International Business Machines Corporation
600 14th Street, NW, Suite 300
Washington, DC 20005

February 18, 2011

Federal Trade Commission
Office of the Secretary
Room H-113 (Annex)
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Re: FTC Staff Preliminary Report on Protecting Consumer Privacy
File No. P095416

Submitted online via:
https://ftcpublic.commentworks.com/ftc/consumerprivacyreport/

Dear Sirs and Madams:

IBM welcomes the opportunity to comment on the Federal Trade Commission's Staff Report, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers." As a company whose commitment to privacy extends back decades, we applaud the Commission's attention to consumer privacy in the digital era.

Introduction

IBM understands that public trust is essential to the continued health and further development of the Internet and to the realization of the progress that full deployment of information technologies can make possible in areas as disparate as healthcare, commerce, marketing and energy. A contemporary and effective privacy policy framework in the United States can help foster that trust.

At the same time, the digital economy continues to change and grow in ways that outpace prediction. We understand that policymakers, therefore, face a challenge: how to help promote transparency, predictability, and consumer confidence without inadvertently causing damage to the openness and flexibility necessary to foster business confidence and innovation. In that vein, properly calibrated regulatory initiatives, potentially including baseline privacy regulation and voluntary enforceable codes of conduct, can help improve privacy protection for consumers and enhance the confidence of the public

in the digital economy. Several additional areas are promising for public-private collaboration including the development and implementation of the emerging discipline of privacy by design; work to clarify and simplify consumer choice and to promote transparency in data practices; and ongoing work to strengthen consumer awareness.

IBM's Interest

IBM helps organizations become more innovative, efficient and competitive via the application of business insight and advanced information technology solutions including cloud-based solutions and IT services. Approximately 400,000 IBMers worldwide engage with thousands of clients, communities, universities and others to integrate information technology into the key systems that support society: public health, finance, transportation, commerce and food supply chains for example. As a globally integrated enterprise, we must process information across national borders in support of research, technology development and deployment, commerce, HR and other key functions.

The commercial data privacy policy framework thus affects us as a technology and business innovator; a professional services company; a large employer; and a company that must access and use data all over the world.

Internationally, disparate regulatory approaches to cross-border data processing pose a challenge to efficient business operations. We believe that harmonization of data privacy and security policy frameworks in this regard would ease these burdens, directly aiding US business' international competitiveness. In the long run, a more unified U.S. approach to privacy policy would represent a meaningful step toward such international harmonization. However, we should not underestimate the importance of getting this approach "right," as inappropriate regulation could do considerable damage to existing and emerging business models.

Comments

Against this background, IBM offers the following observations on possible approaches to a contemporary US commercial privacy policy framework.

1. **The source, scope and enforcement of any commercial data privacy framework should be technology-neutral and calibrated to protect consumers while avoiding undue burdens to business.**

IBM generally supports the principles of the proposed framework: privacy by design, simplified consumer choice, and greater transparency as to commercial data practices. The proper application of these principles, like fair information practice principles

generally, will depend on context, data elements, and other factors.[1] If this privacy framework is formalized via federal policy, at minimum it should:

- **Remain technology-neutral**, but should create incentives for businesses to create and use privacy-protective technologies, such as encryption, data masking and the like. By avoiding technical mandates and leaving more specific, tailored requirements to voluntary enforceable codes, a new federal privacy framework will maintain its relevance through years of technological change. At this phase of market development, moreover, specific requirements are premature: they may well founder in the absence of public and industry consensus in this area, and could forestall development of options that might ultimately be more useful.

- **Make compliance reasonably achievable** and provide businesses with flexibility to handle data in ways that make sense for their own businesses. For example, the scope proposed in the Staff Report ("all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device") threatens to be unworkably broad. It requires difficult judgment calls that may change over time, as technologies develop. Additionally, data retention periods should not be rigid or across-the-board; acceptable ranges should reflect business realities such as length of useful life.

- **Offer clear safe harbors** for businesses that handle data responsibly, including those who adhere to voluntary enforceable codes. Voluntary enforceable codes also offer scope for non-governmental entities, such as those involved in code design, to help industry self-police, as entities like TRUSTe do today.

- **Clearly distinguish between those businesses that control data and those that are service providers**. In the enterprise context, service providers typically implement the decisions of their customers, who maintain ultimate responsibility for determining how their data should be handled. Service providers usually do not have a relationship with the consumer whose information they received from the data controller, and their ability to take action is accordingly limited compared to that of the data controller. For example, a service provider could not independently choose to be responsive to consumer requests for access, because that decision properly belongs to the data controller who has engaged the service provider. And in many instances the data protection approach used is ultimately determined by the data controller.

[1] Expanded Fair Information Practice Principles (FIPPs) have been proposed by the Department of Commerce Green Paper as a basis for a commercial data privacy baseline. While we believe FIPPs are not suitable for direct enforcement by regulatory bodies, voluntary enforceable codes would be an acceptable vehicle for creating workable FIPPs-based solutions tailored for different audiences. The FTC would be able to enforce them against those who have falsely claimed a commitment to abide by them via publication on their websites or elsewhere. Under this approach, the FTC would be able to continue to conduct privacy investigations under its Section 5 authority.

- **Be consistent with cybersecurity objectives.** Cybersecurity initiatives may in some situations be in tension with regulatory efforts to achieve consumer privacy. For example, law enforcement may argue for longer retention periods to retain evidence against wrongdoers, while data privacy advocates argue for shorter retention periods and data minimization. Regulators should make every effort to reconcile these goals: companies should not have to follow one set of data protection principles for a commercial data privacy framework and a different set for cybersecurity.

- **Include a broad preemption provision** to provide certainly and simplicity to businesses within the scope of the framework, while leaving states free to regulate concerns that arise outside it.

- **Provide effective and workable protection.** Effective regulation focuses on real risks to consumers and practical action to avoid and mitigate risk, rather than on theoretical possibilities or technical foot-faults. It establishes goals that industry can meet in evolving and innovative ways, and avoids technical mandates. It also improves compliance by reducing the costs and complexities associated with it.

- **Be enforced exclusively by federal regulators**, rather than state attorneys general or via a private right of action. Federal regulation with preemption could protect consumers as or more effectively than regulation by the states -- while costing business less in time, money and the managerial focus needed to meet multiple state requirements. Whether such efficiency is achieved depends not only on the substantive law, but on the manner of enforcement. Enforcement of a single federal law by a single federal regulator would best assure uniformity of interpretation and application.

2. Government and industry alike should work to develop and launch mechanisms to promote transparency and promote informed choices.

The Internet today can make exercise of informed choice seem like a full-time job; confusing and inconsistent privacy policies are just one example. IBM agrees that much can be done to help consumers understand how data that pertains to them is being handled and to make decisions accordingly. Here are some approaches:

- **Standardized ways to compare privacy policies** should be developed (ideally by multistakeholder groups) and the results of those comparisons communicated to consumers, as the Department suggests. Icons are one promising approach. These icons, however, should clearly convey to consumers not only the risks but the benefits of granting permissions to use data (for example, better-aimed advertising, personalized offerings and improved user experience), and recognize that consumer preferences as to data privacy vary widely.

- **Use restrictions and purpose specifications** can be helpful, but they must be implemented with balance in mind. For example, repeatedly requiring consent for distinct narrow uses would inundate consumers with pointless requests. In this regard, exempting clearly defined "commonly accepted" practices would be useful; if a consumer has placed an order, it should not be necessary to ask permission for the use of data for fulfillment activities. Defining (and refining) those "commonly accepted" practices will be the challenge. "Commonly accepted" practices should be defined to include those things that companies must do to fulfill its transactions, to market to consumers on a first party basis, to comply with legal requirements and to prevent fraud. Further, businesses need continued freedom to understand their data, via analytics or otherwise. The universe of data is expanding to include communications from a wide range of devices, not all of which have directly to do with people (e.g., sensors in infrastructures). Analytics can provide tremendous benefit to society, from curing disease through analysis of patient data to conserving energy through analysis of smart grid data. Thoughtful use of privacy-by-design principles, organizational accountability, and privacy-protective technologies can protect individuals without depriving business and society at large of the insights and progress that analytics offers.[2]

- **Provide effective notice and choice,** especially in areas of particular consumer concern, such as use of sensitive data in marketing and for data practices outside the "commonly accepted" norm. Notice must be clear and choice easy to effect – but no single method of notice and choice will be effective across the board or as new uses emerge. It is entirely feasible for industry and regulators alike to help consumers understand the choices they are making, for example, by moving toward more standard formats and terminology for describing data practices. This can be achieved in a variety of ways depending on context – on data collection forms or via signage for information gathered offline, via a "short form" with a link to a standardized statement suitable for display on a mobile device, and/or via a set of standard icons that consumers could come to recognize.

- **Encourage mechanisms by which consumers can make their choices effective across the board, rather than site-by-site.** The proposed "Do Not Track" mechanism is an example of this approach. However, it is important to note that this issue is far more complex than the "Do Not Call" legislation to which it is so frequently compared. Because of the various Internet entry points an individual may have, through different networks and different devices, any such mechanism would seem to have to be device- or IP-address targeted, not based on the individual. A mechanism of this kind would also have to be accompanied by a clear and balanced explanation of why or why not a consumer might wish to opt

[2] Paul M. Schwartz, *Data Protection Law and the Ethical Use of Analytics,*10 Privacy and Security Law Report 70, Jan. 10, 2011, *available at* http://www.paulschwartz.net/pdf/Schwartz_Analytics_Ethics_BNA_Priv_Sec_Law_2011.pdf. Forthcoming as a White Paper, OECD Working Party on Information Security and Privacy (WPISP).

out. Moreover, many -- if not most -- consumers might prefer something more granular than a simple yes/no option. While the framing of this choice for consumers has received considerable attention, we also point out that such a mechanism could and should frame choices for business in a positive way. Offering one or more choices to consumers that permit data use in ways that are agreed to be responsible while offering an opt-out of uses understood to be more risky would create a powerful incentive for companies to adopt those responsible data practices. It seems premature, however, to require "Do Not Track" legislatively at present, when a clear understanding of what consumers expect, want, and need is only beginning to emerge.

- **Maintain parity among marketing channels.** Rather than restricting first-party marketing to the context in which data was gathered, a federal data privacy framework should aim to support the creation of consistent consumer expectations and competitive equality among marketing channels. For example, if a first-party marketer can contact a customer through a range of channels using information gathered in person, it should be able to do the same for information gathered in an online relationship. Moreover, first-party marketing should be considered to include marketing by affiliates. As one of the world's most recognized and respected brands, IBM believes consumers are, by and large, quite knowledgeable regarding the companies with whom they choose to do business. Where it is or reasonably should be clear to the consumer that a relationship exists between (a) a business with whom the consumer has interacted and (b) a second entity, that second entity should be permitted to engage in marketing to the consumer without the consumer's explicit consent, as long as the practice of sharing of consumer data among business affiliates should be clearly disclosed in the respective privacy policies of the business entities. A more stringent approach to the sharing of consumer data may of course be appropriate for businesses and on-line entities that market to children and for sensitive information**.**

3. Government encouragement of privacy-protective innovation.

While privacy-erosive practices may capture the headlines, responsible companies continue to find new ways protect their customers and manage their own risk by developing and implementing best practices and deploying new technologies. Government can encourage both new developments and more widespread dissemination of approaches in a variety of ways:

- By educating the public on data privacy and security issues. Consumer awareness will create demand for new and better practices and technologies – and will drive broader deployment of those that exist already.

- Government can create strong positive incentives by providing safe harbors for companies that adopt good practices that demonstrate accountability. We note

also that while privacy-protective technologies continue to be developed by IBM[3] and other organizations, incentives for their actual use are particularly important at the deployment stage. That is, those responsible for data practices are more likely to invest in technology-enabled methods of enabling good privacy practices if persuaded that use of such innovations will be helpful in establishing eligibility for the benefits of a safe harbor.

Conclusion

The Staff Report rightly calls for simplified consumer choice and improved transparency in data practices. We particularly welcome the Staff Report's emphasis on privacy by design, an approach IBM has long supported.

At the same time, the Commission's proposals are made against a background of rapid change, both in technology and in consumer expectations and wants. We have offered the foregoing comments in the confidence that improved consumer privacy can be achieved without technological mandates and without sacrificing flexibility and support for innovation.

Thank you for the opportunity to submit these comments.

Sincerely,

Harriet P. Pearson
Vice President, Security Counsel & Chief Privacy Officer
IBM Corporation

Christina Peters
Senior Counsel, Security & Privacy
IBM Corporation

[3] IBM's researchers continue to make breakthroughs in privacy-protective technologies. The award-winning Identity Mixer offers identity management without compromising privacy via anonymous credentials. See http://www.zurich.ibm.com/news/10/innovation.html. Homomorphic encryption permits processing of data in its encrypted state, and offers the promise of improved security in cloud computing. http://domino.research.ibm.com/comm/research_projects.nsf/pages/security.homoenc.html. Another example showcases privacy by design. On January 28, 2011, at the preeminent global conference on Privacy by Design in Toronto, IBM Distinguished Engineer Jeff Jonas keynoted and debuted for review to the expert audience his "G2" privacy-enabling analytics engine. IBM's work in this area is based on Jonas' patented privacy technology innovations and on homomorphic encryption. See http://www.jeffjonas.typepad.com/jeff_jonas/2011/02/sensemaking-on-streams-my-g2-skunk-works-project-privacy-by-design-pbd.html.