A Report on Privacy Law and Policy Development in the United States

March 2, 2009

Toronto, Ontario, Canada

Remarks of Christopher Wolf, Co-Chair of the Future of Privacy Forum, to the Conference Board of Canada Council of Chief Privacy Officers

Thank you very much for the opportunity to be with you tonight, and for your warm hospitality.

I have been asked to share with you tonight my perspective on the current privacy landscape in the United States, and what we might expect now that we have a new administration and a new Congress. I am of course happy to give you the view from where I sit. Physically, I sit in an office building next to the FBI on Pennsylvania Avenue, half-way between the White House and the Capitol. I also sit as co-chair of the Future of Privacy Forum, a newly-formed think tank with broad industry, government and academic participation. Those two perches, combined, gives me a decent perspective on privacy happenings in Washington.

But frankly, when I heard I would meeting with the premier group of CPOs in Canada, I was hoping I could come up here and take home some privacy and data security advice from each of *you.* After all, you operate in a jurisdiction with far more comprehensive privacy protections than in the US and a much tidier statutory regime. Indeed, my first reaction when given the topic assignment was: "Why would a group of Canadian privacy professionals -- who operate in a jurisdiction that enjoys what we in the States regard as quite comprehensive

regulation of privacy -- want to hear about the patchwork quilt of US privacy laws – with all of its overlaps and gaps?"

Perhaps there is what might be called a "Canadian privacy *schadenfreude."* Maybe you really like hearing about the trials and tribulations of how we in the States struggle to improve privacy. After all, it is not for nothing that the EU deems your legal framework as providing adequate protection for personal data -- in contrast to the work-around Safe Harbor, binding corporate rules or model contract arrangements in the US that allow us barely to pass EU muster.

So, as I asked myself about why there is such an interest here in how we are dealing with privacy and data security, I remembered a remark by your late Prime Minister Pierre Trudeau that I suspect you have heard before. The Prime Minister observed that living next door to the United States was in some ways like sleeping with an elephant. He went on to say that no matter how friendly or even-tempered the beast is, one is affected by every twitch and grunt. Certainly with respect to the privacy of Canadians' data, one twitch – if I can call it that – with which Canada has been concerned of late is the collection and surveillance of data by US officials in a post-9/11-Patriot Act world.

I also realize that another reason that you are concerned with how privacy law protects the personal data of Canadians is that – as I understand it -- in Canada, there are no restrictions on the export of personal information except for personal information that is subject to the Freedom of Information and Protection of Privacy Acts of Alberta, British Columbia and Nova Scotia, and the equivalent in Quebec – laws passed in response to our Patriot Act.

And while there is authority for the application of PIPEDA extraterritorially to those in the US holding personal data of Canadians, the exercise of jurisdiction southward has been limited so far.

So, it turns out, our US privacy laws have a real and immediate impact on data pertaining to Canadians that flow south across the border. To put it simply: Our laws affect the privacy and security of Canadians' data.

And, as your Privacy Commissioner Jennifer Stoddard graciously has explained – quoting now -- "there is no shortage of ideas, and if [privacy professionals] are looking for inspiration, we might want to begin by looking south [to the U.S.]." She probablyw as being overly-kind, but certainly in sheer number, we probably have more privacy professionals thinking about the issues.

In a speech Commission Stoddard gave in Vancouver last Fall where she made that comment, she complimented the efforts in my country at the federal level to put the issue of identity theft into sharp focus by creating an Identity Theft Task Force in 2006. She also praised what she called "some very creative and avant-garde legislative developments in the United States." She was referring to the new laws in Massachusetts and Nevada that will require businesses collecting personal information about state residents to encrypt sensitive data stored on portable devices such as laptops, Blackberries and cell phones. The Massachusetts law requires even more of every business holding data, including a written data security plan and training. Shortly after the Commissioner's speech, it is worth noting that Massachusetts decided to defer until May 2009 the implementation of its encryption law because of the difficulties businesses were facing to be compliant in time for the January 1, 2009 effective date. Just last month, the deadline was extended again, to January 2010 in the wake of broad protests about the compliance burdens. So the Massachusetts law was a good idea, maybe, but one difficult to implement fully.

Commissioner Stoddard also heralded a recently-enacted federal law making it easier for prosecutors to go after cyber crooks, a law that ensures that victims receive compensation when identity thieves are ordered to pay restitution.

Also at the federal level, Commissioner Stoddard praised our new "Red Flags" Rules – requirements for financial institutions and other creditors such as automobile dealers and utility and telecommunications companies to adopt written identity theft prevention policies. These new requirements are called "Red Flag Rules" because organizations are required to set up programs to identify and respond to patterns of behavior, practices or specific activities – red flags – that may indicate identity theft. Unfortunately, as with the Massachusetts law, the compliance deadline of last November was seen as too aggressive because businesses were having difficulty complying in time, so for some businesses under the jurisdiction of our Federal Trade Commission, the deadline has been pushed back to May 1, 2009. A small plug here: I am the co-author of a Practising Law Institute guide to the Red Flags rules, but no I am not selling them in the lobby!

Commissioner Stoddard also went out her way to praise our data security breach notification laws, which requires businesses and government to notify individuals if their personal data appears to have been acquired or exposed to unauthorized persons (such as through a lost laptop, missing back-up tapes, or hacking intrusion). While the concept of these laws is sound – to enable people to protect themselves against identity theft, I have to tell you as someone who helps clients comply, the fact that there are now more than 45 separate data security breach notification laws with varying and sometimes conflicting requirements, makes compliance a challenge. So, while the concept of notification is sound, a uniform requirement is clearly called for.

So, we appreciate the "shout outs" Commissioner Stoddard has been sending our way with respect to some of our newer privacy laws, but the situation remains that in the US, most of our privacy laws and regulations are geographic, sectoral and/or reactive, and not part of a coherent arrangement here in Canada – or what seems to be a coherent arrangement to this US citizen.

I will save for another day a discussion of whether our First Amendment to the US Constitution guaranteeing free speech has a chastening effect on the regulation of the use of data in our country but not in yours, but that may account for the differing approaches of neighbors so connected geographically and culturally. I will note briefly that I was on a panel with our Supreme Court Justice Scalia on Global Privacy Day at the end of January, and it is his view that the First Amendment trumps privacy in most commercial cases. (On the other hand, he views our Fourth Amendment as placing significant limits on government access to private information.)

Now, as to the future of privacy in the US. Our new President polled strongly on the campaign trail as the candidate most likely to advance individual privacy rights, and although – understandably -- the principal attention in Washington thus far has been on the financial crisis, we already have seen a major privacy and data security development in the fiscal stimulus bill passed last month. The economic stimulus legislation that President Obama signed into law last week makes sweeping changes to the Health Insurance Privacy and Portability Act, or HIPAA. The American Recovery and Reinvestment Act of 2009 adds a first-ever statutory data security breach notification requirement to HIPAA, requiring "covered entities" -- typically employers or insurers that sponsor health plans -- to notify individuals in writing if their personal health information is compromised. The notice must be within 60 days of discovering the privacy

breach. If it involves 500 or more individuals, plan sponsors also must notify the Department of Health and Human Services and "prominent media outlets serving a state or jurisdiction."

When HIPAA was enacted in 1996, it did not require notification of individuals affected by privacy breaches. It only required employers to protect the personal health information. It was up to the employer" to decide whether to notify plan members. While more than 40 states have security breech notification laws, only two—Arkansas and California—govern notification of unauthorized disclosure of personal health information. This first-ever federal statutory notice requirement -- while limited to health information -- may set the precedent leading to other federal notification mandates.

And for the first time, the American Recovery and Reinvestment Act extends *direct* HIPAA enforcement to "business associates," such as benefit consultants, third-party administrators and disease management and wellness program providers. In addition, the legislation gives state attorneys general the authority to bring lawsuits seeking statutory damages and attorneys fees for HIPAA violations on behalf of affected state residents. Previously, the HHS Office of Civil rights handled HIPAA enforcement solely. The provision granting state attorneys general HIPAA enforcement authority almost certainly will lead to increased litigation over violations.

The increased penalties went into effect with the signing of the bill. In 60 days, the HHS secretary is required to issue guidance on what constitutes unsecured health information subject to HIPAA rules. Most of the other provisions take effect a year from the law's February 17 signing.

In other news, last Wednesday, the United States Supreme Court heard arguments in a case that will determine whether immigrants who include identification numbers that are not theirs, but don't intentionally impersonate others, can be subject to harsh criminal immigration punishments under federal law. In *Flores-Figueroa v. United States*, the petitioner challenged his conviction for "aggravated identity theft." Privacy advocates have urged the Justices to protect techniques that allow individuals to safeguard privacy. For example, EPIC explained that the crime of "identity theft" should require an *intent* to impersonate another. The EPIC brief urges the Court to avoid "a precedent that might inadvertently render the use of privacy enhancing pseudonyms, anonymizers, and other techniques for identity management unlawful." Reports of the oral arguments at our Supreme Court suggest that a ruling requiring intent is a likely outcome.

And, of course there was big news in the States concerning Facebook and its attempt to change itsTerms of Service. Facebook announced new Terms of Service on Feb. 4, in which it asserted broad, permanent, and retroactive rights to users' personal information - even after they deleted their accounts. The changes were widely criticized – showing that *someone* is reading the legalese in these policies, and Facebook backed down. And just last week, Facebook announced a new participatory paradigm with respect to prospective changes in policy, in which members will have a say about new or changed provisions in the Facebook privacy policy.

On the enforcement front, Federal regulators proposed last Tuesday to impose more than $12 million in fines on 600 telecoms that failed to file paperwork in 2008 explaining how they protect their customers' private information. The issue concerned annual reports that phone companies, internet telephony concerns, and calling-card companies need to file explaining how they protect individuals' phone records, cell-phone location data and personal information from

data brokers and over-the-line private investigators. The Federal Communications Commission tightened the privacy requirements and expanded the number of companies covered in 2007, but many companies seem to have failed to get the memo or take it seriously. That's why the agency is proposing such widespread and news-making fines.

As to other changes we might expect to see down the road in Washington, I have no better crystal ball than any other Washingtonian, but I have tried to keep my ear to the ground on the future of privacy and so, here are some of my thoughts about what we may see in the next four years:

Internet Safety Act: US Senator Jon Cornyn and Representative Lamar Smith have introduced a bill that would require almost everyone who provides Internet access to retain all records for two years. Right now, that includes big Internet service providers (ISPs) such as Verizon or Comcast. Some also believe that the law may be so broad that the coffee shop that offers free wireless access, or even me if I have an Internet router set up at home that is accessed by several people, may be covered. Another section of the bill says that anyone who "knowingly engages in any conduct the provider knows or has reason to believe facilitates access to, or the possession of, child pornography" can be tried under the law. More than a few ISPs worry that this broad wording includes the mere act of providing services such as e-mail might "facilitate access" to illegal material. Opponents of the bill are calling it a very large invasion of privacy and certainly it runs counter to the trend of ISPs and others to reduce the period of time that data is kept. We need to understand that the legislation may be a reaction to several setbacks suffered by those in favor of more control over the Internet, such as the 10-year demise of the Child Online Protection Act (COPA), which ended this past January in the Supreme Court. Odds are that the legislation will not be passed.

Behavioral Advertising: Behavioral advertising -- the practice of tracking of an Internet user's activities online in order to deliver advertising targeted to an individual consumer's interests -- which Congress examined extensively over the summer -- should continue to generate interest. On February 12th, the Federal Trade Commission, the leading government regulatory agency dealing with privacy, said that it will continue to push for better *self*-regulation of online behavioral advertising. But it did so in a manner that suggested that if industry does not implement some basic protections of consumers voluntarily, then regulation could well follow. After considering public comments over the past two months, the FTC released a revised set of four principles to guide self-regulation of online targeted ads.

They are:

• First: Web sites should prominently note their behavioral advertising practices and give consumers an accessible way to opt out of such programs. Companies are encouraged to make these notifications separate from general privacy policies. Companies that collect information through mobile devices or other means should ensure they have sufficient disclosure mechanisms.

• Second: Companies are encouraged to maintain reasonable security and retention practices with respect to the data they collect.

• Third: Companies are also encouraged to inform consumers of *retroactive material* changes to their data collection policies.

• And fourth: Companies are encouraged to receive express consent from consumers before collecting "sensitive data," such as information about children, health information, and Social

Security numbers. The revised principles were issued with a report that responds to comments the agency received on the topic. The commission voted 4 to 0 to approve the Report, but two commissioners suggested the issue is far from resolved, as I indicated. Commissioner Jon Leibowitz – who many believe will be tapped to be FTC Chair said "Industry needs to do a better job of meaningful, rigorous self-regulation, or it will certainly invite legislation by Congress and a more regulatory approach by our commission," "Put simply, this could be the last clear chance to show that self-regulation can--and will--effectively protect consumers' privacy in a dynamic online marketplace." Still, despite this last clear chance at the *federal* level for self-regulation, we are likely to see behavioral advertising legislative proposals at the state level, with efforts gaining traction in states like New York, where both Houses are now controlled by the Democrats. As with data security breach legislation at the state level, regulation state-by-state would, in my view, be a disaster.

Data Breach Notification: As I mentioned, over the past few years, states have been very active passing legislation that requires businesses that retain information about state residents to notify such residents when that information is compromised. Efforts to pass a preemptive national law have stalled largely because of the greater discretion proposed for business regarding the need to notify. In other words, consumer groups have balked at the notion that the threshold for notification should be as high as business has proposed. That issue will likely continue to impede consensus on a national law, and the state framework is likely to be with us for a while. However, as I mentioned, with notification now required with respect to health records, the way has been paved for sectoral notification requirements.

Legislative activity at the state level concerning the protection of personal information, however, is likely to continue as lawmakers try to respond to several high profile information

security breaches from previous years. Moreover, as we are seeing in Massachusetts, Nevada, Connecticut and elsewhere where new data security laws have been passed, we may see a stronger push at the state level toward requiring affirmative steps to protect personal information, rather than just requiring businesses to respond to a breach incident.

National Privacy Law: Major players in the online marketing sphere, such as Microsoft and Google, have historically expressed support for a generally-applicable privacy law to preempt a growing number of state laws that impose varying requirements on the collection, use, storage and disclosure of personal information. Whether a federal law emerges governing the collection and use of personal data, including for marketing purposes, is a looming question in the new administration. But given the difficulties of finding a consensus when smaller privacy proposals have been brought to the Congress, it is unlikely that we will see anything like PIPEDA very soon.

More Robust Federal Trade Commission: President-elect Obama plans to enlarge the FTC budget and enforcement power to aid in the implementation of his technology and innovation policies. The FTC's expanded powers will likely be used to enforce the Commission's new identity theft Red Flags Rule, when they go into effect in May. The push for more enforcement power may also spur the expansion of the FTC's authority to seek civil penalties and other monetary remedies for violations of the statutes and regulations the Commission enforces. And as I just discussed, the FTC is poised to become more involved in the regulation of behavioral targeting if industry self-regulation is ineffective.

* * *

I'd like to turn now from a report on what is likely to happen to a wish list from the perspective of the new privacy think tank that I co-chair, the Future of Privacy Forum. In November of last year, I helped launch the Future of Privacy Forum. Let me tell you what the Future of Privacy Forum is *not*. We are not a lobbying group. And we are not an industry standards-setting organization. Nor are we a group, like some, that criticizes all instances of data collection and use by government or industry. What we *are* is a place where representatives of industry, academia, public interest groups and government can come together to discuss the state of modern privacy and can share best practices in data management, technology and yes, regulation where it is needed. We recognize the value in society and in commerce of personal data, both to businesses and, yes, to individuals. Indeed, we believe that businesses can achieve greater benefits from the use of technology if consumers are better informed and have more control. In other words, our goal is to advocate for advances in privacy that promote greater transparency and more meaningful user control but in ways that recognize the needs of and practicalities of business.

I am so pleased that leaders in privacy have agreed to serve on the Advisory Board of the Future of Privacy Forum, including the Chief Privacy Officers of AT&T, Microsoft, LexisNexis, MetLife, Intel, Facebook, General Electric, IBM, and WalMart, among others.

I should add that probably my greatest contribution to the Forum was my recruitment of Jules Polonetsky, who has served as Chief Privacy Officer of AOL and Doubleclick, as well as Consumer Affairs Commissioner of New York City, to be the day-to-day Director of the Forum and my co-chair.

An example of our work is a program we held last week in Washington at the George Washington University School of Law entitled "Behavioral Advertising: Exploring

Opportunities to Increase Transparency and Consumer Control". The program was a half-day workshop, held in the wake of the recently released FTC principles, focused on behavioral advertising practices, and we had a wonderful exchange of ideas and best practices from industry leaders, with input from government regulators, academics and public interest group advocates. That's the kind of gathering we hope to repeat with some regularity. In addition, we will be participating in privacy events around North American and abroad. And you can expect to see White Papers and regular blog entries from us.

So, at the Future of Privacy Forum, we have put on our thinking cap, and have come up with the following Consumer Privacy Agenda for the New Administration and Congress:

We Believe that the President Should Appoint a Chief Privacy Officer to Promote Fair Information Practices in the Public and Private Sectors.

We embrace the idea of government catching up to industry by creating the central role of a Chief Technology Officer, as has been announced. But we also point out the need — recognized by hundreds of privacy-sensitive companies — for a senior level Chief Privacy Officer, someone to ensure that data protection is a central consideration for technology, data and policy decisions.

Although many federal agencies have privacy officers, the fact that data is increasingly available across government entities demonstrates the need for a central figure to lead U.S. efforts to respect citizen data. To ensure that the data needed to combat terror will be available while appropriate oversight is in place to protect essential freedoms, the Administration should have an accountable, executive-level figure to drive an agenda based on responsible data practices. And as behavioral targeting, correlation of data across platforms, cloud computing and

the use of personal health records becomes widespread in the business world, the need for a senior figure who can drive a consumer-centric agenda based on Fair Information Practices becomes increasingly crucial.

As data flows have already become a global issue, an empowered central address for U.S. data protection will also more effectively allow the U.S. to engage with data authorities around the world.

We Urge Policies that Ensure that Interactive Tools used by Government Provide Users with Enhanced Transparency and Controls.

As I mentioned, federal policy today requires that government Web sites refrain from using persistent cookies without agency head approval. As a result, government sites either go without the benefit of data-driven services that could optimize their usage and performance, or simply obtain agency approval and make use of such cookies without additional safeguards. At a time when citizens expect a widely expanded form of e-government, including social media and commercial Web 2.0 tools, refraining from the use of innovative tools is not an option. But also unacceptable would be simply using the tools that are available on the market today, without enhanced responsible data use rules.

We think that the OMB and the E-Government Administrator should establish baseline principles for cookies, social media tools and other information use by commercial vendors for government. In doing so, they will drive responsible development of these tools for government and for industry. For example, analytics tools should be required to delete log-files after a defined period of time, cookies should have limited expiration periods and should not be used to

store information unprotected, IP addresses should be obscured as soon as possible, and the use of the tools and user options should be transparent and prominently explained.

In addition, a very limited amount of funding for basic research could challenge our best and brightest researchers to create completely new technologies that would deliver the benefit of current day cookies while also increasing transparency and truly protecting privacy.

The Federal government can lead the way in driving companies to provide consumer-centric services that provide users control over data.

We propose modeling a set of requirements similar to the concept of Section 508 of the Rehabilitation Act, which requires federal agencies to make their electronic and information technology accessible to people with disabilities. Section 508 was enacted to eliminate barriers in information technology, to make available new opportunities for people with disabilities and to encourage development of technologies that will help achieve these goals.

We live today in a society where the public has different abilities with regard to managing data collection. As our government Web sites become increasingly interactive, the federal government should require that federally-supported agencies and grantees drive requirements to provide users with enhanced transparency and controls.

We Think It is Time to Establish a Standard Definition of Personal Information.

Most privacy commitments today rely on a definition of personal information, but with the exception of a few statutes such as HIPPA and Gramm Leach Bliley, the interpretations of

what constitutes personal information are wide ranging. Companies rely on a myriad of methods, from encryption to simple encoding to use purportedly non-personal information to aggregate, track, and target robust amounts and types of on- and off-line data. The National Institute of Standards and Technology should work with the FTC and the proposed Chief Privacy Officer to establish standards for levels of anonymity and identifiability.

We Believe in Increased Technology and Research Support for the Federal Trade Commission.

The FTC must become a technology leader to further increase its effectiveness in understanding and countering increasingly complex threats to individual privacy. It should have a significantly expanded team of technologists and an enhanced operations center to track and respond to abuses. The FTC should be provided with authority and funding for Centers of Excellence that can lead research into how to communicate about privacy to users. It should also develop a deeper liaison relationship with the academic and security research communities so that it can both respond to new concerns and help guide external efforts on the type of research that is of value to Commission staff. The FTC should also develop a major effort to evaluate and promote the use of Privacy Enabling Technologies (PETS) that can be used to mask personal information while allowing for robust information use in commerce and analysis.

We Also Believe in Enhanced Criminal Law Enforcement Support for the Federal Trade Commission.

The FBI and DOJ must allocate their limited resources to combat terror and prosecute child predators, and are currently unable to adequately attend to the increasingly dangerous criminals involved in spam, spyware, phishing, identity theft and malware. Appropriate global

criminal law enforcement support must be dedicated to support the efforts of the FTC so that it can use its expertise to ensure full prosecution of those responsible for these threats to user data.

Although there has been increased cooperation between criminal law agencies and the FTC in recent years, dedicated support would ensure that serious harms uncovered by the FTC would lead to a significant threat of criminal charges, as opposed to only civil action.

We Encourage Accountable Business Models

The Internet has led to the development of highly-efficient business models, by which companies collaborate and combine their individual expertise to provide a customer service. A user, by requesting one Web page, can share data with dozens of companies – a Web publisher, an ad network, an ad exchange, a search engine, an analytics company, a content distribution network, multiple advertisers and more. Despite the fact that consumers may believe the brand they are visiting is responsible for the data activity on the page, the complexity, lack of transparency and, sometimes, bargaining power imbalance has created a situation where data flows are dispersed and responsibility is often unclear. The DOC should partner with the FTC and industry groups to address this problem and identify steps that may foster accountable online business models.

* * * *

Having provided you with a little insight into what is on the minds of privacy professionals in the US in terms of what the future may and should hold, I probably should stop here. Let me again thank you for having me speak to you, and for your hospitality. And I would be happy to take any questions you may have.