



Identity, Privacy & Security—Can Technology Really Reconcile Them?

**David Loukidelis
Information and Privacy Commissioner for British Columbia**

February 2004

Good morning everyone. I'm very pleased, and rather surprised, to see such a large number of you here so early in the morning to hear me speak about identity, privacy and security—especially those of you who've heard me speak before.

Let me start by doing two things. First, I should tell you that after I heard my good friend and colleague Ann Cavoukian speak so compellingly yesterday, as she always does, I scurried up the street to my office and started re-working my remarks. Now, it shouldn't surprise you or me, given the theme of this conference and what Ann and I do for a living, that her speech and mine would share some ground. Still, what follows to a considerable degree shifts

the focus of my remarks from what I had worked up before yesterday.

The second thing I'm going to do is conduct a scientifically-valid poll—right here, right now—about security. The results of this poll will be valid 20 times out of 20 and there will be no margin of error. Actually, it occurs to me that, as soon as I leave this room, I should run back to my office and publish the poll's results in an on-line journal that is *not* academically refereed and that accepts advertising from both security technology manufacturers *and* privacy consultants.

Now for my rigorously defined poll, which has several questions. After the poll is completed, I will explore some implications for our privacy of the answers you will give—I'm not displaying any bias here—and the conditions underlying those answers.

First, let me see your hands up—way up high—if you *feel* secure sitting here today?

OK, that's about ___% of you. Maybe you're the intuitive ones amongst us today.

Let me see your hands—even higher up—if you actually *know* beyond a doubt that you are completely secure from harm sitting here today.

So about ____% of you are smarty-pants know-it-alls.

Next, how many of you either feel or know, for sure, that you're *less*—not more—secure today than on September 10, 2001?

For the roughly ____% of you who believe you're more vulnerable now than you were before 9/11, your belief raises some questions. Does your perception of increased vulnerability stem from *certain* knowledge that you are, *factually*, less safe? Or does your perception of vulnerability refer to a state of mind in which you *feel* less protected for reasons you find it difficult to identify or quantify?

I've asked you these questions because in recent years—especially since September 9, 2001—our public discourse has tended to assign great, and sometimes almost super-ordinate, value to 'security' and 'safety'. Our political leaders and pundits commonly speak of the need to maximize security—to protect us from harm—and in doing so they usually explicitly characterize

the security imperative as being driven by risks of harm from terrorist acts.

Now, I'm not for one second suggesting that law enforcement and security agencies shouldn't be trying to protect us from harm—that's their job and I'm grateful to them for doing it. Nor am I implying that everything is the way it was before 9/11—that would be a silly thing to suggest. What I am suggesting, however, is that the focus on—some might say, obsession with—security generally fails to account for the different meanings it can have, which in turn has significant implications for how we assess security risks and for the actions we take to enhance security.

Our failure to define what we mean by security, and what it means for our lives individually and as a society, means that our assessments of security threats are prone to both unintentional and, dare I say it, intentional distortion. And distorted analysis can and will have potentially serious implications for our safety, on the one hand, and for our privacy and other rights and freedoms. My point is we must be as dispassionate, as politically disinterested, and as rational as possible in assessing security risks, in considering measures to enhance security, and in analyzing their inter-play with our rights and freedoms.

Let me first re-state the question I asked each of you to answer a minute ago—does ‘security’ for you mean a state of being in which an individual is protected against physical harm? Is it a state of being where she’s at ease, where she’s free from worry? More likely, without thinking about it, we perceive ‘security’ as blending each of these concepts—we see ‘security’ as a state in which our bodies *and* our minds are safe and at ease. This is to state the obvious, since how we feel is to greater or lesser degrees connected with our knowledge of the risk of physical peril, our awareness that we or are not physically safe.

Most of us would agree, of course, that we should, as a society, try to optimize both the feeling and the actuality of security. The rub, of course, is that it’s possible to *feel* less secure even though we are not. We can only make our individual judgements about our level of our security—or that of our loved ones—based on the information we have about the world around us and the risks it presents. But what information do we have these days? Because we depend on information about the world around us, it’s entirely possible that we can feel or believe we are more vulnerable, believe we are less secure, even though we are not.

Let me give you one example from my work as a privacy commissioner. I've on many, many occasions had to respond to those who support increased police surveillance of our streets because crime rates are skyrocketing and our communities are daily descending ever further into vicious lawlessness.

We're constantly bathed, if we want, in the bloody red glow of crime shows that daily depict, in graphic detail, the most gruesome imaginable murders. These images are projected right into our homes, our most private places, and we sit there in grim, transfixed fascination. When we turn on the news, surf the Internet or read the newspaper, we have instant—often literally graphic—access to information about murders and atrocities around the world. This diet of crime and violence surely is part of what makes us feel less safe—and in saying this, I'm *not* blaming the media. We get what we ask for.

But we're allowing this information to distort our perceptions of risk. Canadian crime statistics, at least, tell a different tale than the perception many of us have about violent crime. Year after year since 1991, violent crime has gone down in Canada. There was a noticeable spike upward in the 1970s, as us Baby Boomers broke into our violent stride, but violent crime has been trending down

for well over a decade. The last time I checked, it was almost 25% lower than in 1991 and still heading down.

So the fear many of us have that we're less secure, and that a crimson tide of violence is about to engulf us, squares with reality TV and not reality. And many of us therefore support more scrutiny, more surveillance of the population, because we *feel* less safe against all evidence.

The UK offers a good example of how feelings about safety can override. Polls there have shown that a clear majority of the British public accept the pervasive video surveillance in that country. Violent crime in the UK is not decreasing like it is here, and has increased in recent years in many areas, so one wonders how well video surveillance is working to enhance security, if it's working at all (something even Home Office studies have questioned). Yet the efficacy of all this routine surveillance doesn't seem to matter, since a majority of Britons have also told pollsters they like video surveillance simply because it makes them *feel* safer. Small wonder, you might think, that the British government has in this light spent hundreds of millions of dollars on politically-popular surveillance. The same risk of, quite frankly, garbage-in garbage-out public opinion exists post-9/11—

and the stakes are higher because we're allowing our governments to make those stakes higher.

Speaking of how governments around the world have characterized the risks, and what we are told are the necessary responses, it's always struck me how much the official post-9/11 response has been driven by more than the natural and justified horror we each share about those atrocities—and by more than concerns about risk to ourselves and loved ones. Surely some of the post-9/11 reaction has been driven by the United States' place in the world and the message-shaping power of American media? Surely Canada's relationship with our powerful southern neighbour has much to do with the measures we've taken in Canada? It's got to be more than the scale of the atrocities. After all, as I speak, the Air India murder trial is under way in Vancouver—and remember that on a per capita basis as many mostly Canadian citizens were killed in that one terrorist act as were killed on 9/11.

Returning to my theme, it is crucial after 9/11 that decision-makers not abdicate their responsibility to, as disinterestedly as possible, do three things. First, our elected representatives—they work for us, after all—must focus on real risk. Second, they must at all times act on the knowledge that risk can never be eliminated.

Third, they must act on the principle that pandering to fear, much less creating the conditions for it to flourish, are not acceptable in a free and democratic society.

More specifically, national security measures—ranging from terrorist threat level warnings to routine surveillance of the general population—must never be implemented only to make people *feel* more secure. The public's *comfort* would not by any stretch be sufficient reason, for example, for Parliament to enact the Draconian national security laws that were hastily passed immediately after 9/11. The *appearance* of quick action that such laws communicated to Canadians—making us *feel* like something was being done to protect us—would not be an acceptable motive for these laws.

Jeffrey Rosen—who spoke so well at this conference last year—argues in his excellent new book, *The Naked Crowd*, that our democracies have become or are becoming risk averse. As he points out, much of this has to do with human psychology—with our tendency to let fear of the unknown over-ride rational assessments of risk.

But it's more than that. When our conclusions as to risk are increasingly based on bad information—such as mistaken perceptions of crime—or on information that governments tell us they have, but which must remain secret and unquestioned—our human nature will tend towards fear and towards feelings of insecurity. And why wouldn't politicians be tempted, quite rationally, to pander to that? Their power would, in such an environment, increasingly depend on their instituting measures popularly felt to make us more secure from what we think may be growing crime rates or imminent threats of terrorism.

Maybe it's an impossible thing to expect—I hope and believe not—but our leaders must have the courage to resist, at all times, any instinct for their own short-term political advantage when they assess the need for, and fashion, security laws and measures.

My purpose here is not to be cynical or jaded—far from it. Rather, I'm concerned that we've created, or are at risk of creating, a false dichotomy—between insecurity and fear, on the one hand, and security and comfort, on the other. Give us comfort and peace at all costs, many of us ask—watch over me, keep me safe. Has anything ever been certain, though? We don't need to fall into an abyss of gloom to recognize that nothing is for sure, that there's

always risk—we can't even take for granted the support of a hitherto benign older brother. And yes, that was a purposeful—and perhaps regrettable—allusion to Orwell.

As we move down the road of increased surveillance and diminished rights and freedoms, we have to keep it clearly in view that our steps in that direction will have long-term impact, one way or the other, on our freedom, without there necessarily being any benefit in terms of better or more security. If we yearn to find 'security', therefore, we've got to constantly question what it means and we must always remember that, whatever we are seeking, we risk a great deal for ourselves and the kind of society in which our children will live. Freedom is about risks, and the more freedom you give to people, the greater the risks. The more we try to maximize security, the more we're likely to curtail freedom.

Now more than ever, it's critical that governments not enact any rights-curtailling laws or adopt freedom-limiting security measures simply because they make people feel more secure without actually making them more secure. And even if there's a security enhancement, it's incumbent on governments—applying the usual constitutional tests—to demonstrate that the measure is clearly

justified and that its security benefits outweigh the harm to our rights and freedoms.

Let me give you an example of how a rush to adopt security measures can jeopardize privacy and our other rights. My example is CAPPSS 2. The US government is this year embarking on an anti-terrorist screening program known as CAPPSS 2, which stands for Computer-Assisted Passenger Pre-screening Program, release 2.0.

Reduced to its crude essentials, CAPPSS 2 will build on CAPPSS 1, which is already in place, by aggregating data on air passengers, which will be drawn from a variety of government and commercial sources. There is some doubt as to how the program will actually work on roll-out—the Transportation Security Administration has, in response to criticisms, recently signalled some shift as to how the final configuration will operate.

But CAPPSS 2 will use predictive data mining techniques to assign risk ratings to would-be airline passengers—and good luck if you try to find out how the CAPPSS 2 software was designed and what predictive criteria have been deemed cogent and acceptable. These green, yellow and red risk ratings will be used to decide what level

of security screening should be imposed on individuals. If you're red-coded, you're not going to fly home, as an Iowa college student recently found out when coded red by CAPPs 1. If you're yellow-coded, you'll be put through the ringer before you can get on the plane.

You heard yesterday what Bruce Schneier has said about the rate of false positives in ID systems. What do you think the incidence of false red ratings will be in a system that attempts to assign risk using software that many have pointed out attempts to predict the unpredictable? What will the consequences be for those of us here today, directly or indirectly? Will 10% or 40% of us in this room be falsely branded as red? What will this mean? Apart from being stranded at an airport, will we wind up on terrorist watch lists until we can disprove our guilt?

Another model of CAPPs 2 that's been talked about seems more like an identification verification system. We're hearing lately that public and private sector data—including credit-rating information and government watch lists—will be analysed only in order to determine if you are who you say you are. The suggestion, it seems, is that the data mining software will not predict that you may be a terrorist. It will just identify you as someone who is for

some other reason already a known risk—for example, because you're already on a terrorist watch list.

A December 2003 study by the Consumer Federation of America and the National Credit Reporting Association found errors in names and other identifying information in 1 out of 10 credit reports, which are the very sources of information to be used in this version of CAPPS 2. I've little doubt what Bruce Schneier would say about the number of false positives and false negatives such a system would generate.

Perhaps worse—and this is again something to which Ann alluded yesterday—what will the consequences be of our tendency to be lazy, in this case when the technology—in which we tend to place unwarranted trust—falsely accords someone a green-means-go rating? I was joking yesterday with my friend Bruce Philips—a former Privacy Commissioner of Canada and an eloquent privacy advocate—that for all I know he could be a clean terrorist, a sleeper who's been biding his time. I can't imagine CAPPS 2 would brand Bruce as anything other than green card, which would let him continue to go through life as one of the trusted. And mark my words, if a clean or disposable terrorist is coded green, he or she is almost certain to be waived through security a dozen times

before actually exploiting the system's mis-placed trust and launching an attack. I can hear it now at airport security: "I see you've got a green rating sir, so I won't trouble you further. Have a nice flight."

Systems like CAPPs 2, in other words, promise only one thing for certain—we are all under surveillance and many of us will be wrongly presumed to be guilty or at least suspected of something. These systems will promise only to invade everyone's privacy and will do so in open-ended ways. Quite clearly, collections of primary data—and the secondary information derived using data mining techniques—will be too rich a resource for either criminals or governments to long resist exploiting somehow, sometime. As my predecessor David Flaherty has demonstrated in his comparative work on surveillance societies, the phenomenon of function creep—whether official or illicit—is a law of data protection as absolute as any law of nature. Data collected for one purpose will always find another purpose and that as yet unascertained other purpose could well have profound effects on our privacy and other rights.

Ann Cavoukian has already given you her thoughts on the perils and pitfalls of a national ID card. Like Ann, I testified, last February, about Denis Coderre's ill-defined plans for a national ID

card—or system as he took to calling it—before the Parliamentary Standing Committee on Citizenship and Immigration. I won't repeat what I said then, since Ann said many of the same things yesterday, about the infirmities of a national ID card. I will, however, add my voice to hers in saying that any card or system that attempts a one-to-many identity match is all but destined to be an incredibly costly failure.

Further, a national ID card will almost invariably use a single, universal identifier, and that identifier will *not*, I repeat *not*, be used solely for anti-terrorist purposes or serious crime purposes. You can bet your bottom dollar that it will be used to link databases and track individuals for a much wider array of purposes and such an identifier will be a showcase for function creep. You need only look to Canada's social insurance number, or SIN, for an example of this. Since its introduction in the mid-1960s, the SIN's uses have expanded from the two purposes promised at the time to some 27 legitimized official purposes and countless illegitimate uses. And, while I reject the notion that the SIN is the same as the national ID card talked about last year, its life-experience does illustrate the reality of function creep.

In closing, I readily agree with Ann Cavoukian that technology can be designed to work for security and privacy. Take the example of biometrically-powered authentication systems that Ann mentioned yesterday, which I suggested to the Standing Committee on Citizenship and Immigration should be incorporated into enhanced passports, as an alternative to a new national ID card.

But technology can only serve to reconcile security and privacy if we approach the issues rationally and clearly. We have to *require* decision-makers to clearly define what they mean when they cite the security imperative as prevailing over all else.

We have to force them to assess risk realistically and meaningfully, unswayed by either our own fears or their own political or career interests—and I say this recognizing it's a very tall order.

We have to require decision-makers to be clear-eyed about technology, to adopt only those technologies that actually address real security risks and to do so in ways that, as far as possible, build in privacy protections.

Technology is a tool, though we are often too ready to ascribe magical healing powers to it. It's not up to technology to reconcile privacy, security and identity—it's up to us, using good old-fashioned policy-making methods.

Thank you so much for your time this morning.

* * *