level offenses is typical of personal dataveillance, which gives the state tremendous discretion to single individuals out of the crowd and then to punish them for trivial crimes that are far easier to detect.

By contrast, mass dataveillance – which involves scanning the personal data of millions of citizens who have not been identified as suspicious in the hope of

preventing terrorism before it occurs – poses very different dangers. These dangers are by no means new: in some ways, mass dataveillance looks very much like the general warrants that the framers of the Fourth Amendment to the Constitution were determined to prohibit. General warrants allowed the agents of King George III to break into any citizen's home and riffle through his private papers in a fishing expedition for evidence of disloyalty to the crown. In the course of fishing for unspecified evidence of guilt, these general searches ran the risk of exposing a great deal of innocent but embarrassing private information – from personal diaries to private letters – to public view. Because the invasiveness of the search was so vastly out of proportion to the unspecified crimes that it might detect, the Framers of the Fourth Amendment to the Constitution forbade general warrants, and insisted that magistrates couldn't issue warrants without probable cause to suspect wrongdoing, and without "particularly describing the place to be searched, and the persons or things to be seized."

Mass dataveillance, like general warrants, allows the government to scan a great deal of innocent information in the course of fishing for signs of guilt. And in the process, it threatens both privacy and equality, and diverts government resources away from more effective responses to terrorism. First consider privacy. One reason that the Framers of the Fourth Amendment feared general warrants was the risk of blackmail and politically motivated retaliations against opponents of the government. Although this sort of abuse of power is thankfully harder to conceal

in a more transparent age, it was only a generation ago that President Richard Nixon engaged in similar abuses, monitoring the private activities of anti-war protesters and vindictively prosecuting them for low-level tax offenses. In an age when the personal data of far greater numbers of citizens are analyzed by the government in personally identifiable ways, it's not wrong to fear versions of the Nixon effect on a broader scale. Moreover, the very existence of personally identifiable dossiers would be a temptation to those who wished us ill in the private sphere: as those who have endured messy divorces can attest, vindictive spouses are all too happy to fish for embarrassing personal information and to expose it to the world.

If technology and law are allowed to erode the old barriers that prevented government from searching citizens at random and prosecuting them for the most minor infractions of the law, many more citizens will experience the sense of indignation at living in a zero tolerance society – an experience that, before 9/11, was limited largely to citizens in minority communities. A zero tolerance society should be distinguished from one that uses the prosecution of low level crimes to prevent more serious crimes. In 1982, James Q. Wilson and George Kelling published a celebrated article called "Broken Windows" in *The Atlantic Monthly*, which argued that policing lower-level public disorder – loitering, drug use, gang activity, and public drinking – best diminished the fear and social disorder that allowed more serious crime to flourish. But broken- windows policing was not

based on the principle of "zero tolerance," which advocates mass arrests for low level crimes on the theory that some turnstile jumpers may turn out to be wanted for more serious crimes. The broken-windows approach instead urged cities to use quality-of-life offenses to increase police discretion, not to eliminate it. By allowing police to choose among a wide variety of legal and nonlegal sanctions for public disorders – from informal warnings to formal citations – the broken-windows policy viewed arrest as a last resort. By contrast, when the broken-windows approach morphed into zero tolerance policing, the minority community in New York began rioting in the streets because people began to feel like they were living in a police state. It was the zero tolerance approach that led to undercover operations like Operation Condor, during which officers shot Patrick Dorismond in the course of approaching him to buy marijuana that he turned out not to possess. Under Operation Condor, narcotics officers volunteered to work overtime to arrest people for minor crimes, such as smoking marijuana and trespassing. Operation Condor drove low level drug-trafficking indoors, but it had little impact on the homicide rate, which actually increased, or on the rate of narcotic-felony arrests, which decreased by nine percent. In other words, the zero-tolerance thesis – that turnstile jumpers often turn out, under investigation, to be carrying illegal guns – proves, after a certain point, to be wrong: many pot smokers are guilty of nothing more than smoking pot. The experience of being accountable to the police for offenses so trivial that no one expects to be prosecuted for them made minority citizens take to the streets in protest. And in a

zero tolerance society in which all of our personal data were transparent to the government, it's not hard to imagine broader groups of citizens being moved to similar protests against what they perceived to be the inordinate power of a police state.

Because they are searching for needles in haystacks, the new technologies of mass dataveillance also run the risk of generating a very high number of "false positives" – alerts in which innocent citizens are misidentified as potential terrorists. (For a statistical illustration of why data mining systems are not very good at picking very few individuals out of very large crowds, please see Chapter Three.) Anyone who has been taken aside repeatedly for special searches on a particular airline will recognize the feeling of indignity and helplessness that results from being flagged as a threat in a computer database without knowing why or even having the power to confirm or deny that a blacklist actually exists. The chief architect at Microsoft described these feelings after being wrongly flagged for an airport search by the Computer Assisted Profiling System because he had trained for a pilot's license and bought a one way ticket: "I suddenly felt as if in the grip of a giant vise, a terrible feeling I had last experienced as a teenager before fleeing Communist Hungary .... My friends may suspect I am suffering from some Hungarian Refugee Syndrome, which makes me overly sensitive to perfectly reasonable intrusions by the state. I try to explain: The communism I had fled was hardly traumatic or violent. One aspect of the horrible vise was the

constant minor humiliations I had to suffer, such as interaction with the block warden, the party overlord of a block of houses, who had to give his assent to all matters tiny or grand, including travel. On this Friday in the United States, I was being singled out for an unusual and humiliating search .... So I did what I had done 30 years ago: I chose to be humiliated just so I could reach my goal."[29] Of course, the indignity that the Microsoft architect suffered in communist Hungary is very different than the indignity that he suffered in the United States; but the sense of being wrongly identified on the basis of secret information that the government refuses to disclose is one that could well infuriate Americans if this kind of profiling becomes widespread.

Mass dataveillance threatens more than embarrassment and invasions of privacy: it also threatens values of equality in ways that could transform the relationship between citizens and their government. Risk profiles ensure that different groups of individuals are treated differently in the future based on their behavior in the past. As the temptation to use profiling technology expands, it is not hard to imagine a society in which citizens, in all of their interactions with the government, are treated differently based on the level of trustworthiness they have been assigned by a computer search. In this sense, risk profiles are technologies of classification and exclusion, limiting people's opportunities and stifling their power to define themselves. "[R]educing the issue to one of 'privacy' simply deflects attention from .... a social situation in which electronic languages are

permitted to define us and channel our social participation," David Lyon has written. "[T]he language of surveillance all too often classifies, divides, and excludes."[30]

Classification and exclusion are already common in the consumer sphere, in which technologies of customer relations management are designed to put customers in separate categories based on their perceived value to the company. When the same technologies are applied in the civic sphere, however, they result in different citizens being put in different risk categories based on the threat they are perceived to pose to the state. In this sense, risk profiles extend harms similar to those imposed by racial profiling across society as a whole, creating electronic layers of second class citizenship that determine who is singled out for special suspicion by state officials. They represent what Lyons calls a technology of "social sorting" and "digital discrimination."[31] Individuals who are classified as especially high risk are likely to experience a sense of helplessness at their inability to confront the unknown accusations that dog them and a constant sense of having to prove their innocence in the face of a presumption of guilt.

There is a final danger of poorly designed technologies that make us feel safer without actually increasing our security: they may divert the government's resources and distract its attention from developing more effective responses to terrorism – responses that might actually save lives rather than temporarily easing

anxieties. In airports, for example, human intelligence has proved far more effective than machines. El Al, the national airline of Israel, is famous for the zeal of its human security guards, who ask passengers where they are going, where they have come from, why they want to visit Israel, and who they plan to see. The guards are trained to look for changes in facial expression or body language that might indicate nervousness, and are subject to elaborate simulation exercises that test their ability to pick suspicious travelers out of the crowd. Unlike the American Computer Assisted Passenger Screening System, or CAAPS, a data mining program that tries to predict who will be a terrorist, El Al only tries to determine whether a particular passenger poses a serious risk after he has been questioned by a human security guard who has been trained in psychological analysis.[32] Relying on the kind of visual profiles that Americans reject as a violation of equality, El Al screeners tend to single out Arabic-looking men, women traveling alone, and "shabbily dressed" people.[33] This crude visual profiling proved effective in 1986, when El Al officials prevented the bombing of a flight from London to Tel Aviv by focusing on a pregnant, Irish woman who was traveling alone. Faced with additional questions, the women admitted she was engaged to a Palestinian man, the father of her unborn child, who had packed a box of presents for her to carry to his family in the West Bank; on inspection, the bag turned out to contain explosives.[34] El Al has been similarly effective in using behavioral profiling, focusing on passengers who seem unusually nervous or anxious. In a more recent case, El Al screeners apprehended a German criminal

whose ticket had been purchased by a Palestinian terrorist group which paid him $5,000 to carry what he thought were drugs. When the German couldn't explain why he was taking the trip or who had bought his ticket, security officers opened his bags and found hidden explosives.[35] After being trained in techniques of psychological profiling, El Al screeners must pass at least 150 security checks a year, including efforts by members of the Mossad, Israel's C.I..A., to test their human intelligence abilities by imitating passengers who offer incongruous stories. Instead of relying on computer algorithms, the Israelis recognize that there is no substitute for face-to-face human discretion.

If properly designed to guarantee liberty and privacy as well as security, there is no reason that these technologies of identification couldn't play a useful (if limited) role in identifying potential terrorists, working in conjunction with the human intelligence that has proved to be the most effective way of catching and deterring serious criminals. But as the example of the Blob Machine shows, there is no reason to expect that technologies of identification will be designed in ways that target the guilty while sparing the innocent. There is a grave danger, in other words, that our emotional response to the new fears that menace us will lead us to adopt ineffective and unnecessarily invasive architectures of identification and risk profiling that could linger long after the fears that inspired them have passed.

In the pages that follow, I will argue that there is no need for this grim state of

affairs to come to pass. It is possible to resist the excesses of the Naked Crowd; possible, that is, to design laws and technologies that protect liberty and security at the same time. But the challenge ahead will not be easy. Chapter One, A Cautionary Tale, takes us to Britain for a vision of a society in which the crowd's emotional demands for security are more or less unchecked by legal or constitutional restraints. In the face of widespread fears of terrorism, Britain wired itself up with thousands of surveillance cameras – a technology that (unlike the Blob Machine) threatens privacy and equality without empirically measurable benefits for security. Chapter Two, the Psychology of Fear, explores the reasons why the crowd, left to its own devices, reacts to threats emotionally rather than analytically, and is more concerned about feeling safe than being safe. As a result of these biases of public opinion, we are vulnerable to being terrorized by dramatic but low probability events – acts of terror that inspire fear vastly disproportionate to the immediate human carnage left in their wake. Chapter Three, The Silver Bullet, describes the search in Silicon Valley and Washington for security technologies that will protect individuals without requiring government officials to make discretionary human judgments about who is trustworthy and who is not. But although it is possible to design these technologies in ways that protect liberty as well as security, the technologists are more likely to choose designs that dramatically favor security over liberty: they are creatures of the market, and the market craves efficiency above all. Chapter Four, The Path of the Law, argues that Congress is more likely than the courts to

resist the public's demand for a zero risk society. Legislators have proved to be more willing than judges to resist the most sweeping claims of executive authority, although little more willing to demand that the most invasive searches and seizures are reserved for the most serious crimes. Chapter Five, Identity Crisis, suggests that the crowd's unrealistic demand for a zero risk society is related to our anxieties about identity. Because we can no longer rely on traditional markers of status to decide whom to trust, the crowd demands that individuals in the crowd prove their trustworthiness by exposing as much personal information as possible; individuals in an exhibitionistic and narcissistic age are happy to oblige in an effort to establish an emotional connection with the crowd. In the Epilogue, An Escape From Fear, I will explore ways that legislators, the courts, and the public itself might respond to our modern anxieties in constructive ways that protect freedom, privacy, and security. In my view, political rather than judicial checks and balances provide the most promising avenues for regulation. But the Naked Crowd wants what it wants; and tends to get what it demands; so it would be foolish to underestimate the challenges ahead.

At least the path we need to resist is clear. For a cautionary tale, please follow me to England.

Prologue: The Naked Crowd

1. Kevin Maney, "The Naked Truth About a Possible Airport Screening Device," *USA Today*, August 7, 2002, p. 3B.

2. Mick Hamer, "All-Seeing Scan Spares Your Blushes," *New Scientist*, August 17, 2002, p. 10.

3.Brandon C. Welsh and David P. Farrington, *Crime Prevention Effects of Closed Circuit Television: A Systematic Review*, Home Office Research Study 252, August, 2002, p. 44, available at <http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf>.

4.Alan M. Dershowitz, "Why Fear National ID Cards?" *The New York Times*, October 13, 2001, p. A23.

5.Steven Brill, *After: How America Confronted the September 12 Era* (New York: Simon & Schuster, 2003), pp. 614-15.

6.Steven L. Nock, *The Costs of Privacy: Surveillance and Reputation in America* (New York: Aldine de Gruyter, 1993).

7.Anthony Giddens, *Self and Society in the Late Modern Age* (Stanford: Stanford Univ. Press, 1991), p. 3.

8.Ibid., p. 126.

9.Ibid., p. 119.

10.Thomas Mathiesen, "The Viewer Society: Michel Foucault's 'Panopticon' Revisited," THEORETICAL CRIMINOLOGY 1(2) 215, 221 (1997).

11.John Stuart Mill, "On Liberty," in *On Liberty and Other Essays* (New York: Oxford Univ. Press, 1998), pp. 73, 81.

12.Gustave Le Bon, *The Crowd: A Study of the Popular Mind* (New York: Ballantine Books, 1969), p. 31.

13.Ibid., p. 62.

14.Ibid., p. 34.

15.*See* Richard H. Thaler, *Quasi Rational Economics* (New York: Russel Sage, 1993).

16.*See* Herbert A. Simon, "Theories of Bounded Rationality*,"* in *Decision and Organization: A Volume in Honor of Jacob Marschak*, B. McGuire & Roy Radner eds. (Amsterdam, North-Holland Pub. Co., 1972.).

17.*See, e.g.*, Gerd Gigerenzer and Peter M. Todd, "Fast and Frugal Heuristics: The Adaptive Toolbox," in *Simple Heuristics That Make Us Smart*, Gerd Gigerenzer et al., eds. (New York: Oxford Univ. Press, 1999).

18.Walter Lippmann, *Public Opinion* (New York: The Free Press, 1965), p. 9.

19.Ibid., p. 19.

20.Ibid., p. 202.

21.Ibid., pp. 110-11.

22. Daniel J. Boorstin, *The Image: A Guide to Pseudo-Events in America* (New York: Atheneum, 1987), p. 57.

23.Cass R. Sunstein, *The Laws of Fear: The Perception of Risk*, 115 HARV. L. REV. 1119, 1128-29 (2002).

24.Richard A. Posner, "The Truth About Our Liberties," *The Responsive Community*, Summer 2002, p. 5.

25.Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 SO. CAL. L. REV. 1083 (2002).

26.Roger Clarke, "Information Technology and Dataveillance," November 1987, available at <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html>.

27.Paul Farhi and Linton Weeks, "A Surprise Ending: With the Sniper, TV Profilers Missed Their Mark," *The Washington Post*, October 25, 2002, p. C1.

28.Ann Davis, "Far Afield: FBI's Post-Sept. 11 'Watch List' Mutates, Acquires Life of Its Own," *The Wall Street Journal*, November 19, 2002, p. A1.

29.Charles Simonyi, "I Fit the Profile," *Slate*, May 25, 1997, available at <http://slate.msn.com/?id=2058>.

30.David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Minneapolis: Univ. of Minnesota Press, 1994), p. 197.

31.David Lyon, ed., *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (London and New York: Routledge, 2002).

32.Edward Wong, "In Airport Security, Think Low Tech," *The New York Times,* September 15, 2002, sec. 4, p. 6.

33.Liam Braber *Korematsu's Ghost: A Post-Sept. 11 Analysis of Race and National Security*, 47 VILL. L. REV. 451, 457-58 (2002).

34.*Hearing on Airport Security Before the Subcomm. on Aviation of the House Comm. on Transp. and Infrastructure*, 107th Cong. 64 (2001) (statement of Isaac Yeffett).

35.*Regulations Needed to Ensure Air Safety, Hearing Before the House Gov't. Reform Energy Policy Subcomm. of the House Natural Resources Comm*., 107th Cong. 53 (2001) (statement of Isaac Yeffett).