SKATING ON STILTS

Why We Aren't Stopping Tomorrow's Terrorism

Stewart A. Baker

HOOVER INSTITUTION PRESS
Stanford University Stanford, California

14 Privacy for the Real World

By now you may be asking, "Okay, Mister-I'm-a-privacy-advocate-too, what's *your* solution to the tension between information technology and our current sense of privacy?"

That's a fair question. The short answer is that we should protect privacy, but not by defying the course of technology or by crippling government when it investigates crimes. We can do it by working with technology, not against it. In particular, we can use information technology to make sure that government officials lose *their* privacy when they misuse data that has been gathered for legitimate reasons. Information technology now makes it easier to track every database search made by every user, and then to follow any distribution of that data outside the system. In other words, it can make misuse of the data in government files much more difficult and much more dangerous.

But before talking about what might work, let's take a closer look at some of the ideas that don't. Privacy campaigners have a limited repertoire; they usually roll out one of three basic solutions to the privacy problem. Unfortunately, these three solutions either don't protect our privacy in any meaningful way or they make it so hard to catch terrorists and criminals that they will end up getting thousands of us killed. Or both.

Their first privacy solution is one we've already seen. It's the Brandeisian notion that we should all "own" our personal data. That has some appeal, of course. If I have a secret, it feels a lot like property. I can choose to keep it to myself, or I can share it with a few people whom I trust. And I would like to believe that sharing a secret with

a few trusted friends doesn't turn it into public property. It's like my home. Just because I've invited one guest home doesn't mean the public is welcome.

But in the end, information is not really like property. Property can only be held by one person at a time, or at most by a few people. But information can be shared and kept at the same time. And those with whom it is shared can pass it on to others at little or no cost. If you ever told a friend about your secret crush in junior high you've already learned that information cannot be controlled like property. As Ben Franklin is credited with saying, "Three may keep a secret if two of them are dead." The redistribution of information cannot be easily controlled in the best of times, and Moore's Law is making the control of information nearly impossible.

The recording and movie industries discovered the same thing. If these industries with their enormous lobbying and litigation budgets cannot control information that they own as a matter of law, the rest of us are unlikely to be able to control information about ourselves. Gossip is not going to become illegal simply because technology amplifies it.

That's why Brandeis's proposal never really got off the ground, at least not as he envisioned it. Buoyed by Brandeis's prestige, the idea that private facts are private property lingered on in the courts for years, but what survived of his proposal is scarcely recognizable today.

In fact, so transformed is Brandeis's privacy doctrine that it is now described, accurately, as a "right of publicity," which surely would have him turning in his grave. Currently, most states honor Brandeis by allowing lawsuits for unauthorized commercial use of a person's likeness, either by statute or judge-made law.

Over time, courts lost sight of Brandeis's purpose. They began to take the analogy to property literally. Brandeis wanted to treat private information like property because that was the only way to give a remedy for the "mental pain and distress, far greater than could be inflicted by mere bodily injury," that he thought a man suffered when his photo was published without permission. But as people got used

to having their pictures taken, the mental pain and distress slowly drained out of the experience.

All that was left was the property analogy. And so judges began shrinking the right until it only had bite in the one set of circumstances where the right to control one's image actually feels like a property right—when the image is worth real bucks. Thus, the courts require disgorgement of profits made when a celebrity's name, face, voice, or even personal style is used without permission to sell or endorse products. As a result, the right to exploit a celebrity's image really is property today; it can be sold, transferred, and even inherited.

There's only one problem with this effort to turn privacy into property. It hasn't done much for privacy. It simply protects the right of celebrities to make money off their fame. In fact, by monetizing things like celebrity images, it rewards those who have most relentlessly sacrificed their privacy to gain fame.

The right of publicity is well named. It is the right to put your privacy up for sale. Not surprisingly, a lot of people have been inspired to do just that. Ironically, Brandeis's doctrine has helped to destroy the essence of what he hoped to preserve.

Oh, and in the process, Brandeis's approach has stifled creativity and restricted free speech—muzzling artists, social commentators, and businesspeople who want to make creative use of images that are an essential part of our cultural environment. It's a disaster. Slowly, courts are waking up to the irony and limiting the right of publicity.

The same "private information as property" approach has also made a modest appearance in some consumer privacy laws, and it's worked out just as badly. At bottom, consumer privacy protection laws like the Right to Financial Privacy Act[1] treat a consumer's data like a consumer's money: You can give your data (or your money) to a company in exchange for some benefit, but only if you've been told the terms of the transaction and have consented. Similarly, the Cable Communications Policy Act of 1984[2] prevents cable providers from using or releasing personal information in most cases unless the providers get the customer's consent.

The fruit of this approach is clear to anyone with a bank account or an Internet connection. Everywhere you turn, you're confronted with "informed consent" and "terms of service" disclosures; these are uniformly impenetrable and non-negotiable. No one reads them before clicking the box, so the "consent" is more fiction than reality; certainly it does little to protect privacy. Indeed, it's turning out a lot like the right of publicity. By treating privacy as property, consumer privacy protection law invites all of us to sell our privacy.

And we do. Only for most of us, the going price turns out to be disconcertingly cheap.

The second way of protecting privacy is to require what's called a "predicate" for access to information. That's a name only a lawyer could love. In fact, the whole concept is one that only lawyers love.

Simply put, the notion is that government shouldn't get certain private information unless it satisfies a threshold requirement—a "predicate" for access to the data. Lawyers have played a huge role in shaping American thinking about privacy, and the predicate approach has been widely adopted as a privacy protection. But its value for that purpose is quite doubtful.

The predicate approach to privacy can be traced to the Fourth Amendment, which guarantees that "no Warrants shall issue, but upon probable cause." Translated from legalese, this means that the government may not search your home unless it has a good reason to do so. When the government asks for a search warrant, it must show the judge "probable cause"—evidence—that the search will turn up criminal evidence or contraband. Probable cause is the predicate for the search.

Lawyers spend a lot of time thinking about the Fourth Amendment. Every law student spends weeks exploring its intricacies. Evidence from an illegal search cannot be used in a criminal prosecution. So millions of defendants have made claims under the Fourth Amendment after being convicted, giving the courts many opportunities to apply the amendment. All problems look like a nail to someone who has only a hammer.

And all privacy problems tend to look like the Fourth Amendment to lawyers who have grown up parsing its protections.

It's been applied to cops on the beat, for example. A traffic stop is pretty close to an arrest, and a pat-down is even closer to a full-fledged search. But requiring warrants and probable cause would make it impossible to pat down rough customers in a bad part of town or to stop drivers just to check license and registration. So the courts came up with a new predicate for such intrusions on our freedom—"reasonable suspicion."

When a flap arose in the 1970s over the FBI practice of assembling domestic security dossiers on Americans who had not broken the law, the attorney general stepped in to protect their privacy. He issued new guidelines for the FBI. He was a lawyer, so he declared that the FBI could not do domestic security investigations of Americans without a predicate.

The predicate wasn't probable cause; that was too high a standard. Instead, the attorney general allowed the launching of a domestic security investigation only if the bureau presented "specific and articulable facts giving reason to believe" that the subject of the investigation may be involved in violence.

Actually, the story of the FBI guidelines shows why the predicate approach often fails. The dossiers being assembled by the FBI were often just clippings and other public information. They usually weren't the product of a search in the classic sense; no federal agents had entered private property to obtain the information. Nonetheless, the FBI guidelines treated the gathering of the information itself as though it were a kind of search.

In so doing, the guidelines were following in Brandeis's footsteps—treating information as though it were physical property. The collection of the information was equated to a physical intrusion into the home or office of the individual. Implicitly, it assumes that data can be locked up like property.

But that analogy has already failed. It failed for Brandeis and it failed for the RIAA. It failed for the FBI guidelines, too. As clippings became easier to retrieve, clippings files became easier to assemble.

Then Google made it possible for anyone to assemble an electronic clips file on anyone. There was nothing secret about the clippings then. They were about as private as a bus terminal.

But the law was stuck in another era. Under the guidelines, the FBI and the FBI alone needed a predicate to print out its Google searches. You have to be a pretty resilient society to decide that you want to deny to your law enforcement agencies a tool that is freely available to nine-year-old girls and terrorist gangs. Resilient but stupid. (Not surprisingly, the guidelines were revised after 9/11.)

That's one reason we shouldn't treat the assembling of data as though it were a search of physical property. As technology makes it easier and easier to collect data, the analogy between doing that and conducting a search of a truly private space will become less and less persuasive. No one thinks government agencies should have a predicate to use the White Pages. Soon, predicates that keep law enforcement from collecting information in other ways will become equally anachronistic, leaving law enforcement stuck in the 1950s while everyone else gets to live in the twenty-first century.

I saw this lawyerly affinity for predicates up close at DHS. The issue was laptop searches at the border. The government has always had the right to search anything crossing the border without probable cause. Smugglers are smart and highly motivated; they would find a way to exploit any limitations on the authority to conduct searches. The first Congress knew that quite well, and in 1789, two months before it sent the Fourth Amendment to the states for approval, Congress gave the customs service "full power and authority" to search "any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed."[3]

Obviously, DHS and its border predecessors didn't search laptops in 1789. But they did search books, papers, correspondence, and anything else that could store information. That was the law for two hundred years, with one exception. The Supreme Court has ruled that a few extraordinarily intrusive techniques—body cavity searches and forced x-rays—require a "reasonable suspicion."[4]

Laptops are treated like books and papers. They are searched whenever border officials think that such a search is likely to be productive. And even the famously liberal Ninth Circuit, the court of appeal that includes California, has had no trouble approving that practice.[5]

For good reason. Laptop searches pay off.

Take *United States v. Hampe*, triggered by a 2006 border search at Bar Harbor, Maine. The search turned up a laptop with numerous images of child pornography; officers also found "children's stickers, children's underwear, children's towels or blankets with super heroes printed on them," as well as "12-15 condoms" and "a container of personal lubricant." The lawbooks are full of unsuccessful appeals by convicted pedophiles and child porn smugglers, claiming that the laptops holding the evidence against them should not have been searched without a predicate.[6]

After 9/11, we used laptop searches to find possible terrorists. That's in part because investigators famously failed to inspect the laptop of one of the 9/11 conspirators, Zacarias Moussaoui, when it might have done some good. Found early enough, the information on his laptop might have helped uncover Moussaoui's ties to al Qaeda. Having learned that lesson, we began using laptop searches more often when terrorism was a risk.

In 2006, for example, border officials at the Minneapolis-St. Paul airport referred a suspect traveler to secondary inspection. There they found that his computer contained video clips of IEDs being used to kill soldiers and destroy vehicles and a video on martyrdom. He was also carrying a manual on how to make improvised explosive devices, or IEDs—a weapon of choice for terrorists in Afghanistan and Iraq.

Despite two hundred years of history and precedent, as well as the proven value of searching electronic media, privacy groups launched a campaign against laptop searches toward the end of the Bush administration. This was a strange and unhappy era in the debate over privacy. By 2005, privacy advocates had found a growing audience for claims that the Bush administration had abandoned all limits in pursuing

terrorism—that it had swung the pendulum violently away from privacy and in favor of government authority.

By attacking alleged privacy violations in the war on terror, the privacy groups found that they could tap a passionate core of support. But apart from adoption of the USA PATRIOT Act, there hadn't been that many domestic legal changes after 9/11. But the privacy groups weren't about to stop shooting just because they were running out of targets. Instead, the rights groups started attacking security practices that had been established in the 1990s or earlier. I watched the return to pre-September 11 thinking with dismay. But even I was surprised to find groups seriously proposing to swing the pendulum back, not to September 10, 2001, but to July of 1789. (Perhaps I didn't realize, said one colleague, just how long the ACLU thought the Bush administration had been in power.)

The privacy advocates' solution to the laptop issue was the lawyer's favorite—a predicate requirement. Laptops should not be searched at the border, they argued, unless the border official could articulate some specific reason for conducting the search. That argument was rejected by both the Bush and the Obama administrations after careful consideration.

We rejected it for two reasons. It wouldn't have protected privacy in any meaningful way. And it would have helped pedophiles and terrorists defeat our border defenses. Other than that, it was jim-dandy.

Why wouldn't it help protect privacy? Because as a practical matter, no border official today searches a laptop without some reasonable suspicion about the traveler. The exponential increase in commercial jet travel and the unforgiving thirty-second rule mean that only one traveler in two hundred is sent to secondary inspection for a closer look. Once there, many travelers quickly satisfy the officials that they don't deserve more detailed inspection.

Everyone at the border is busy; there's another jet or another bus arriving in minutes. Border officers don't have the luxury of hooking up the laptops of random travelers for inspection without a good reason. Officers who waste their time and DHS's resources that way are

going to hear from their supervisors long before they hear from the travelers' lawyers.

Okay, you may say, the rule wouldn't do much good. But surely it can't hurt, can it? If border officials only search laptops today when they have a good reason to do so, why not make that a requirement? What harm can it do to make reasonable suspicion a predicate for laptop searches at the border?

Plenty. Requiring reasonable suspicion before a laptop search will open every border search to litigation. And in court, it may be hard to justify even some very reasonable judgments.

Sometimes, the primary inspector will send the traveler to secondary simply because the inspector is not comfortable with the traveler. Remember Mohamed al Kahtani—the twentieth hijacker? He was sent to secondary inspection on the basis of intuition—there was no evidence of illegality in the fact that he did not speak English and hadn't filled out his arrival forms. But the inspector's intuition was dead right. Kahtani deserved all the scrutiny he got, and more. Still, if the inspector had opened the terrorist's laptop on the basis of his intuition, could he have been sure the courts would agree that he had a reasonable suspicion? That uncertainty would undermine the effectiveness of border procedures, perhaps giving a free ride to wealthy travelers or those who threaten legal action if they are delayed.

Inevitably, enforcement of a predicate requirement for border searches will produce litigation. The litigation will focus on the motives of the border officials. The courts will tell those officials that some reasons are not good enough. Defense lawyers will want to see the personnel records of border officials, hoping to show that they've inspected a disproportionate number of laptops belonging to minorities, or to Saudis, or to men, or any other pattern that might get the case thrown out. Border officials will have to start keeping detailed records justifying each laptop search. New paperwork and new procedures will clog the inspection process, backing up travelers and penalizing any inspector who searches a laptop.

A predicate requirement would mean that every official who inspects a laptop will get to spend quality time on the stand with a defense counsel dedicated to questioning the officer's motives and painting the officer as a racist, sexist, or whatever else the lawyer thinks might work. In close cases, it's inevitable that border officials will be slow to conduct a search that brings with it a host of paperwork and the chance to be cross-examined. And that inevitably means that we'll catch fewer criminals and terrorists.

Wait a minute, you might ask, what if those officials really are racists or sexists? Shouldn't we do something about that? Surely my laptop shouldn't be searched because of prejudice?

A lot of academics and lawyers are too quick to assume that law enforcement is full of racists or sexists; disliking cops is about the only form of prejudice that is still respectable in their circles.

But let's assume that their prejudice is right, at least sometimes, and that there are biased officials at work on the border. Surely there's a better way to find them and get them off the job than to count on criminal defense lawyers exposing them on the witness stand years after the event.

By now, notice, we're not even talking about privacy anymore. The "predicate" solution has, in effect, changed the subject. We're talking about the motives of border officials, or ethnic profiling, or something; but it isn't privacy. We're also moving the whole discussion into territory that lawyers find comfortable but that ordinary people might question.

The Fourth Amendment approach to privacy assumes that privacy is best protected by letting criminals challenge the search that produced the evidence against them. But before adopting that solution, we ought to be pretty sure that we're going to get benefits that match the cost of letting guilty defendants go free, something that isn't obvious here.

The predicate solution also creates more litigation and gives lawyers new power to discomfit officials. It's easy to see why that would appeal to lawyers, but American litigation is surely the most costly policymaking process on the planet—and not exactly democratic,

either. Again, we'd need to foresee real benefits that can't be achieved in some other fashion before buying into that approach. And, for all the reasons I've given, there are very few benefits to be gained from the "predicate" approach to most privacy problems.

That leaves the third approach to privacy, one we've already seen in action. If requiring a predicate is the lawyer's solution; this third approach is the bureaucrat's solution. It is at heart the approach adopted by the European Union: Instead of putting limits on when information may be collected, it sets limits on how the information is used.

The European Union's data protection principles cover a lot of ground, but their unifying theme is imposing limits on how private data is used. Under those principles, personal data may only be used in ways that are consistent with the purposes for which the data were gathered. Any data that is retained must be relevant to the original purposes and must be stored securely to prevent misuse.

The EU's negotiating position in the passenger name records conflict was largely derived from this set of principles. The principles also explain Europe's enthusiasm for a wall between law enforcement and intelligence. If DHS gathered reservation data for the purpose of screening travelers when they cross the border, why should any other agency be given access to the data? This also explains the EU's insistence on short deadlines for the destruction of PNR data. Once it had been used to screen passengers, it had served the purpose for which it was gathered and should be promptly discarded.

There is a core of sense in this solution. It focuses mainly on the consequences of collecting information, and not on the act of collection. It doesn't try to insist that information is property. It recognizes that when we give information to others, we usually have an expectation about how it will be used, and as long as the use fits our expectations, we aren't too fussy about who exactly gets to see it. By concentrating on how personal information is used, this solution may get closer to the core of privacy than one that focuses on how personal information is collected.

It has another advantage, too. In the case of government databases, focusing on use also allows us to acknowledge the overriding importance of some government data systems while still protecting against petty uses of highly personal information.

Call it the deadbeat-dad problem, or call it mission creep, but there's an uncomfortable pattern to the use of data by governments. Often, personal data must be gathered for a pressing reason—the prevention of crime or terrorism, perhaps, or the administration of a social security system. Then, as time goes on, it becomes attractive to use the data for other, less pressing purposes—collecting child support, perhaps, or enforcing parking tickets. No one would support the gathering of a large personal database simply to collect unpaid parking fines; but "mission creep" can easily carry the database well beyond its original purpose. A limitation on use prevents mission creep, or at least forces a debate about each step in the expansion.

That's all fine. But in the end, this solution is also flawed.

It, too, is fighting technology, though less obviously than the predicate and property approaches. Data that has already been gathered *is* easier to use for other purposes. It's foolish to pretend otherwise. Indeed, developments in information technology in recent years have produced real strides in searching unstructured data or in finding relationships in data without knowing for sure that the data will actually produce anything useful. In short, there are now good reasons to collate data gathered for widely differing purposes, just to see the patterns that emerge.

This new technical capability is hard to square with use limitations or with early destruction of data. For if collating data in the government's hands could have prevented a successful terrorist attack, no one will congratulate the agency that refused to allow the collation because the data was collected for tax or regulatory purposes, say, and not to catch terrorists.

What's more, use limitations have caused great harm when applied too aggressively. The conflict with the EU is a reminder that the "wall" between law enforcement and intelligence was at heart a use limitation.

It assumed that law enforcement agencies would gather information using their authority, and then would use the information only for law enforcement purposes. Intelligence agencies would do the same. Or so the theory went. But strict enforcement of this use limitation ended up preventing cooperation that might have thwarted the 9/11 attacks.

Like all use limitations, the "wall" between law enforcement sounded reasonable enough in the abstract. While no one could point to a real privacy abuse arising from cooperation between the intelligence and law enforcement agencies in the United States, it was easy to point to the Gestapo and other totalitarian organizations where there had been too much cooperation among agencies.

What was the harm in a little organizational insurance against misuse of personal data, the argument ran. The rules allowed cooperation where that was strictly necessary, and we could count on the agencies to crowd right up to the line in doing their jobs. Or so we thought. In fact, we couldn't. As the pressure and the risk ratcheted up, agents were discouraged from pushing for greater communication and cooperation across the wall. All the Washington-wise knew that the way to bureaucratic glory and a good press lay in defending privacy. Actually, more to the point, they knew that bad press and bureaucratic disgrace were the likely result if your actions could be characterized as hurting privacy. Congress would hold hearings; appropriators would zero out your office; the second-guessing arms of the Justice Department, from the inspectors general to the Office of Professional Responsibility, would feast on every detail of your misstep. So, what might have been a sensible, modest use restriction preventing the dissemination of information without a good reason became an impermeable barrier.

That's why the bureaucratic system for protecting privacy so often fails. The use restrictions and related limits are abstract. They make a kind of modest sense, but if they are enforced too strictly, they prevent new uses of information that may be critically important.

And often they are enforced too strictly. You don't have to tell a bureaucrat twice to withhold information from a rival agency.

Lawsuits, bad press, and Congressional investigations all seem to push against a flexible reading of the rules. If a use for information is not identified at the outset, it can be nearly impossible to add the use later, no matter how sensible the change may seem. This leads agencies to try to draft broad uses for the data they collect, which defeats the original point of setting use restrictions.

It's like wearing someone else's dress. Over time, use restrictions end up tight where they should be roomy—and loose where they should be tight. No one is left satisfied.

So what will work? Simple: accountability, especially electronically-enforced accountability.

The best way to understand this solution is to begin with Barack Obama's passport records—and with Joe the Plumber. These were two minor flaps that punctuated the 2008 presidential campaign. But both tell us something about how privacy really is protected these days.

In March of 2008, Barack Obama and Hillary Clinton were dueling across the country in weekly primary showdowns. Suddenly, the campaign took an odd turn. The Bush administration's State Department announced that it had fired or disciplined several contractors for examining Obama's passport records.

Democrats erupted. They remembered when Bill Clinton's files had been examined during the 1992 campaign, and Obama's lengthy stays outside the United States as a child had become a simmering underground issue in this campaign. It wasn't hard to jump to the conclusion that the candidate's files had been searched for partisan purposes. An Obama campaign spokesman called the records search "outrageous . . . This is a serious matter that merits a complete investigation, and we demand to know who looked at Senator Obama's passport file, for what purpose, and why it took so long for them to reveal this security breach."[7]

After an investigation, the flap slowly deflated. It soon emerged that all three of the main presidential candidates' passport files had been improperly accessed. Investigators reported that the State Department was able to quickly identify who had examined the files

by using its computer audit system. This system flagged any unusual requests for access to the files of prominent Americans. The fired contractors did not deny the computer record. Several of them were charged with crimes and pleaded guilty. All, it turned out, had acted purely out of "curiosity."

Six months later, it was the Republicans' turn to howl about privacy violations in the campaign. "Joe" Wurzelbacher, a plumber, became an overnight hero to Republicans in October 2008. After all, he was practically the only person who laid a glove on Barack Obama during the campaign. The candidate made an impromptu stop in Wurzelbacher's Ohio neighborhood and was surprised when the plumber forced him into a detailed on-camera defense of his tax plan. Three days later, "Joe the Plumber" and his taxes were invoked dozens of times in the presidential debates.

The price of fame was high. A media frenzy quickly stripped Joe Wurzelbacher of anonymity. Scouring the public record, reporters found that the plumber had been hit with a tax lien; they also found government data that raised doubts about the status of his plumbing license.

Reporters weren't the only ones digging. Ohio state employees also queried confidential state records about Wurzelbacher. In all, they conducted eighteen state records checks on Wurzelbacher. They asked whether the plumber owed child support, whether he'd ever received welfare or unemployment benefits, and whether he was in any Ohio law enforcement databases. Some of these searches were proper responses to media requests under Ohio open records laws; others looked more like an effort to dig dirt on the man.

Ohio's inspector general launched an investigation and in less than a month was able to classify all but one of the eighteen records searches as either legitimate or improper. (One search could not be traced because it came from an agency outside the jurisdiction of the inspector general.)[8]

Thirteen searches were traced and deemed proper. But three particularly intrusive searches were found improper; they had been carried out at the request of a high-ranking state employee who was also

a strong Obama supporter. She was suspended from her job and soon stepped down. A fourth search was traced to a former information technology contractor who had not been authorized to search the system he accessed; he was placed under criminal investigation.

What do these two flaps have in common? They were investigated within weeks of the improper access, and practically everyone involved was immediately caught. That's vitally important. Information technology isn't just taking away your privacy or mine. It's taking away the privacy of government workers even faster. Data is cheap to gather and cheap to store. It's even getting cheap to analyze.

So it isn't hard to identify every official who accessed a particular file on a particular day. That's what happened here. And the consequences for privacy are profound.

If the lawyer's solution is to put a predicate between government and the data and the bureaucrat's solution is to put use restrictions on the data, then this is the auditor's solution. Government access to personal data need not be restricted by speed bumps or walls. Instead, it can be protected by rules, so long as the rules are enforced.

What's new is that network security and audit tools now make it easy to enforce the rules. That's important because it takes the profit motive out of misuse of government data. No profit-motivated official is going to take the risk of stealing personal data if it's obvious that he'll be caught as soon as people start to complain about identity theft. Systematic misuse of government databases is a lot harder and more dangerous if good auditing is in place.

Take another look at why government officials accessed these files. It wasn't to steal identities. (In fact, these would be pretty dumb places to go for identity theft. If you want to know what's in your passport file, get your passport out and take a look at the one page with printed data on it. It's got less sensitive information than your driver's license—a photo and your birth date and state. Not even an address, let alone a Social Security number or credit card number.)

No, the reason most of these people accessed the data was simple curiosity. Even the one access that may have been for more

reprehensible reasons—the woman who checked confidential child support and welfare records for Joe the Plumber—was quickly caught and the data never leaked.

The speed and nearly complete effectiveness of the audit process in these cases tells us that network auditing tools can transform the way we enforce the rules for handling data in government. For example, if we catch every error, we can improve compliance and at the same time reduce the penalties for mistakes. Harsh penalties are not the most effective way to enforce rules. In fact, they're usually a confession of failure. When we can't stop a crime, we keep increasing the penalties, to make an example of the few offenders we do catch. But when we catch every offender, we can afford to lower the penalty. Parking fines are lower than tickets for driving alone in a car pool lane in part because parking violators are easier to catch.

Lighter, more certain penalties for privacy violations serve another purpose, too. We've talked a lot about the oddly protean nature of privacy. Not causing harm in unexpected ways is at the core of the concept, but it's nearly impossible to write detailed rules spelling out what is and is not a violation of privacy. Indeed, the effort to write such rules and stick to them is what gave us the wall, and thousands of American dead. So something must be left to discretion. Government employees must use good sense in handling personal data. If they don't, they should be punished. But if we are confident that we can identify any questionable use of personal data and correct it quickly, the punishments can be smaller. They can be learning experiences rather than penological experiences.

So why did we criminally prosecute the poor schlubs whose hobby was looking at the passport pictures of famous people? Everyone would agree that they shouldn't have done it and that they should have been disciplined. But a criminal record? How did that happen?

The election happened. Everything that touched on the election was put under a microscope. Evil motives were always ascribed to the other side. The State Department had to make a blood sacrifice to show that accessing the data was not part of an evil plot by one

party against the other. Opening a criminal investigation was a way of condemning the access in the clearest possible fashion. That the poor schlubs probably only deserved demotions counted for little in the super-heated atmosphere of a presidential campaign.

That shows one of the problems with the audit approach. It is too easily turned into a phony privacy scandal. In both the Wurzelbacher and Obama cases, the audits did their job. With one possible exception, they caught the government staff that broke the rules. They prevented any harm to either Wurzelbacher or Obama. And they made sure that the officials who were responsible would never repeat their errors again.

The system worked. Privacy was protected. But that's certainly not the impression that was left by coverage of the affairs. Indeed, the chairman of the Senate Judiciary Committee, Senator Leahy, used the passport flap to tout new legislation strengthening privacy protections on government databases.

From a political point of view, then, the system failed. There were no thanks for the government officials who put the system in place, who checked the audit logs, who confronted and disciplined the wrongdoers, and who brought the solved problem to public attention. To the contrary, they were pilloried for allowing the access in the first place—even though preventing such access is an impossible task unless we intend to re-erect walls all across government.

How's that for irony? Audits work. But they work too well. Every time they catch someone and put a stop to misuse of personal data they also provide an opening for political grandstanding. In the end, the finger pointing will discourage audits. And that will mean less privacy enforcement. So, the more we turn every successful audit into a privacy scandal, the less real privacy we're likely to have.

That would be a shame, because the auditor's solution to the problem is the only privacy solution that will get more effective as technology advances. And we're going to need more solutions that allow flexible, easy access to sensitive databases while still protecting privacy.

If the plight of government investigators trying to prevent terrorist attacks doesn't move you, think about the plight of medical technicians trying to keep you alive after a bad traffic accident.

The Obama administration has launched a long-overdue effort to bring electronic medical records into common use. But the privacy problem in this area is severe. Few of us want our medical records to be available to casual browsers. At the same time, we can't personally verify the bona fides of the people accessing our records, especially if we're lying by the side of the road suffering from what looks like brain or spine damage.

The electronic record system won't work if it can't tell the first responders that you have unusual allergies or a pacemaker. It has to do that quickly and without a lot of formalities. The side of the road is no place for emergency medical staff to be told that they can't access your records until they change their passwords or send their medical credentials to a new hospital. No one wants to be the punch line in an updated surgeon's joke: "The privacy system was a success; unfortunately it killed the patient."

Auditing access after the fact is likely to be our best answer to this problem, as it is to the very similar problem of how to let law enforcement and intelligence agencies share information smoothly and quickly in response to changing and urgent circumstances. The Markle Foundation has done pioneering work in this area, and its path-breaking 2003 report on privacy and security in the war on terror recommends embracing technologies that watch the watchers. A unique mix of security, privacy, and technology experts managed to reach agreement in that report; they found that one key to protecting privacy without sacrificing security was a network that included "access control, authentication, and full auditing capability."[9]

The Markle report urges that large databases with personal information use emerging technologies that can identify all users of the system with certainty and then give them access that depends on their roles at any particular time. This includes "the ability to restrict access privileges so that data can be used only for a particular purpose, for a

finite period of time, and by people with the necessary permissions."[10] The technologies they cited are not pie in the sky. They exist today: "smart cards with embedded chips, tokens, biometrics, and security circuits" as well as "[i]nformation rights management technologies."[11] The Markle task force later did a thoughtful paper on one of those technologies, which would preserve audit logs even if high-ranking officials seek to destroy or modify them later.[12]

These technologies can be very flexible. This makes them especially suitable for cases where outright denial of data access could have fatal results. The tools can be set to give some people immediate access, or to open the databases in certain situations, with an audit to follow. They can monitor each person with access to the data and learn that person's access patterns—what kinds of data, at what time, for how long, with or without copying, and the like. Deviations from the established pattern can have many consequences. Perhaps access will be granted but the person will be alerted that an explanation must be offered within twenty-four hours. Or access could be granted while a silent alarm sounds, allowing systems administrators to begin a real-time investigation.

There's a kind of paradox at the heart this solution. We can protect people from misuse of their data, but only by stripping network users of any privacy or anonymity when they look at the data. The privacy campaigners aren't likely to complain, though. In our experience, their interest in preserving the privacy of intelligence and law enforcement officers is pretty limited.

When I was general counsel of the National Security Agency, a well-known privacy group headed by Marc Rotenberg filed a Freedom of Information Act request asking the NSA to assemble all documents and emails sent "to or from Stewart Baker." Then as now, the NSA was forbidden to assemble files on American citizens who were not agents of a foreign power. Even so, Rotenberg was asking NSA to assemble a dossier on me. Since NSA and I were locked in a battle with Rotenberg over encryption policy at the time, the purpose of the dossier was almost certainly to look for embarrassing information that might help Rotenberg in his political fight. Indeed, Rotenberg

claimed when I confronted him that he was planning to scrutinize my dossier for evidence of misconduct.

Had the FBI or NSA assembled a dossier on *their* political adversaries, it would have been a violation of law. In fact, it would have caused a privacy scandal. But Rotenberg saw no irony in his request. It wasn't a privacy problem, in his view, because government officials deserve no privacy.

I still think Rotenberg's tactics were reprehensible; he had singled me out for a selective loss of privacy because he didn't like my views. But I've come to appreciate that there's a core of truth to his view of government. Anyone who has access to government files containing personal data has special responsibilities. He should not expect the same privacy when he searches that data as he has while he's surfing the net at home. And now that technology makes it easy to authenticate and track every person, every device, and every action on a network, perhaps it's time to use that technology to preserve everyone else's privacy.

In the end, that's the difference between a privacy policy that makes sense and one that doesn't. We can't lock up data that is getting cheaper every day. Pretending that it's property won't work. Putting "predicates" between government and the data it needs won't work. And neither will insisting that they may only be used for purposes foreseen when it was collected.

What we *can* do is use new information technology tools to deter government officials from misusing their access to that data.

As you know by now, I think that some technology poses extraordinary risks. But we can avoid the worst risks if we take action early. We shouldn't try to stop the trajectory of new technology. But we can bend it just a little. Call it a course correction on an exponential curve.

That's also true for privacy. The future is coming, like it or not. Our data will be everywhere. But we can bend the curve of technology to make those who hold the data more accountable.

Bending the exponential curve a bit. That's a privacy policy that could work.

And a technology policy that makes sense.

The Hoover Institution on War, Revolution and Peace, founded at Stanford University in 1919 by Herbert Hoover, who went on to become the thirty-first president of the United States, is an interdisciplinary research center for advanced study on domestic and international affairs. The views expressed in its publications are entirely those of the authors and do not necessarily reflect the views of the staff, officers, or Board of Overseers of the Hoover Institution.

www.hoover.org

Hoover Institution Press Publication No. 591

Hoover Institution at Leland Stanford Junior University,
Stanford, California, 94305–6010

First printing 2010
16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

Manufactured in the United States of America

The paper used in this publication meets the minimum Requirements of the American National Standard for Information Sciences—Permanence of Paper for Printed Library Materials, ANSI/NISO Z39.48-1992. ♾

Cataloging-in-Publication Data is available from the Library of Congress.
ISBN-13: 978-0-8179-1154-6 (cloth)

ISBN-13: 978-0-8179-1156-0 (e-book)