



---

International Business Machines Corporation  
600 14<sup>th</sup> Street, NW, Suite 300  
Washington, DC 20005

January 28, 2010

National Telecommunications and Information Administration  
U.S. Department of Commerce  
1401 Constitution Avenue, NW  
Room 4725  
Washington, D.C. 20230

Re: Docket No. 101214614-0614-01  
*Submitted online to: [privacynoi2010@ntia.doc.gov](mailto:privacynoi2010@ntia.doc.gov)*

Dear Sirs and Madams:

IBM is pleased to submit the following comments to the Commerce Department's Green Paper, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework." As a company whose commitment to privacy extends back decades, and which understands that consumer trust underpins sustained economic growth in every era, we welcome attention to these important and far-reaching issues by the Department and others.

The Green Paper represents an important step toward a new partnership between government and industry with respect to privacy, and reflects the contributions of many respondents, including IBM, to the Privacy and Innovation Notice of Inquiry (NOI) of April 23, 2010. We support the Department's efforts to find a workable and balanced commercial privacy framework that could set the stage for smoother cross-border data flows. Development of voluntary enforceable codes would be an excellent way to translate Fair Information Practice Principles into workable, flexible, and enforceable form. A national data breach notification law with federal preemption would greatly simplify current practice, and provide equivalent or better protection to citizens at less cost to business. And the nation is in real need of a voice for data privacy in the executive branch, such as the proposed Privacy Policy Office in the Department of Commerce.

We do believe, however, that the Department's proposals would benefit from some refinement with a view toward better protecting consumer privacy while avoiding undue impact to the private sector. Our suggestions as to those refinements are also provided in the attachment.

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

## **Introduction**

IBM welcomes the current focus by regulators, industry and the public alike on commercial data privacy policy. We believe that privacy issues must be satisfactorily addressed to foster economic growth and progress, and that strong international and domestic engagement by the Department of Commerce on these issues has great value to American business. We also believe that properly calibrated regulatory initiatives, potentially including baseline privacy regulation and voluntary enforceable codes of conduct, can help improve privacy protection for consumers; drive the development and implementation of privacy by design; and increase the confidence of the public in the digital economy.

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 and energy. A contemporary and effective privacy policy framework in the United States that is consistent with international standards could 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 create transparency, predictability, and consumer confidence without damage to the openness and flexibility necessary to foster business confidence and innovation. In responding to the Department's request for comments, we join President Barack Obama in advocating and seeking "the right balance . . . [to] make our economy stronger and more competitive, while meeting our fundamental responsibilities to one another."<sup>1</sup>

## **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 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, sales, 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.

---

<sup>1</sup> Barack Obama, "Toward a 21st-Century Regulatory System," The Wall Street Journal, Jan. 18, 2011, <http://online.wsj.com/article/SB10001424052748703396604576088272112103698.html>

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.<sup>2</sup> 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.

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 a baseline commercial data privacy framework should be technology-neutral and calibrated to protect consumers while avoiding undue burdens to business.**

Expanded Fair Information Practice Principles (FIPPs) have been proposed as a basis for a commercial data privacy baseline. We know from experience that these are principles whose proper implementation depends on context, data elements, and other factors. The principles themselves may take different forms in different contexts; a specific set of FIPPs developed for a government agency will differ from one developed for a large private business. 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.<sup>3</sup> 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.

If baseline commercial data privacy principles are formalized via federal policy, at minimum they should:

---

<sup>2</sup> IBM has worked toward this goal by supporting the APEC Privacy Framework, which addresses these issues by promoting consistent privacy approaches among member-countries while avoiding unnecessary barriers to the free flow of information throughout the region. IBM believes that the APEC Privacy Framework and its implementation through the Cross Border Privacy Rules system can effectively support responsible and accountable personal information transfers across the APEC region.

<sup>3</sup> Our experience with multistakeholder bodies suggests to us that voluntary enforceable codes would be best developed without direct involvement by regulators until the codes are substantially complete, unless the developing body seeks earlier input. Further, the incentive of safe harbors will create adequate motivation for industry to move forward in a timely way.

- **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** for the broad swath of business and for most data, with higher bars for data covered by existing sector-specific regulation and for those businesses willing to comply with more stringent voluntary enforceable codes. Over time, experience will guide regulators as to whether and how to impose more demanding requirements. They should also provide businesses with flexibility to handle data in ways that make sense for their own businesses. For example, data retention periods should not be rigid or across-the-board; acceptable ranges should reflect business realities such as length of useful life and rate of data decay.
- **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 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.
- **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 certainty 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 makes 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 their data is being handled and 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). As IBM explained in more detail in its Comments,<sup>4</sup> 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.<sup>5</sup>

- **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 FTC’s 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 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 permitting 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, as a clear understanding of what consumers expect, want, and need is only beginning to emerge.

---

<sup>4</sup> Comments, pp. 4-5.

<sup>5</sup> 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](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).

- **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. 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.
- **Privacy Impact Assessments (PIAs)** are useful tools for business as well as for government to understand and mitigate risk, but it is important to distinguish between the business context and the governmental one in which transparency is a key feature of the relationship between government and citizens in a free society. First, a PIA may contain proprietary or competitively sensitive information that ought to be shielded from disclosure. Moreover, using PIAs in the business context as a transparency tool rather than a risk management tool threatens to blunt their importance. To encourage the self-criticism and frankness that makes PIAs most useful, businesses should not be required to disclose them. That said, businesses may choose to make PIAs public; a consumer business, for example, might find a PIA helps provide transparency around a new practice or a practice of particular public concern.

### 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:

- IBM supports the establishment of a Privacy Policy Office (PPO) within the executive branch to provide more leadership to the development of U.S. privacy policy, and to more credibly articulate U.S. interests in the international privacy debate. A PPO could also serve as a focus of government engagement with industry, privacy experts and consumer advocates to foster communication and

innovation.

- 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 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.

#### **4. A federal data breach notification law with federal preemption could provide as or more effective protection to consumers at lower cost to business.**

IBM believes that a federal data breach notification law could more effectively and efficiently provide for data breach notice to consumers than the current patchwork of nearly 50 state laws does today. A federal data breach notification law that preempts disparate state legislation would greatly simplify and speed the notification process, while at the same time achieving the primary objective of the state laws: notifying consumers in the event of a data breach. Making notification itself less costly and burdensome would, in turn, increase compliance.

We believe the key elements of an effective federal data breach notification law include:

- **Risk of harm standard.** The law should require notice only when there is a material risk of harm to consumers. A law that requires notice without consideration of harm would habituate consumers to notifications unrelated to real risk, and would accordingly discourage them from taking appropriate action. For the consumer, it would become difficult to distinguish a breach of concern from background noise.
- **Data elements related to risk of harm.** The law should apply to the following types of information, the misuse of which can create a risk of harm to people: social security numbers, state ID numbers, drivers' license numbers or equivalents, bank and financial account numbers and "pin" codes for these accounts. These are the types of information which can harm consumers; other categories of information will result in the over-notification problem described above.
- **Time frame that permits investigation and remediation.** The notice time frame should provide for expeditious notice and at the same time permit the organization to fully investigate incidents, remediate dangerous situations, and cooperate with law enforcement without arbitrary deadlines that can create rather than mitigate risk in complex situations. We favor language requiring expeditious notification consistent with those needs, and a law enforcement exception that takes into account the fact that direction from law enforcement can take many forms,

including an oral form. Requiring notice before investigations are completed or remediation put in place creates unnecessary further risk.

- **Knowledge and reasonable likelihood of harm.** Notice should be required when the organization knows that an unauthorized third party has or is likely to have accessed and obtained the data, and that there is a reasonable likelihood of harm to consumers arising from the breach. Breaches that do not meet these criteria do not rise to the level of a public risk, and requiring notification would create the over-notification risk described above.
- **Flexible notice provision.** The law should provide flexibility as to how notice is provided, by permitting notice via letter, documented phone call, or email where email is a normal means of communication between the parties and there is no reason to believe e-mail addresses are not accurate, and by permitting alternative notice where these methods are not practicable.
- **Notice to data subjects; differentiation between controllers of data and service providers.** The law should provide for notice to those parties potentially affected and best placed to take action -- the data subjects, or, for service providers, the entity who must notify the data subjects. Any notice to regulators that might be required where a breach reaches a significant threshold should be to a single federal regulator, such as the FTC.
- **Safe harbor.** The law should provide an explicit and technology-neutral safe harbor for data effectively protected from unauthorized access, even if the digital or physical “container” in which they are held was compromised. Such a safe harbor would not only reduce notifications unconnected with a real risk of harm, but would also increase overall protection of consumers by providing businesses with a greater incentive to invest in encryption and other protective technologies.
- **Preemption.** Federal data breach notification law should preempt state laws. Preemption would improve compliance of notifying organizations by simplifying the process and reducing costs to notifying organizations. As notifying organizations are often public and taxpayer funded, preemption reduces costs to taxpayers as well.

##### **5. Laws on government access to data are due for re-examination in order to promote consumer trust in the digital economy and citizen trust in government.**

The continued health and development of the Internet requires not only consumer trust in business, but citizen trust in government. Indeed, the preservation of liberty in the digital age requires a special focus on government respect for individual privacy. To that effect, IBM strongly supports a thoughtful re-examination of ECPA, not only with respect to cloud computing but across the board. In the years since ECPA's passage, electronic communications and other digital records have become central to the lives of most citizens, both economically and personally. In key respects, ECPA no longer reflects

today's environment or citizens' expectations of privacy, and does not provide clear guidance in contemporary practice. IBM also supports review of CALEA, FISMA, and the Privacy Act to ensure that government statutes authorizing collection of and access to personally identifiable information are consistent and reflect contemporary understandings and use of digital communications. Clear, even-handed, and technology-neutral laws regarding government access to digital data encourage public trust – as does a clear government commitment to the rule of law in the digital sphere.

**6. Privacy in cloud computing can be managed using Privacy by Design and other approaches familiar from other computing models, and can be best regulated in the same technology-neutral ways.**

Cloud computing is an on-demand computing model that has gradually emerged over the past decade, used by consumer and enterprises alike. That is, cloud computing permits computing services to be accessed and used as needed. It is available over a network and accessible through standard mechanisms (e.g., browsers), independent of the type of user (enterprise or individual) and the type of hardware used. It satisfies user processing and storage demands across a multi-tenant infrastructure (or single tenant, in the case of private or hybrid clouds), with locations that change dynamically. It allows users to increase or decrease their capacity and computing power at their option (that is, it is “scalable”). Because charges tend to be based on usage (instead of requiring an infrastructure and IT support investment), it tends to be more economical than other computing models. Cloud computing comes in several forms: public clouds, private clouds and hybrid clouds, each with its own advantages and disadvantages.

IBM believes that cloud computing overall does not pose a truly distinct challenge for privacy and security policy. Accordingly, regulation in this area should continue to be technology-neutral, and focused on the actual uses of data. Just as they have done within the context of other computing models, organizations need to make sound, risk-based choices about infrastructure and implementation to secure data appropriately; for example, in the cloud context, organizations should choose a private cloud for more sensitive data, public cloud for less sensitive.

Indeed, in important ways enterprises that use cloud computing are likely to improve the security and privacy of the data for which they are accountable. First, cloud computing is driving the modernization of data centers. Such modernization will help support better security and perhaps improve privacy-by-design efforts. Cloud computing enables much more flexible IT acquisition and improvement by enterprises by allowing them to adjust to the sensitivity of the data. And as open standards for cloud computing continue to develop, they should promote data portability and interoperability among cloud services. Specifically, open standards will benefit cloud users by establishing baseline data security features common across cloud architectures regardless of provider. In addition, open standards will allow cloud users to more easily compare offerings (from a data security perspective as well as for other concerns) and choose the option that suits them best. Similarly, enterprise users of cloud services will be able to be more responsive to consumer expectations of privacy.