# Federal Trade Commission

**Office of Privacy Commissioner of Canada Roundtable**

**Toronto, Canada**

**Remarks of David C. Vladeck[1]**
**Director, FTC Bureau of Consumer Protection**

**April 29, 2010**

Good morning. I am delighted to be here in Toronto. First, let me thank Commissioner Stoddart and Liz Denham for thinking that I might have a contribution to this important privacy consultation that the Privacy Commissioner's Office is conducting. I hope I won't disappoint. I saw the Commissioner last week at IAPP where a number of different discussions took place on a way forward on privacy. It's not an easy task to embark on a consultation. Logistics aside, it is challenging to identify the key issues at stake and to frame the discussions on how to address those issues and explore them. The agenda today is an exciting one and I look forward to the dialogue on these issues that the FTC is also tracking – not in any surreptitious way – quite closely.

What I'd like to do this morning is talk to you about the FTC's privacy consultation - where we are in the process and where we are going. But, first a bit of background about why

[1] The views expressed here are my own and do not necessarily represent the views of the Federal Trade Commission or any Commissioner.

we saw the need to even go down this challenging but exciting road.

We have learned that existing privacy frameworks have limitations. The notice and choice model puts the burden on the consumer to read and understand lengthy, complicated privacy policies. The harm-based model recognizes only a narrow set of harms, but, privacy is an important value in itself. A recent FTC enforcement action demonstrates the limitations of these models. This action involved a major American department store chain. The company failed to disclose adequately the scope of personal information it collected from consumers via a downloadable software application. According to the FTC's complaint, the company paid $10 to consumers who visited the company's websites and agreed to download "research" software that the company said would confidentially track their "online browsing."[2] In fact, the software collected vast amounts of information, including the contents of consumers' shopping carts, online bank statements, drug prescription records, video rental records, passwords, and library borrowing histories. Only in a lengthy user license agreement, available to consumers at the end of a multi-step registration process, did the company disclose the extent of the information the software tracked. The settlement calls for the company to stop collecting data from the consumers who downloaded the software, to destroy all data it had previously collected, and not to engage in similar conduct in the future. This case tells us that meaningful consent is challenging today and we need to think about how transparency can be achieved.

Just a few weeks ago, it was reported that approximately 7,500 consumers had "sold their souls" to an online computer game retailer. To make the point that consumers simply don't read disclosures when shopping online, the company included a clause in their terms of use that by

[2] *Sears Holdings Mgmt. Corp.*, FTC File No. 082-3099 (final order Aug. 31, 2009).

placing an online order on the Website, consumers were granting the company "a non transferable option to claim, for now and for ever more, your immortal soul." In this case, there was even the ability to opt-out of that particular "soul selling" clause, but very few did. Thankfully, the company has stated that it would not be enforcing its ownership rights and planned to email customers nullifying any claim on their soul.[3]

When things work well, you leave them alone and hope they keep on working. That's a pretty good strategy in most areas of life. But when they're no longer working well, you can't ignore it. In the case of privacy frameworks, it became abundantly clear that the old models were simply put, outdated. They just aren't keeping up with the times. This re-examination is centered on a series of three roundtables. The first took place in Washington in December of last year. The second was in Berkeley California in January. The final roundtable took place just a little over a month ago in March back in Washington, DC. We were fortunate that Commissioner Stoddart joined us at the most recent roundtable and participated in one of the sessions.

At the first roundtable, we discussed the wide variety of ways by which consumer information brings benefits – through subsidizing the Internet and more relevant advertising – as well as the risks posed by the possible misuse of that information. We heard experts confirm what we have sensed – that consumers do not really understand data collection and are largely unaware that there may be companies collecting and analyzing their data for other companies to use, particularly for targeted advertising. We discussed in greater detail the collection and use of data in two specific contexts – behavioral advertising and the information broker industry – that

[3] *See* Fox News, *7*,500 Online Shoppers Unknowingly Sold Their Souls (Apr. 15. 2010), www.foxnews.com/scitech/2010/04/15/online-shoppers-unknowingly-sold-souls.

remain highly visible issues in consumer privacy. Finally, we heard discussions about various approaches to managing the privacy and security of consumer information – the fair information principles, the harm-based approach, sector-specific regulation, and self-regulation.

We continued these discussions in January in Berkeley that focused on themes of technology and privacy. We discussed how technology could enhance consumer privacy and how it might challenge or circumvent consumer privacy. We examined these questions specifically in the context of social networking, cloud computing and the mobile environment.

At our third roundtable in March we tackled one of the biggest questions relating to the Internet. Can we build security and privacy into the Internet after the fact? Or is the cat out of the bag? Can we create a secure, authenticated structure on top of the foundation that was built to be trusting and open? We also talked about health-privacy issues which affect each and every consumer. Is there a way to reconcile individual health privacy with important society interests in research, and public health, aiming to improve our collective health? We also addressed the issue of sensitive information. What is sensitive? Is there a consensus on what that really means? Can it be defined objectively or is "sensitive information" purely a subjective construct? Are there policy approaches that would enable people to apply their preferences themselves without the need for some kind of consensus?

Each of these roundtables provided a tremendous amount of food for thought. Our panelists included some of the privacy leaders both in the United States and internationally as well. We have gathered a wealth of collective wisdom to guide us going forward. And I should note that we're not done with our public dialogue on privacy issues - we are also embarking on a review of the Children's Online Privacy Protection Rule. In light of rapidly changing technology such as the increased use of smartphones and other devices to access the Internet, we

are hosting another public roundtable on June 2, 2010 to explore whether to update the rule. The rule was enacted in 2000 and requires Website operators to obtain parental consent before collecting, using, or disclosing personal information from children under 13. Roundtable topics will include whether the rule should be applied to emerging media such as mobile devices, interactive television, and interactive gaming; potential expansion of the rule to cover more items of information that might be collected from children; and a review of the parental verification methods used by Web site operators. These issues will naturally inform our broader consideration of privacy issues developed through our other roundtable events.

And so the real question is what do we do now? Earlier in my remarks this morning, I pointed out that it is no easy task to organize a roundtable discussion and identify the themes and key issues to discuss. Well, truth is, that's a lot easier than what we have to do now. Let me tackle that by first taking about what we want.

1. We want consumers to have greater control, recognizing that they don't want to spend time reviewing a lot of privacy disclosures.
2. We want to distinguish between data uses that truly raise privacy concerns from those that don't. But we also want to recognize that privacy preferences may differ for different people and that it may be difficult to draw the lines.
3. While we want to protect privacy, we don't want to stifle innovation in a marketplace that clearly is using personal data to develop innovative new products and services that many consumers like.
4. We want to accommodate the incredibly diverse business models as well as the privacy concerns that exist today. AND that may be developed tomorrow. Mobile devices,

social networking, online shopping, location based services, etc. etc. etc. Believe me, this is not a comprehensive list.

5. And if you can believe it after all the "WANTS" that I've just talked about, we want a relatively simple framework, so that everyone can understand the norms and expectations.

We don't see this as starting over. But we want to improve on the current privacy models, while building on the progress made under those models and supporting valuable privacy work that is already underway.

Industry has taken some steps in our call for greater transparency, particularly in the behavioral advertising area. But there's a lot more work to do.

Okay, so we know what we want. How do we get there? For now, we are still processing all the input we have received during the roundtable process. Both the discussions as well as the written comments that we collected - we have received more than 100 submissions. We intend to continue the collaborative process we started with these roundtables. We aren't about to launch a new framework on our own that's fully cooked. We'll need to put our thoughts together and put those out for public comment as we often do.

Essentially, what I am telling you is that today is the easy part. I do recognize that it's a lot of work putting these events together. I know and I thank the great FTC staff for pulling off three of them. But it's what you do tomorrow that's really hard. But, the good news is that neither of us is alone. We should take advantage of one another and share what we have learned. I look forward to working with the Office of the Privacy Commissioner in the future, as we have in the past, to tackle these tough but important issues. And we are not the only ones. A similar consultation is taking place in Europe on their privacy framework, and we are fortunate that an

official from the European Commission participated in one of our roundtables. None of us operates in a vacuum and we continue to identify ways to work together.

I do want to just clarify something about the privacy work at the FTC. While this re-examination is one of our top priorities, I don't want to give the impression that we are doing nothing else. We are still engaging in our core business, so to speak, and that is enforcement.

We recently announced a case involving a company's false claims relating to identity theft prevention and data security. The FTC's complaint in this case, involving a company called Lifelock, charged that the company used false claims to promote its identity theft protection services, which it widely advertised by displaying the CEO's Social Security number on the side of a truck.[4] This enforcement action was coordinated with the attorneys general in 35 of the United States and is one of the largest FTC-state coordinated settlements on record. According to the FTC complaint, the company made this statement as well as others: "LifeLock protects against this ever happening to you. Guaranteed." Our complaint, among other things, charged that these claims were false, given that the services provided did not provide absolute protection. Further, the complaint alleged that the company made deceptive claims about its own data security practices. In fact, the company's data system was vulnerable and could have been exploited by those seeking access to customer information. The settlements reached with the FTC and the states attorneys general bar deceptive claims and require LifeLock to establish a comprehensive data security program and obtain biennial independent third-party assessments of that program for twenty years. And, they must hand over $12 million dollars. $11 million to the FTC and $1 million to the states. The FTC will use the $11 million it receives from the settlements to provide refunds to consumers.

[4] *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-NVW (D. Ariz., final order Mar. 15, 2010).

Another recent case recently settled involves a company that consumers relied on to certify the privacy and security of online retailers and other Web sites. In this case, the FTC alleges that the company misled consumers about how often it monitored the sites and the steps it took to verify their privacy and security practices.[5] The company, the third-party privacy and security certification program, ControlScan, provided a "seal" to convey that an independent party is auditing the practices of the site regularly to be sure that the data is has collected is not vulnerable. In this case, we alleged that ControlScan provided these seals to Web sites with "little or no verification" of their security or privacy protections. The FTC complaint alleges that the company engaged in deceptive business practices that violated the FTC Act. The settlement with this company bars future misrepresentations and included a monetary judgment.

But that's not all. We are currently examining practices that undermine the effectiveness of tools consumers can use to opt out of behavioral advertising, and we hope to announce law enforcement actions in this area later this year.

Finally, I'd like to add how much we value our relationships with our international colleagues. I had the pleasure of first meeting Commissioner Stoddart in Madrid last November at an international privacy conference, and the FTC and the Office of the Privacy Commissioner have a very strong productive relationship and I know that will continue to grow. We value collaboration on policy issues, as well as enforcement. Both our offices were instrumental in launching the newly formed Global Privacy Enforcement Network (GPEN) that we hope will foster greater cooperation in the enforcement of privacy laws. We only expect the network to grow from its original 11 members. In addition, within APEC, the Asia Pacific Economic

[5] *FTC v. Control Scan, Inc.*, (N.D. Ga., final order Feb. 25, 2009).

Cooperation forum, both of our offices have been involved in the development of the arrangement to facilitate enforcement cooperation among APEC member economies. These projects are very important. We can do more than one thing at a time. While evaluating and thinking about privacy and its regulatory frameworks, we can still enforce, and cooperation is essential.

We have a great agenda ahead of us today, so I will end here. Again, thank you for inviting me today and I appreciate your interest in the work we are doing.