NYMITY

Privacy Interviews with Experts
April 2011

Toronto / Washington DC / Brussels
www.nymity.com

Tanya Forsheit
Founding Partner
InfoLawGroup

David Navetta
Founding Partner
InfoLawGroup

Scott Blackmer
Founding Partner
InfoLawGroup

The Commercial Privacy Bill of Rights Act of 2011: It's Here! What Might It Mean For Industry?

Senator John Kerry (D-MA) has been circulating various draft versions of his bill for weeks now, providing an opportunity for many groups to review and comment. The bill has now been officially introduced by John Kerry (D-MA) and John McCain (R-AZ).

Tanya Fosheit, David Navetta and Scott Blackmer, founding partners of InfoLawGroup provide us with not only an excellent summary of its current content, but also highlight some of the key challenges industry will face given the draft remains as written. They also share a perspective about its way forward in the coming weeks.

Tanya L. Forsheit is one of the Founding Partners of InfoLawGroup LLP. Tanya founded InfoLawGroup in 2009 after 12 years as a litigator and privacy/data security counselor at Proskauer where, most recently, she was Co-Chair of the firm's Privacy and Data Security practice group. In 2009, Tanya was named one of the Los Angeles Daily Journal's Top 100 women litigators in California. Tanya is President-Elect of the Women Lawyers Association of Los Angeles and is a Trustee of the Los Angeles County Bar Association.

David Navetta is a Founding Partner of the Information Law Group. David focuses on technology, privacy, information security and intellectual property law. He is also a Certified Information Privacy Professional through the International Association of Privacy Professionals. David has enjoyed a wide variety of legal experiences, including work at a large international law firm, in-house experience at a multinational financial institution, and an entrepreneurial endeavor running his own law firm. David currently serves as a Co-Chair of the American Bar Association's Information Security Committee

Scott Blackmer is a Founding Partner of InfoLawGroup LLP. He has practiced IT law since 1982 in Washington DC, Brussels, and Salt Lake. Scott advises global companies, start-ups, nonprofits, and government agencies on information privacy and security issues in cross-border operations, outsourcing, and online transactions.

Nymity: What are the key obligations in the draft Commercial Bill of Rights Act of 2011?

David: The draft bill gives the FTC significant authority to create rules as to how businesses collect, use, transfer and maintain personal information. The bill envisions transparency and accountability, obligating businesses to be up front with consumers about how they handle personal information and requiring businesses to establish reasonable data security measures. The definitions of the information protected under the bill are broad, which gives the FTC flexibility to construct a list of more specific categories of information and requisite levels of protection required for each category.

The bill emphasizes the importance of giving individuals notice as to how their information is collected and used. Companies are required to tell people what information they collect and how that information is going to be used. Companies aren't allowed to collect whatever information they like – they are required to minimize the amount of personal information collected. When information is obtained or used in certain ways, companies are required to give people the choice to opt-in or opt-out of those

practices. Also, individuals will have the right to access the information that companies collect about them and correct inaccuracies. The bill gives the FTC authority to craft rules as to how notice should be given and how companies should obtain consumer consent with respect to the collection and use of their personal information. Last, but certainly not least, the bill also creates substantial obligations for companies that transfer personal information to other entities.

Nymity: Given the summary of the obligations above, which do you see as the most impactful to industry and why? Which industries or businesses will face the most change and why? Given it takes time within most companies to effect change or to retrofit systems and business processes, are there elements of this bill that you might suggest that companies begin to think seriously about integrating into their future plans for change if they are not already doing so?

Tanya: The obligations on companies that transfer personal information to other companies may significantly impact the way companies handle information. First, the bill requires that individuals be given notice if a company handling their personal information wants to transfer the information to other entities. Companies will need to clearly explain how their business structure may involve the transfer of personal information to other entities, identify the entities that may receive information via transfer, the purpose for transferring information, and the way any transferred information will be used. Companies will likely need to create website policies explaining these concepts to provide individuals with sufficient notice as to their information practices. The may need to overhaul their existing policies to ensure their notices are clear, comprehensive, accurate and address the requirements of the bill.

Scott: In addition, the bill will dictate how organizations select parties who they transfer personal information to, and will impact the contracts between those parties. When a company transfers information to another entity, the bill requires the transferring company to enter into a contract with the entity receiving the information. Before contracting with another entity for information transfers, the bill requires a company to conduct a thorough investigation to ensure that the receiving entity is legitimate and will properly safeguard any information it receives. A contract for the transfer of information must spell out how the entity receiving information will use and protect the information. The contract must also prohibit the receiving entity from combining any non-personally identifiable information it receives with other information in order to identify specific individuals.

As the bill prohibits companies from transferring information to entities that may violate the contract or have violated the contract, this puts a substantial burden on businesses that transfer information to sufficiently investigate any companies that will receive information via transfer. This means understanding not only how entities receiving personal information plan to use the information, but also how they safeguard information in order to protect it from unauthorized use by others. Businesses will have to fully investigate the possible ways information may be transferred to other entities, who those entities are, and how those entities handle personal information. The duty is on companies covered by the bill to employ knowledgeable staff that can implement internal procedures to control the transfer of information and evaluate the data use and security practices of all receiving entities.

David: To achieve everything mentioned by Scott and Tanya, companies obligated to comply with these provisions may need to undergo substantial structural changes in order to ensure compliance with the bill's requirements. Internet firms and the online advertising industry may face the most change, as the bill could impact internet firms' advertising-driven business models which often rely on online tracking and targeted ads to maximize revenues. Online advertising firms may have to change their information practices completely in order to continue doing business with other companies obligated to comply with the bill's provisions.

With FTC privacy enforcement already on the rise, companies are well advised to take proactive approach to compliance with privacy and information security laws, regulations, guidelines and best practices. The FTC expects companies to collect, use, disclose and process personal information in a fair and transparent way, and to accurately represent their privacy and security practices to consumers. The bill incorporates elements of the FTC's "privacy by design" approach, requiring companies to implement comprehensive information privacy programs designed to safeguard personal information throughout the data life cycle. Companies should look to the FTC and DOC's Fair Information Practice Principles and consider how they business can apply the principles to personal information practices. Additionally, companies should conduct thorough due diligence before transferring data in order to understand the procedures receiving companies have in place to safeguard information, why those companies are receiving information, and how those companies use the information they receive.

Nymity: Given the summary of the obligations above, which do you see as the most impactful to individuals and why?

Tanya: The bill stresses the importance of consumer choice as to how their information is collected, used, stored, and transferred, and is based on the idea that individuals have a significant interest in their personal information, and should be given options to control the flow of their information.

Although most companies already disclose their data practices on some level, the bill ***requires*** companies to be explicit about the information they collect. The bill gives individuals the right to access their information and correct inaccuracies. And while some companies obtain consumer consent to data practices using opt-in or opt-out mechanisms, the bill ***requires*** companies to give individuals the right to opt out when their information is used in an unauthorized way and opt-in consent is inapplicable. In its current form, the bill requires companies to obtain explicit opt-in consent before collecting, using, or transferring "sensitive" data, defined expansively as personally identifiable information that if lost, compromised or disclosed without authorization poses a significant risk of economic or physical harm, or information related to a person's medical condition, health record, or religious affiliation.

. Under the bill, individuals are given more detailed notice about the information companies collect about them, and are given the choice to avoid data practices with which they do not agree.

Notably, there is no private right of action under the bill – the FTC and state attorneys general will enforce it, and companies that violate their obligations can face fines up to $3 million dollars. However, companies must establish a process for being responsive to complaints from individuals regarding how their personal information is handled.

Nymity: Given the summary of the obligations above, which do you see as the most impactful to the US FTC and DOC agendas, as represented in their recent papers and why? What do you see as the way forward for this bill, especially given the current focus on economic recovery?

David: The FTC has declined to take a stand as to whether Congress should enact privacy legislation such as this bill. Interestingly, the bill does not explicitly address the well-known "Do Not Track" mechanisms that the FTC has recently discussed. Creating and enforcing specific rules under the bill stands in stark contrast to the FTC's general deference to industry self-regulation. This is not to say that the FTC will not continue to advocate that businesses incorporate "Do Not Track" if this bill (or one similar to it) is enacted requiring the FTC to promulgate rules. As the bill tasks the FTC with promulgating and rules and enforcing the bill's provisions, the FTC may incorporate ideas stemming from its policies of self-regulation into the formal rules it creates. Under the bill's framework, the FTC can also take into account the positions of government agencies and other stakeholders to develop enforceable best practices or codes of conduct based on the bill's baseline principles without the need for additional legislation.

In December, the DOC released a "Green Paper" on consumer data privacy encouraging the adoption of "fair information practice principles." These principles included transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing. The DOC has since thrown itself behind the enactment of legislation that provides baseline consumer data privacy protections and gives the FTC the authority to enforce those protections. This bill may draw support from the DOC as it addresses all of the DOC's fair information practice principles and gives the FTC the authority the DOC believes is necessary to provide a stronger statutory framework to protect consumer privacy interests. While one of the DOC's concerns in backing a privacy bill was that legislation could prove to be too inflexible to address changing markets, the bill provides the FTC with the authority to offer a safe harbor for companies that implement codes of conduct that are consistent with the bill's baseline protections. This provision may influence the DOC to conclude that the bill provides a framework that is sufficiently flexible to address such concerns.

Tanya: It is important to note that while there are legitimate concerns that privacy legislation may lead to reductions in business revenues and stifle innovation, most of the proposals on the table seek to strike a balance between business needs and privacy concerns. The stated aim of the Kerry bill is to enhance individual privacy protections as a way to stimulate commerce by instilling greater consumer confidence. The bill establishes a framework that can address specific privacy issues as they emerge. By granting the FTC rulemaking authority, the bill allows for considerable input from other agencies as well as commercial entities in crafting

specific rules that will not unduly stifle economic interests. Additionally, making the U.S. privacy and data security framework more interoperable with international frameworks could benefit companies by reducing their compliance burdens overseas.

Nymity: Given the summary of the obligations above, which do you see as the most impactful to the EU agendas, as represented in their recent papers/speeches regarding the Data Protection Directive/Retention Directive/eCommerce Directive and why?

Scott: The bill's incorporation of baseline privacy protections holds the promise of making the U.S. consumer data privacy framework more interoperable with international frameworks. The bill's incorporation of fair information practice principles may address some international concerns that current U.S. privacy and data security laws do not sufficiently protect consumer privacy as a fundamental value.

More importantly, the bill's deference to the FTC to enforce the bill's provisions through rulemakings will allow stakeholders to help shape enforcement of the bill's baseline privacy and data security requirements in the U.S. Giving the FTC the authority to create and enforce the rules may help reduce barriers to cross-border data flow by increasing the global interoperability of privacy frameworks. While the privacy laws across the globe have substantive differences, these laws are frequently based on similar fundamental values, and the bill gives the FTC an opportunity to promulgate rules based on these similar values.

Nymity: In closing, what have we not asked that would be meaningful for our readers to know about?

Tanya: Many agree that a fundamental problem with the current state of privacy and data security practices is that many Americans don't fully understand and appreciate what information is being collected about them, and how they are able to stop certain practices from taking place. Even if nothing further happens with this bill, some companies are incorporating privacy protections in their business models in response to the surging demand for online privacy protections. For example, Mozilla added a do-not-track tool to an upcoming version of its Firefox browser. Microsoft likewise added a "Do Not Track" header and other support in its new Internet Explorer 9 browser.

Dave: I would also add that companies need to be aware of the actions taken by states on the data privacy and security front. Fifteen state attorneys general have officially supported the continued protection of consumer privacy. While the draft bill calls for preemption of state privacy and data security, except those dealing with health or financial information, data breach notification, or other state laws to the extent those laws relate to acts of fraud, some state attorneys general are opposed to federal preemption. Companies must prepare themselves for the possibility that, absent a federal bill preempting state laws, some states may enact privacy and data security laws obligating companies to reform their information practices. I would also advise companies to monitor privacy-based litigation, as the plaintiff's bar has the potential to materially impact privacy practices and liabilities even in the absence of specific privacy regulations.

Scott: Especially in the current political environment, Congress may be unwilling to give the FTC regulatory carte blanche to the extent contemplated by the bill's authors. But the bill is groundbreaking in approaching the commercial use of personal information across the board rather than in a limited sectoral context such as healthcare or financial services. Combined with some level of preemption of inconsistent state regulation, such legislation at the federal level could deliver more predictability for businesses and consumers alike.