DEPARTMENT OF VETERANS AFFAIRS
Washington DC 20420

February 23, 2011

The Honorable Gary Locke
Secretary of Commerce
Washington, DC 20230

Dear Mr. Secretary:

The Department of Veterans Affairs (VA) appreciates the opportunity to comment on the Department of Commerce's "Green Paper," entitled: *Commercial Data Privacy and Innovations in the Internet Economy: A Dynamic Policy Framework,* December 16, 2010.

VA has longstanding experience in data privacy issues arising from the broad spectrum of health- and non health-related product lines we deliver to our Nation's Veterans. Experience in these lines of business, we believe, provides us with a unique perspective among governmental agencies about the balance between consumer privacy and efficient business processes.

We hold ourselves to high standards in protecting the privacy of our Veterans and the confidentiality of their personal information. We also have a responsibility to efficiently administer the benefits we deliver. Based on our experience, we are keenly aware that privacy protections and effective business processes can and do efficiently coexist.

The Department of Commerce's "Green Paper" is a valuable contribution to public dialogue on the important issues in this area. We believe these issues affect Veterans as much as any consumer. Thus, we offer the comments in the enclosure to this letter with the hope we can contribute to the dialogue.

We would be pleased to work with the Department as this discussion continues. If you need further information, please have a member of your staff contact Peter L. Levin, Ph.D., Senior Advisor to the Secretary and Chief Technology Officer, who may be reached at (202) 461-4833.

Sincerely,

John R. Gingrich
Chief of Staff

Enclosure

Department of Veterans Affairs

Comments on

Department of Commerce: *Commercial Data Privacy and Innovations in the Internet Economy: A Dynamic Policy Framework,* December 16, 2010

The Department of Veterans Affairs (VA) appreciates the opportunity the Department of Commerce has extended to it and to the public to comment on its "Green Paper"[1] on protecting consumer privacy in commercial settings.

VA has longstanding experience in data privacy issues arising from the broad spectrum of health- and non health-related product lines we deliver to our Nation's Veterans.

- The Veterans Health Administration delivers comprehensive health care to Veterans via the largest integrated health plan in the United States: VA operates 153 multidisciplinary medical centers in all 50 states and in Puerto Rico and Guam; delivers care to Veterans through 958 hospital-based and community-based outpatient clinics throughout the United States and in the Philippines, and provides nursing home care through 133 community living centers. VA's customer satisfaction and clinical quality are routinely judged to be the best in the country.

- The Veterans Benefits Administration provides financial and non-financial benefits to Veterans who have been disabled during their service to our country. In addition to disability and pension payments, VA sends directly to Veterans, it also provides educational assistance, mortgage insurance, and vocational rehabilitation. VA also administers a life insurance program which protects Veterans' families during their service career and throughout their lives.

- The National Cemetery Administration delivers the nation's final honor to Veterans through the country's largest system: 131 national cemeteries in 39 states and Puerto Rico and 33 soldiers' lots and monument sites. More than 3.5 million Americans, including Veterans of every war and conflict, are buried in VA's cemeteries. Each time during the past 10 years the independent National Consumer Satisfaction Index has surveyed its customers, VA's cemetery system has been judged to be the best in the nation.

Experience in these lines of business, we believe, provide us with a unique perspective among governmental agencies about the balance between consumer privacy and

[1] U.S. Department of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Dec. 16, 2010) ("Commerce Report"), available at http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

efficient business processes. We hold ourselves to high standards in protecting the privacy of our Veterans and the confidentiality of their personal information. We also have a responsibility to efficiently administer the benefits we deliver. Based on our experience, we are keenly aware that privacy protections and effective business processes can and do efficiently coexist.

We also recognize that if businesses processes are to be efficient – or sometimes to occur at all – there must be foundational elements of trust. Since economic activity is dependent on the voluntary engagement by both the consumer and business, commerce cannot thrive in an environment without an effective trust fabric. If consumers lack confidence that they will be treated fairly or that their personal information will be appropriately protected, they may be reluctant to do business, or decline to engage altogether.

The trust fabric is critical to VA, as we have achieved much success in improving our relationship with Veterans via new online technologies. Veterans can now apply for many benefits online[2] and can download their own personal health information via the online Blue Button℠.[3] We recognize, however, that Veterans engage with many organizations other than VA; their views about the credibility and trustworthiness of online and other commercial transactions are affected by their non-VA experiences. Veterans who distrust online or other commercial transactions because of privacy issues experienced elsewhere will be less willing to engage online with VA or to share their personal information with us. This will impair VA's ability to efficiently administer taxpayer-supported benefit programs and, worse, may mean that Veterans will not be able to receive the benefits they have earned through their service to our nation.

We join the Department in recognizing the importance of an effective and workable framework which achieves privacy protection goals without impairing the free flow of commerce or stifling innovation in the development of new goods, services, technologies or business models. We are aware that the Federal Trade Commission (FTC) has expressed the same views in a preliminary Staff Report also published in December.[4]

With these perspectives, VA offers the following comments.

---

[2] See: http://vabenefits.vba.va.gov/vonapp/main.asp; https://www.1010ez.med.va.gov/sec/vha/1010ez/.

[3] See: http://www.whitehouse.gov/open/innovations/BlueButton. "Blue Button," the Blue Button logo, and "Download My Data" are Service Marks of the U.S. Department of Veterans Affairs.

[4] U.S. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers,* Preliminary Staff Report (Dec. 2, 2010) ("FTC Report," "Staff Report" or "FTC Staff") available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

I. Scope of the Privacy Framework

VA agrees that a set of privacy guidelines – often characterized as Fair Information Practice Principles (FIPPs) – should broadly apply to commercial practices and to commercial entities that collect, maintain, share, or otherwise use consumer data.

"Consumer data" or "personally identifiable information" (PII) should be defined as any information which can be reasonably linked to any consumer.[5] This definition should be broader than just the name and other identifying or demographic information about an individual: computers, mobile phones, PDAs, and other mobile devices have unique device identifiers or device locators which are monitored and collected during routine use. These identifiers can often be accessed even when devices are not being actively used.[6] Thus, the framework should be based on the principle that it applies to any collection of consumer data which can be reasonably linked to a specific consumer, computer, or other device.

We also agree the framework should apply to all commercial entities which collect PII in either online or offline[7] contexts, regardless of whether those entities interact directly with consumers or indirectly collect and use PII.

VA strongly agrees with the Commerce Report that the scope of any commercial privacy framework should not duplicate existing privacy protection systems established by law.[8] Specifically, privacy aspects of health- and health-related activities are currently governed by the Health Insurance Portability and Accountability Act (HIPAA) and its pertinent regulations.[9] The HIPAA privacy scheme works because health care providers, plans and systems have devoted significant resources during nearly a decade to make it work. Adding an additional and potentially conflicting layer of privacy rules to the HIPAA scheme would do little if anything to enhance protection of

---

[5] This approach would significantly assist in resolution of issues arising from the decreasing relevance of data class-based definitions of PII to distinguish from data classes which are non-PII. FTC Report, 35.

[6] *See,* Commerce Report, 28; FTC Report, 36-7.

[7] We believe the risk to privacy of PII does not disappear when a Veteran or other consumer engages with a business in other ways. For example, it is not uncommon for a business to routinely collect customer zip codes during in-person point-of-retail-sale transactions. Consumers acquire merchant-specific "affinity" or discount cards by providing names, addresses, telephone numbers, email addresses and at times household composition and income levels. Obtaining service for one's automobile usually requires disclosure of auto make, model, mileage, license plate number and vehicle VIN. For these reasons and particularly due to the data aggregation issues discussed in Sec. IV(B) below, PII privacy issues do not end when a Veteran or consumer goes offline.

[8] Commerce Report, 4-5: A " focus on commercial data privacy does not cover privacy laws and policies that cover information maintained by the Federal Government or that cover specific industry sectors. . . ." These other laws include the Privacy Act, Pub. L. 93-579 (1974), 5 U.S.C. § 552a; and the sector-specific statutes listed in the Commerce Report at 11-12, nn. 22-25.

[9] Pub. L. 104-191 (1996); 45 CFR Parts 160; 164, Subparts A and E.

personally identifiable health information (PHI). It would, however, dilute return on the considerable investments made in HIPAA implementation by VA and the rest of the health care industry. Thus, where existing law already comprehensively regulates privacy practices in an industry or government segment, any new privacy framework should not intrude.

II. Creation of the Framework

The FTC and Commerce Reports each explore whether a new privacy framework for commercial activities can be effectively implemented by voluntary industry codes of conduct.[10] VA concurs with the views in the Commerce Report,[11] that this question deserves significant discussion in an open multi-stakeholder process.[12] We also concur with Commerce's views that the principles underlying either voluntary standards or other implementing mechanisms should be:[13]

- Transparency: disclosures and consents which are simple and understandable
- Specificity in the purposes for which PII is collected
- Limiting use of PII to those purposes, and
- Accountability.

III. Consumer Choice and Consent

VA agrees with both agencies[14] that consumers face great burdens in understanding lengthy, legalistic and typically overwhelming privacy policies. Contemporary privacy policies are, with unfortunately rare exception, incomprehensible to ordinary consumers. A consumer which cannot understand a policy cannot effectively exercise informed choice as to whether they will agree to that policy. We concur with both agencies that to achieve transparency a simplified, standardized approach is needed to increase transparency to consumers, be less burdensome to businesses and maintain the free flow of commerce.

---

[10] Commerce Report, 41-43 ; FTC Report, iii.

[11] Commerce Report, 41.

[12] There are multiple processes via which multi-stakeholder input could be received; OMB Circular A-119 seems particularly pertinent in this context. *See,* http://www.whitehouse.gov/omb/circulars_a119/.

[13] Commerce Report at pp. 30-40.

[14] Commerce Report, 31, *et. seq.;* FTC Report, 19-20, 70.

A. Standards should be agnostic to business sectors and to technology.

We agree with the Commerce Report[15] and FTC Staff[16] that privacy standards should be dynamic, written in functional terms without reference to specific lines of business or any particular technology.

Standards in any framework should be written to apply to future business models and future technologies as yet unimagined. They should define *what* must be *achieved* to protect privacy, and leave decisions on *how* those protections are to be achieved to the ingenuity of the innovator and the flexibility of the free market.[17]

B. General Rule: Consent to use PII in commercial Settings

The basic rule of a privacy framework should require a consumer to consent both to provide their PII and for any use of that information. Exceptions to this basic rule should be limited.

C. Exception to the Rule: "Commonly Accepted Practices" which do not require consent

We agree there should be a list of "commonly accepted practices" not requiring consent for disclosure or use.[18] The list should be short. Definitions should also be short and simply written. PII practices not defined specifically as "commonly accepted" should be subject to requirements for obtaining consumer consent.

"Common" practices should be limited to capture and use of data essential to fulfillment of ordinary course-of-transaction processes between the consumer and business. For example, in an online transaction, "common" data could be limited to customer name, address, credit card information and possibly an email address if used solely for the purpose of direct communications to the consumer to, *e.g.,* provide shipping information. In an in-person point-of-sale cash transaction, no PII should be collected or used at all, since those data are not essential to the transaction. HIPAA's "minimum necessary data" concept[19] provides an effective model in this area.

---

[15] Commerce Report, 3.

[16] FTC Report, 35.

[17] For example, any technology-centric rules written more than five years ago would likely not have considered how privacy should be protected in a cloud computing environment. And as noted below in section III(D), previous notice-and-consent practices are entirely unsuited to the new technology of mobile devices.

[18] Commerce Report, 23 ("baseline FIPPs"); FTC Report, 53.

[19] Note 9, *supra.*

Other "common" practices may include use of consumer data entirely internal to the business which collects it,[20] fraud prevention and the sharing of information under specified circumstances with law enforcement authorities and credit bureaus. HIPAA health care privacy rules[21] offer a model for how these types of "common" practices could be defined in commercial settings.

D. Mobile Device disclosure and consent

Due to the limited amount of information that can be displayed on a mobile device's small screen, delivering notices and consents via those devices presents particular concerns. For example, some applications for Apple's iPhone have user agreements 100 screens or more in length.[22] As a practical matter, few users who simply want to download a song from iTunes will attempt to wade through the legalese, and those hardy souls who try to do so will quickly find themselves frustrated by the latency between each of the 100 screens.

Lengthy texts, whether informational or transactional, are incompatible both with the fundamentals of informed consent and with the technology-driven use of mobile devices. VA agrees with the FTC staff that a readily-recognizable icon such as VA's Blue Button℠ with common meaning across business lines may be helpful. VA also agrees with both the Commerce Report and FTC staff that standardized disclosures can be leveraged to facilitate commerce via mobile devices. The alternative – which we do not find attractive – would be to prohibit consents via mobile devices for non-"common" data capture and use.

IV. Evaluating the bargain: Free PII as the price for internet services

We agree with the agencies that consumers pay for free or inexpensive access to internet content by agreeing to free disclosure of their PII and to its use, re-use, sale and re-sale. FTC staff write of this bargain as "trade-offs consumers make when they share their data in exchange for services."[23]

The Commerce Report agrees with this proposition while in the process of making an even more important observation: "The current policy framework provides consumers with a limited basis to understand the basis of this economic bargain."[24] In another

---

[20] The Commerce Report, 39, suggests a particularly pertinent example of how internal-to-the-business use of PII for fraud prevention can provide significant benefits to both consumers and the business which uses those data.

[21] Particularly pertinent are HIPAA's permissible "common" uses of health data for "treatment, payment and operations," and its exception for disclosure to, *e.g.,* law enforcement or public health agencies.

[22] FTC Report, 70.

[23] FTC Report, 61.

[24] Commerce Report, 32.

quite significant comment, the Commerce Report speaks of the need for consumers to have the ability to make "the well informed choice" about whether to share PII and agree to its use.[25]

We believe that enhancing transparency in disclosures and consents will go far in informing consumers of how their PII might be collected and used. That said, if there is to be a true bargain between PII discloser and PII user, the consumer must have "an informed and meaningful"[26] opportunity to "say no;" to decline either to provide PII or to permit its use.

To that end, we offer the following comments.

A. "Take It or Leave It" Consent

FTC staff request comment as to whether it is appropriate for companies to offer choice as a "take it or leave it" proposition, "whereby a consumer's use of a web site, product or service constitutes consent to the company's information practices." [27]

For example, a commercial Web site may simply state that *any* use of the site constitutes consent to the company's privacy terms – even if those terms are not available unless the consumer "uses" the Web site to read them. Such implied-by-use consent is typically on an "all or nothing" basis; even when making a single purchase a consumer does not have an option to agree to some terms essential to the transaction and reject other terms which are not. The question arises as to whether the consumer has a meaningful opportunity to "say no."

We agree that "take it or leave it" consent practices deserve significant discussion in an open multi-stakeholder process.

B. "Do Not Track"

FTC staff suggests consumers should have an option to tell businesses "Do Not Track."[28] Similar to the "Do Not Call" registry for telemarketing, "Do Not Track" would allow a consumer to decline to allow a specific business or all businesses to collect any information other than that permitted by "common" practices.

We join the Department of Commerce in the view that discussion and development of this technology should be encouraged via an open multi-stakeholder process.[29]

---

[25] Commerce Report, 33.

[26] FTC Report, 57, also 26.

[27] FTC Report, 61.

[28] FTC Report, 63-69.

[29] Commerce Report, 47, 72.

We also suggest these discussions include dialogue as to whether consumers should have an option to tell any business "Do Not Share." The Commerce Report notes the practice of "creative re-use of existing information"[30] which can support substantial value-added innovations, " . . . but not at the expense of consumer privacy. . . . Consumers need to know that when their data are re-used, the re-use will not cause them harm or unwarranted surprise."[31]

FTC staff note that re-use practices have become a "ubiquitous collection of consumer data that occurs in multiple contexts and at numerous points throughout a given day." These data are then shared without limitation, including companies "many layers removed from and [which] typically do not interact with consumers."[32] A number of privacy concerns are mentioned. With a "Do Not Share" option, a consumer could agree a particular company may collect and use their PII but decline consent for its sale to or re-use by third parties.

We believe a careful structuring and balancing of guidelines relating to "Take it or Leave It," "Do Not Track" and "Do Not Share" would continue to allow innovation based on the creative re-use of a consumer's PII, yet place in the hands of the consumer a meaningful opportunity to "say no."

Again, VA appreciates the opportunity to comment in this important area. We stand ready to work with the Department and other interested parties in the development of a privacy framework for Veteran and consumer PII used in commercial settings.

---

[30] Commerce Report, 38.

[31] Commerce Report, 39.

[32] FTC Report, 23.