KEYNOTE ADDRESS

THE VALUE OF PRIVACY

ELIZABETH DENHAM
INFORMATION AND PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

12TH ANNUAL PRIVACY AND SECURITY CONFERENCE

February 17, 2011

CHECK AGAINST DELIVERY

Thank you for your very kind introduction.

I am also very pleased to welcome you to Victoria, and I am honoured to participate in this conference with some of the world's best minds in privacy and security.
Our conference speakers and participants come from many different professions and specializations – from cyber-law and e-crime-fighting, to civil liberties and social media research, to name just a few.

I'm also very happy to see many friends and colleagues from out of town, including my colleagues:

Gary Dickson, Information and Privacy Commissioner of Saskatchewan, Dulcie McCallum, my colleague from Nova Scotia, Ken Anderson Assistant Commissioner from Ontario, and an extra warm welcome to Sigrid Artz, from Mexico's Access and Data Protection Authority and so many others.

Whatever our perspectives, the one thing we all have in common is the dedication to identifying and addressing the day to day privacy and security issues. These issues affect billions of people whose personal information is collected, collated, matched and mined through the Internet, as well as through government services. We also share a common interest in discussing the best way to enforce privacy!

We are blessed – or perhaps cursed, some might say – in that we live in a pivotal and fascinating era for those charged with safeguarding privacy while ensuring transparency and accountability in government. We are witnessing breathtaking technological and cultural shifts before our eyes. Getting the public policy right in this climate is essential, yet the challenges in getting it right for privacy regulators, including my office, have never been so great!

Today, I would like to talk about one aspect of those cultural shifts. I can best do this by describing my life with an Internet, Hollywood and, now, Saturday Night Live icon, Mark Zuckerberg. As everyone with a computer knows, Zuckerberg is the co-creator, president and CEO of Facebook, the largest social networking platform on the planet. This could be a very short speech, since I have never had the pleasure of speaking with Mr. Zuckerberg, although he did make a cameo appearance when I visited Facebook's offices in California a couple of years back. My relationship with Mr. Zuckerberg has been more virtual which, given his line of work and mine, is only fitting.

Facebook is closing in on 600 million subscribers posting about a billion new pieces of content daily. It is a global phenomenon. So when Zuckerberg talks, people listen. He has famously declared "privacy as a social norm is no longer relevant." He is not alone in his views.

Former Google CEO Eric Schmidt has also argued privacy is no longer relevant. When asked in a CNBC interview about whether users should be concerned about

sharing so much information with Google, Mr. Schmidt responded, “If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.” To public outcry about Google Street View’s invasion of privacy, Schmidt said concerned citizens could “just move.” Moving to Mars might initially seem like a good choice, but then Google would likely introduce Mars Canal View.

Mr. Zuckerberg also famously stated early last year privacy was being replaced with “a new social norm of not only sharing more information and different kinds, but more openly and with more people.” He believes Facebook itself is a major agent of social change: “We view it as our role in the system,” he said, “to constantly be innovating and be updating what our system is to reflect what the current social norms are.”

Of course, Zuckerberg and Schmidt are not the first to proclaim the alleged irrelevance or demise of this fundamental human right we call privacy. In April 1999, when Zuckerberg was a mere 14 years old, the widely respected magazine, the *Economist* was already saying privacy was doomed. “In the future,” it suggested, “nobody will know for certain who knows what about them. That will be uncomfortable. But the best advice may be: get used to it.”

But is the current social norm really to accept the decline of privacy? I suggest that Schmidt and Zuckerberg’s view of privacy as an outmoded norm has been strongly challenged in recent years.

The Office of the Privacy Commissioner of Canada was responsible for one of those challenges. The Office recognized the emerging threat to personal privacy created by Facebook and other social media. The Commissioner had received a complaint from a privacy advocacy group concerned about the risks to personal information of Canadian Facebook users.

I was Assistant Commissioner at the federal office at the time. My team travelled to Facebook’s offices in Palo Alto, California at the end of an exhaustive, 14-month investigation, to present our findings. Among other privacy concerns, the investigation revealed the excessive sharing of users' personal information with third-party developers that create popular Facebook applications. The federal Privacy Commissioner’s office was the first regulator to delve deeply into the inner workings of social networking sites. It brought to light both the privacy risks and the necessary fixes. The behind-the-scenes story of how the site operates appeared to be a revelation to much of the public.

The office’s final report prompted significant changes in how Facebook handles the sensitive personal information of its users. Among other positive changes, the company agreed to retrofit its application platform to prevent developers from accessing users' personal information unless they give explicit consent. Yes, a small team at the federal Privacy Commissioner’s office helped shape the privacy policies of the mighty Facebook, but even more importantly, raised awareness in the media, the public and other regulators. Of course, the story does not end there. The public and regulators

continue to critique and monitor Facebook as its evolution brings new challenges to users' privacy and security.

Another prominent example of the public's concerns about privacy involved Facebook's tracking tool, Beacon. Without advance notice to users, Beacon began broadcasting information about users' activities at other websites. Public outcry forced the company to allow users to turn off Beacon. Since then, Facebook has introduced new privacy settings and given users control over others, including the ability to hide friends' lists and lists of interest pages from the public. Recently, Facebook unveiled a new dashboard, which allows mobile phone users to see what information they share and to adjust the settings on the go.

Last year, Google's ill-fated Buzz social network program also encountered a privacy backlash. Outrage among online users was almost immediate. Their concerns included a feature that automatically created circles of friends based on a Buzz user's most frequent contacts on Gmail. This meant that those circles could easily be exposed to others without the user even realizing it.

One user blogged about how Buzz automatically added her abusive ex-boyfriend as a follower and exposed her communications with a current partner to him. Other bloggers suggested that repressive governments in countries such as China or Iran could use Buzz to expose dissidents.

Now, except for a very small group of fanatical users, Buzz is effectively dead. And support for and continued public interest in privacy is very much alive.

In an interview on the program 60 Minutes last year, even Mr. Zuckerberg seemed to move away from the view that privacy is an outdated social norm when he admitted that privacy is among an individual's most important rights.

Businesses and government agencies will strengthen their privacy culture when citizens, customers and regulators push back. And guess what! Paying attention to privacy has been good for business. Having the best privacy controls is now considered a competitive advantage for many Internet-based products and services. Public and private sector organizations must understand that they face a real risk to their reputations – and bottom lines – if they act without ensuring public trust in their actions.

For example, web browsers like Firefox, Microsoft Internet Explorer, Google's Chrome and Opera are all scrambling to outdo the competition with privacy features, including "do-not-track" options. There are now two search engines focused on avoiding tracking – "Ixquick" and "DuckDuckGo." Even if their names could stand a good makeover, the privacy values of these search engines are sound. Privacy controls have become one of the key selling features in a modern web browser. And this development is now extending to a range of other online products and services.

Venture capitalists are also starting to fund consumer privacy tools – for example Reputation Defender, TRUSTe and Abine.

But we must remember Internet providers are interested in making money. And the most valuable thing they have for sale is "you," or at least your online identity and the many items of personal data that define "you" on the Internet. Advertisers pay fortunes for this information, while e-criminals are just happy to steal it.

Privacy remains a fundamental value of Canadians. The Internet has not diminished privacy's importance, nor have the technologies swirling all around us, although they have often made protecting privacy more difficult. If privacy were indeed "on the ropes" as a social norm, we wouldn't see more and more countries adopting privacy laws, including serious proposals for such laws in both Houses of Congress in the United States.

Privacy's value is evident in the vibrant discussion taking place over the December 2010 privacy report of the U.S. Federal Trade Commission. One of the report's recommendations calls for a "do-not-track" mechanism governing the collection of information about consumers' Internet activity for targeted advertisements and other purposes.

Today's privacy dynamic seems to involve a complex and fast-paced evolutionary process. Leading-edge companies offer useful new communication tools that have the potential to breach user privacy. And then the companies are brought back into line by angry users, privacy advocates and government regulators.

The story is far from over. Many challenges remain. And unexpected issues will keep arising as new technologies and innovations hit the market – and users respond to new consumer offerings.

To get better services from companies or from government, we may have to give up some of our privacy. But how much is too much? My concern – shared by many here today – is with the *unintended consequences* of these activities, examples of which abound in our news media. And those are only the ones the public knows about.

Data collection is pervasive and unobserved by most people. This is perhaps the biggest challenge that individuals and regulators face today. As the public becomes increasingly vulnerable to misuse of personal information, whether by internet providers or government, regulators need increased authority and new tools – like meaningful audit tools, proactive investigations and binding guidelines ... tools that enable regulators to ensure that privacy rules are followed!

There is a trend in western democracies towards stronger oversight. For example, Spain has a very strong regime with significant fining power. The UK Information Commissioner's Office has taken steps to put a penalty regime in place for the public sector. New Zealand has binding rules for data-linking by government. And frankly, my

exposure to the federal privacy environment has persuaded me that the federal laws need more teeth. The laws need those teeth where proactive measures and advice and the collaborative approach don't work. Jennifer Stoddart has begun to advocate for order-making power and the authority to name respondents in investigations under PIPEDA.

As the B.C. Commissioner, I have order-making powers, and I do "name names". Having worked under both the ombudsman regime of the federal Office and the order-making regimes in Alberta and B.C., I have concluded that strong oversight is more effective. It helps to ensure that organizations sit up and take notice, and places a greater importance on compliance. For example, earlier this week I released my report into online gaming data security at the B.C. Lottery Corporation.

Some of you may argue that self-regulation is the best way to go and will suggest, for example, that the U.S. Commerce Department's call for self-regulation by Internet companies is appropriate. This approach would leave primary responsibility with companies for protecting personal data in their products and services. But the examples I have mentioned today show that this doesn't always work in the real world. Industries can set standards and introduce guidelines, but co-regulation is necessary.

Although this is an international audience, I would like to focus for a moment on what residents of British Columbia can expect from me on privacy issues in both the public and the private sectors. My approach is to be more proactive, to expend resources on policy work, guidelines, and reviews to ensure that privacy is built into new systems. I have begun this work by closely examining (looking under the hood, as it were) the B.C. government's plans for an identity management system and electronic health systems. I am also reviewing government plans for more horizontal sharing of citizen data across (what have traditionally been) data silos. To support this work, I have reorganized my Office and will soon announce the names of two new Assistant Commissioners; one Assistant Commissioner to lead investigations and the other to lead the team responsible for policy and public education, (functions that staff have been doing off the corners of their desks up to now). I have obtained additional resources which will allow me to secure urgently needed information technology and security expertise and to bolster the capacity of my office in other areas, including consultations and investigations into system-wide problems.

Conclusion

I recognize and support technological innovations that create business efficiencies, enhance citizen-centric services, and introduce cool new ways to communicate and connect. Let me be very clear here, none of these innovations must be allowed to trump the right of individuals to control their personal data. People need full disclosure to make real choices. Powerful social networks and other technologies do not change this fundamental truth.

Citizens and consumers care about their privacy. And it is possible to successfully challenge the potentially intrusive giants of our world, be they government or private sector agencies.

The public may not have the tools to parse every sentence when it comes to understanding the privacy implications of new technologies and new uses of existing technologies. There is a knowledge gap here, and it is our job, as privacy regulators, advocates, and security experts to fill it!

Regulators must cooperate extensively -- nationally and internationally. These problems respect no border.

I hope we use these next few days to work together, learn from each other, and help secure the fundamental human right of privacy in our rapidly changing world.

I wish you all a good conference!