Comments of the Electronic Privacy Information Center

To

The Department of Commerce

Office of the Secretary

National Telecommunications and Information Administration
International Trade Administration
National Institute of Standards and Technology

[Docket No. 101214614-0614-01]
RIN 0660- XA22

"Information Privacy and Innovation in the Internet Economy"

January 25, 2011

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

To

THE DEPARTMENT OF COMMERCE

Office of the Secretary
National Telecommunications and Information Administration
International Trade Administration
National Institute of Standards and Technology
[Docket No. 101214614-0614-01]
RIN 0660- XA22
"Information Privacy and Innovation in the Internet Economy"

January 28, 2011

The Department of Commerce's Internet Policy Taskforce is "conducting a comprehensive review of the nexus between privacy policy and innovation in the Internet economy."[1] On April 23, 2010, the Department sought comments from stakeholders on the "impact of current privacy laws in the United States and around the world on the pace of innovation in the information economy."[2] The Department is now asking for comments on its report entitled, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" [Hereinafter "Commerce Report" or "Report"].[3]

The Commerce Report contains the elements of a useful Administration position on data protection in the modern era. The Report calls for the adoption of "Fair Information Practices" (FIPs), the development of privacy codes of conducts, and the creation of a privacy office.

---

[1] Department of Commerce, Internet Policy Task Force, "Information Privacy and Innovation in the Internet Economy, Notice and Request for Comments, December 16, 2010, *available at* http://www.ntia.doc.gov/frnotices/2010/FR_IPTFPrivacy_RequestforComments_12162010.pdf.
[2] *Id.*
[3] Department of Commerce, "Information Privacy and Innovation in the Internet Economy," December 15, 2010, *available at* http://www.ntia.doc.gov/internetpolicytaskforce [hereinafter *Report*].

But the Commerce Report stops short of any specific legislative proposals, and mostly relies on self-regulation and other voluntary measures. Notably, the Commerce Report makes no meaningful effort to assess the adequacy of self-regulation. The Report also fails to discuss emerging threats to consumer privacy or the growing risk that consolidation of Internet based services poses to users. The Report does not address the proposal that the United States move toward ratification of Council of Europe Convention 108, the widely recognized international treaty for privacy protection. The Commerce Report further misunderstands the relationship between privacy protection and innovation, and threatens to repeat the dreadful mistake of P3P. In summary, the Commerce Report is more focused on facilitating the interests of businesses to collect personal data than it is on the need to safeguard the information of consumers and Internet users. And the multi-stakeholder approach set out in this report appears, almost by design, to ensure that no new meaningful safeguards are established.

Pursuant to the Department of Commerce Notice, the Electronic Privacy Information Center (EPIC) submits these comments and recommendations to address both issues raised in the Report and issues that should have been raised but were not. EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in protecting individuals' privacy on the Internet,[4] and its recommendations center on the need for real enforcement, not self-regulation. EPIC's suggestions include: the creation of an

[4] *See, e.g.,* EPIC: Federal Trade Commission, http://epic.org/privacy/internet/ftc/; EPIC: Online Tracking and Behavioral Profiling, http://epic.org/privacy/consumer/online_tracking_and_behavioral.html; EPIC: Children's' Online Privacy Protection Act (COPPA), http://epic.org/privacy/kids/; EPIC: Choicepoint, http://epic.org/privacy/choicepoint/; EPIC: Cloud Computing, http://epic.org/privacy/cloudcomputing/; EPIC: Social Networking Privacy, http://epic.org/privacy/socialnet/.

independent US privacy agency, the passage of a comprehensive federal privacy law based on Fair Information Practices, and the implementation of a strong international privacy framework to protect consumers and users of new Internet-based services.

Comments and Recommendations

EPIC submits the following comments and recommendations:

1. *Creation of an Independent Privacy Authority Will Improve Privacy Protections*

The Commerce Report recommends the creation of a privacy office within the agency, but this is not the correct approach for an office that should protect the interests of consumers and Internet users. The creation of an independent privacy agency will enhance privacy protections for individuals. Such an entity would have the authority and the expertise to ensure that agencies are complying with the Privacy Act and to help agencies anticipate new challenges involving rapidly changing technology and privacy issues. The organization should be independent of the executive branch. The correct model would be an independent agency, similar to the Federal Trade Commission or the Federal Communications Commission.

In 1973 the Department of Health, Education and Welfare established a special panel to study privacy issues arising from the growing use of automated date processing equipment.[5] That report led to the development and passage of the Privacy Act of 1974.[6] But that report also made clear that the cornerstone of an effective federal policy is a

[5] US Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens*, (July 1973), *available at* http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm.
[6] 5 U.S.C. § 552a (1974).

permanent privacy agency.[7] Virtually every study that has looked at the US experience since 1974 has concluded that the United States needs an independent privacy agency.[8]

In countries across the world, independent privacy agencies have been established to address similar concerns. The European Union has implemented extensive privacy directives that establish legal rights for all citizens in the European Union countries. Non-EU countries, from Canada[9] to Hong Kong,[10] are pursuing comprehensive privacy agendas led by privacy agencies. These government agencies routinely report on the handling of privacy complaints,[11] the emergence of new privacy issues, and proposed measures to protect privacy. These reports help the public and the government understand the status of privacy protections in their country and develop new approaches to replace old ones.

But there is still no privacy agency in the United States. In fact, President Obama is only just beginning *now* to nominate people to staff the Privacy and Civil Liberties

---

[7] HEW Report, *supra* note 5.

[8] *See, e.g.,* Jeffrey Rosen, "Nude Breach: Why Privacy Always Loses," The New Republic, December 13, 2010 (Compared to their European counterparts, U.S. privacy offices lack both independence and regulatory teeth…the Government needs a genuinely independent institution dedicated to protecting Americans' privacy); Bob Gellman, "*A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board,"* 54 HSTLJ 1183,1208, April 2003 ("Only an independent [privacy] agency can criticize the policies and practices of the executive branch…it is undisputed that many routine government functions can have drastic effects on the privacy rights and interests of individuals."); David H. Flaherty, *Protecting Privacy in Surveillance Societies* 22, 381 (1989) ("…it is not enough simply to pass a data protection law . . . an agency charged with implementation is essential to make the law work in practice. . . A statute by itself is an insufficient countervailing force to the ideological and political pressures for efficiency and monitoring of the population that are at work in Western society."); Marc Rotenberg, *In support of a Data Protection Board in the United States*, 8 Government Information Quarterly 79-93 (1991) ("A privacy protection commission was a key component of the original privacy protection scheme developed by the Congress in the early 1970s but was never enacted. Recent public polling data suggests that the creation of a similar board today would be supported by a wide majority of Americans.").

[9] Office of the Privacy Commissioner of Canada, Mandate and Mission of the OPC, http://www.privcom.gc.ca/aboutUs/index_e.asp.

[10] Office of the Privacy Commissioner for Personal Data, Hong Kong, Homepage, http://www.pcpd.org.hk/.

[11] Office of the Privacy Commissioner of Canada, http://www.privcom.gc.ca/i_i/index_e.asp.

Oversight Board.[12] In many respects, this is surprising. It is clear that the absence of a privacy agency in the federal government remains a critical problem. Having announced numerous programs that hinge on the collection and dissemination of Americans' personal information, some institutional balance must be established to ensure that these proposals receive adequate review. This would be a small investment in what many Americans consider their number one concern about our nation's infrastructure – the protection of personal privacy.

The Department of Commerce report proposes a Privacy Policy Office located within the Department of Commerce that would "convene . . . business with civil society in domestic multi-stakeholder efforts. . . to develop consensus-based voluntary codes of conduct."[13] This structure is almost guaranteed to ensure that no meaningful privacy standards emerge. Self-regulation has failed to protect consumers, and the Office proposed by Commerce would be perpetuating the status quo of self-regulation. The report clearly states that the office would not "have any enforcement authority,"[14] rather it would merely function as a "convener" – bringing together groups, to "provide industry with guidance."[15] Without enforcement capabilities, it will be difficult for the Office to create actual privacy protection for consumers. Additionally because the Office would be located within the Department of Commerce, it would not be able to operate independently of the Department, which would prevent it from being as effective as privacy agencies in other nations.

The limitations of a privacy office within a federal agency are apparent when

[12] The White House, Nominations sent to Senate, December 17, 2010, *available at* http://www.whitehouse.gov/the-press-office/2010/12/17/nominations-sent-senate.
[13] Report, *supra* note 3 at 44.
[14] *Id.* at 45 [Recommendation #4].
[15] I*d.* at 45-46.

examining the Department of Homeland Security (DHS) Privacy Office. The mission of the DHS Privacy Officer is to "to preserve and enhance privacy protections for all individuals, to promote transparency of Department operations, and to serve as a leader in the federal privacy community."[16] The Chief Privacy Office has a broad statutory mandate, including the responsibility to ensure that the Department's use of technologies "sustain, and do not erode" privacy protections, and to evaluate any governmental proposals "involving personally identifiable information."[17]

Yet the DHS Privacy Office has not done the work that Congress set out for it to do. The Privacy Office has allowed several projects with detrimental impacts on privacy to go forward, such as Fusion Centers, Full Body Scanners in airports, Closed-Circuit Television Surveillance, and suspicionless electronic border searches.[18] In each of the above cases, the Privacy Office has failed in its statutory duty to assure that the use of technologies does not erode privacy protections relating to use, collection, and disclosure of personal information.[19] The Privacy Office is unable to fulfill its statutory obligations because the decisions of the Chief Privacy Officer are subject to the oversight of the Secretary and the rest of the Executive Branch.[20] This is why an independent privacy office is needed.

The Commerce Department has set out a blueprint for an "anti-privacy agency," an entity that will consume time and resources but will be unable to act on any

[16] Department of Homeland Security, About the Privacy Office, *available at* http://www.dhs.gov/xabout/structure/editorial_0510.shtm.
[17] Department of Homeland Security, Authorities and Responsibilites of the Chief Privacy Officer, *available at* http://www.dhs.gov/xabout/structure/gc_1265225837602.shtm.
[18] *Id.*
[19] *See* Department of Homeland Security, Authorities and Responsibilities of the Chief Privacy Officer, *available at* http://www.dhs.gov/xabout/structure/gc_1265225837602.shtm.
[20] Letter from Privacy Coalition to Reps. Thompson and King, October 23, 2009, *available at* epic.org/security/DHS_CPO_Priv_Coal_Letter.pdf.

recommendations or specifically address consumer concerns. At least under the Safe Harbor regime, which was hardly ideal, the Commerce Department had the obligation to ensure that US firms complied with Safe Harbor obligations. The proposal contained in the Commerce Report lacks even this minimal baseline standard.

2. *Comprehensive Federal Privacy Laws should be based on Fair Information Practices*

The Report appropriately endorses Fair Information Practices (FIPs) as the foundation for privacy protection.[21] The Report states that FIPs "provide flexible protection for privacy interests in commercial data that currently receive little or no statutory privacy protection" and acknowledges the failure of the "notice and choice" model currently used by the Federal Trade Commission (FTC).[22] But in order to work, FIPs must not merely be guidelines or suggestions, they must be codified in comprehensive, enforceable federal legislation. And they are not "Principles," they are the actual "practices" that businesses are expected to adopt.[23]

The Fair Information Practices that form the basis of such legislation should be modeled on the Privacy Act of 1974[24] and on the Organization for Economic Co-operation and Development (OECD) Privacy Guidelines[25]. The guidelines set out by the OECD include: data quality, purpose specification, use limitation, security safeguards,

[21] *Id.* at 23 ("widespread adoption of comprehensive FIPPs is important to achieving the goals we have set for the Dynamic Privacy Framework").
[22] *Id.*
[23] The recent popularization of the phrase "Fair Information Practices Principles" waters down one of the key insights of the 1973 report: that effective privacy protection focuses on what organizations actually do, not what they claim to do.
[24] Privacy Act of 1974, 5 USC § 552a.
[25] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

openness, individual participation, and accountability.[26] The principles outlined in the Privacy Act are very similar:

> (1) Permit an individual to determine what records pertaining to him are collected, maintained used or disseminated by such agencies;
> (2) Permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;
> (3) Permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;
> (4) Collect, maintain, use or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;
> (5) Permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and
> (6) Be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act.[27]

But the Privacy Act only applies to the collection of information by federal agencies in the U.S., not to the collection of information by private companies or non-governmental entities. In these areas, the U.S. followed a policy of sectoral regulation in the 1980s and early 1990s, but then adopted the approach of self-regulation for Internet-based commerce.[28]

The same principles outlined in the Privacy Act should form the basis of comprehensive federal privacy legislation that will protect all citizens' privacy in the face of invasive online tracking and behavioral profiling. In Europe, many countries have

[26] *Id.*
[27] Privacy Act of 1974, 5 USC § 552a.
[28] Anita L. Allen, *Privacy Law and Society,* Thomson Reuters, 2011 ("United States policy-makers have favored a combination of multiple, limited-purpose public laws and industry self-regulation…over the years, Congress has enacted numerous privacy-protection statutes, resulting in a patchwork quilt of special-purpose rules.").

passed national laws based on FIPs that apply to both the public and private sector.[29] It is time for the U.S. to follow that example. The suggestion of the report for "baseline commercial data privacy legislation" should be implemented.[30]

3. *The U.S. Must Support Comprehensive International Privacy Protection and not rely on "Safe Harbor" agreements*

EPIC supports strong international privacy protection frameworks and urges the Department of Commerce to move forward in this area. EPIC strongly supports the Council of Europe Convention 108 and has launched a campaign urging the US Government to support the Council of Europe Privacy Convention. On January 28, 2010, twenty-nine members of the EPIC Advisory Board wrote to Secretary of State Hillary Rodham Clinton to urge that the United States begin the process of ratification of Council of Europe Convention 108.[31] As we explained:

> Almost thirty years after the adoption of the Council of Europe Convention, forty-one countries, including both members and non-members of the Council of Europe, have signed the Convention. However, the United States has not yet signed the Convention.
>
> The protection of privacy is a fundamental human right. In the 21st century, It may become one of the most critical human rights of all. Civil society organizations from around the world have recently asked that countries which have not yet ratified the Council of Europe Convention 108 and the Protocol of 2001 to do so as expeditiously as possible.
>
> It was the United States and Eleanor Roosevelt who helped craft the Universal Declaration of Human Rights on which the Convention is based. And it is the United States that has ratified the Council of Europe Convention on Cybercrime and urged its allies to do so as well.

[29] Robert Gellman, "Fair Information Practices: A Basic History," May 13, 2010, *available at* bobgellman.com/rg-docs/rg-FIPShistory.pdf.
[30] Report, *supra* note 3 at 51.
[31] Letter from EPIC Advisory Board to Secretary Clinton, January 28, 2010, *available at* http://epic.org/privacy/intl/EPIC_Clinton_ltr_1-10.pdf.

> You [Sec. Clinton] reminded us last week "We need to synchronize our technological progress with our principles" and said "The United States is committed to devoting the diplomatic, economic, and technological resources necessary to advance these freedoms."[32]

Twelve privacy groups also signed a resolution to the U.S. Senate on January 29, 2010 endorsing Convention 108.[33] The resolution states simply:

> Expressing a need for the accession to the Council of Europe's Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data
>
> Whereas privacy is a fundamental right, valued by all Americans;
>
> Whereas the increase of automatic processing and sharing of data continuously intensifies the need for more effective implementation and execution of legal instruments;
>
> Whereas data security breaches along with cases of identity theft continue to pose a substantial risk to American consumers and businesses;
>
> Whereas the continued transfer of personal data across national borders raising increasing concerns about the adequacy of privacy protection raises;
> Whereas the current sectoral approach of legislation in the United States is insufficient for appropriate privacy and data protection;
>
> Whereas the domain of privacy and data protection is international and requires an overarching framework in order to acknowledge and protect the fundamental rights of citizens; and
>
> Whereas the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data is the most fundamental international instrument in the field:
> Now, therefore, be it resolved, that the Senate-
> (1) requests accession to the Council of Europe's Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

---

[32] Letter, *supra* note 35.
[33] Privacy Coalition, Resolution, United States Senate, January 29, 2009, *available at* http://privacycoalition.org/resolution-privacy_day.pdf.

The Convention's primary purpose is to strengthen data protection, specifically the legal protection of individuals with regard to automatic processing of personal information relating to them. Such legal rules are needed as computers are increasingly used for administrative purposes. Compared with manual files, automated files have a vastly superior storage capability and offer possibilities for a much wider variety of transactions which they can perform at high speed. Further growth of automatic data processing in the administrative field can be expected in the years ahead, due to the lowering of data processing costs, the availability of "intelligent" data processing devices, and the establishment of new telecommunication facilities for data transmission.

And more recently, to address the growing concerns of a disruption in data transfers between Europe and the United States, EPIC President Marc Rotenberg appeared before the European Parliament in October 2010, where he urged the adoption of a comprehensive international framework to protect the flow of personal data between the US and the EU.[34] Citing the growing concern about the misuse of sensitive data and the absence of effective legal remedies, Mr. Rotenberg said it was time for the US and the EU to develop an effective legal framework that would safeguard the rights of citizens and the users of Internet-based services. These principles should apply to data collection that occurs by both private and public entities. EPIC has previously supported the Madrid

[34] *See,* Marc Rotenberg, President of EPIC, "Data Protection in a Transatlantic Perspective: Future EU-US international agreement on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters," Brussels, Belgium, October 16, 2010, *available at* http://epic.org/privacy/intl/EPIC_EU_Parl_EU_US_Data_Transfers_25_10_2010.pdf.

Privacy Declaration[35] and the Council of Europe Privacy Convention[36] as good models for international privacy frameworks.

One US-EU arrangement that has not been effective is the Safe harbor agreement. The Report recommends the creation of a "safe harbor" for companies that "commit and adhere to a . . . voluntary code of conduct."[37] The Report argues that the Safe Harbor will provide companies with "ample incentive to participate in developing voluntary codes."[38] However, history does not support this supposition. The 2001 Safe Harbor arrangement that the Department of Commerce set up between the U.S. and the European Union when the EU passed its Data Protection Directive is a case in point.[39] A 2001 report evaluating this Safe Harbor" found that of the 75 companies studied, none met all the standards necessary to qualify for the Safe Harbor arrangement.[40] The study also found that only 5% of companies had any procedures in place to ensure compliance with safe harbor principles.[41] A World Privacy Forum Report from November 2010 found that "[t]he Department of Commerce's failure to demand compliance with Safe Harbor requirements has so undermined the value of the program that some European data protection authorities are no longer willing to rely on a participating organization's self-certification

[35] The Madrid Privacy Declaration, November 3, 2009, *available at* http://thepublicvoice.org/madrid-declaration/.
[36] Comments of EPIC, September 14, 2010, before the European Committee on Legal Cooperation, "Draft Recommendations on the Protection of Individuals with Regard to Automatic Processing Personal Data in the Context of Profiling, adopted June 1-4, 2010," The council of Europe, Plenary Meeting, October 11-13, 2010, *available at* http://epic.org/privacy/intl/coeconvention/EPIC_COE_108_Appendix_Comments.pdf.
[37] Report, *supra* note 3 at 43.
[38] *Id.*
[39] US-EU Safe Harbor Framework, *available at* http://www.export.gov/safeharbor/.
[40] Michael Mahoney, "Report: U.S. Businesses Fail 'Safe Harbor; Data Privacy Test," August 17, 2001, *available at* http://www.ecommercetimes.com/story/12875.html.
[41] *Id.*

as reflected on the Department of Commerce's Safe Harbor website."[42]

When the Federal Trade Commission took action against U.S. firms that incorrectly claimed current Safe Harbor certification, the only penalty imposed was that the companies may not in the future misrepresent membership in any privacy, security, or other compliance program.[43] Many in Europe and the U.S. have criticized the safe harbor arrangement[44] and in 2005, EPIC stated that "most companies . . . tried to avoid compliance in any possible way and exploit loopholes of the safe harbor. And although they are compliant with the letter of the Safe Harbor, they haven't complied with the spirit."[45]

4. *Effective Privacy Regulations Will Promote Privacy Innovation*

The Commerce Department Report assumes that privacy stands as an obstacle to innovation. But this is wrong for several reasons. First, without privacy technology such as public key encryption, there would simply be no commercial Internet. It would not be possible to conduct commerce without HTTPS, to take payments, or to transfer credit card numbers. Public key encryption is a significant example of a privacy-enhancing technique that allowed businesses to innovate in a myriad of ways that would have been unthinkable without the encryption system. Online commerce as we know it, including

[42] World Privacy Forum, "The US Department of Commerce and International Privacy Activities: Indifference and Neglect," November 22, 2010, *available at* http://www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf.
[43] "FTC Settles with Six Companies Claiming to Comply with International Privacy Framework," October 6, 2009, *available at* http://www.ftc.gov/opa/2009/10/safeharbor.shtm.
[44] *See* European Justice Commission, "Safe Harbor Decision Implementation Study," October 22, 2004, *available at* http://ec.europa.eu/justice/policies/privacy/docs/studies/safe-harbour-2004_en.pdf.; Chris Connoly, Galexia, "US Safe Harbor – Fact or Fiction?" Privacy Laws and Business International, Issue 96, December 2008, *available at* http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/.
[45] Nikki Swartz, "US Companies Not Complying with EU Safe Harbor Rules," Information Management Journal, Jan/Feb 2005, *available at* http://findarticles.com/p/articles/mi_qa3937/is_200501/ai_n9474038/.

Amazon, eBay, iTunes, and secure internet e-mail, would all not exist if not for privacy techniques.[46]

Second, privacy protection promotes trust and confidence in the deployment of new services.[47] In the absence of clear privacy safeguards, public protest and consumer backlash becomes the norm. That is the history of Facebook and privacy.[48]

Third, privacy regulation can promote the development of privacy solutions that help safeguard consumers and promote innovation. As consumers place more of a value on privacy, companies compete over privacy, which leads to innovation.[49] The Commerce report touches on this idea but does not really understand the concept.[50] In the Commerce view, these privacy-enhancing techniques are little more than links to inadequate privacy policies. What is required is a much deeper understanding of the relationship between regulation and innovation, one that does not start with such a heavy bias against the interests of the consumer. Incentives are necessary to promote privacy innovation; however, market-based incentives do not work – which is why regulatory incentives are needed.[51]

Privacy protection made possible the emergence of the telephone network as reliable basis for US businesses to operate across the across the country and for

---

[46] Marc Rotenberg, "Privacy and Innovation: History, Concepts, Future," talk at Yale Law School: Privacy and Innovation Symposium, October 29, 2010.
[47] *Id.*
[48] *See* EPIC: Facebook Privacy, *available at* http://epic.org/privacy/facebook/.
[49] *See generally,* M. Ryan Calo, "Unknown Unknowns: The Role of Innovation in Privacy," Yale Information Society Project, *available at* http://www.law.yale.edu/documents/pdf/ISP/Yale_ISP_Calo.pdf ("As Reputation Defender and TRUSTe can attest, privacy has become a business model in its own right.").
[50] Report, *supra* note 3 at 45-46.
[51] *See* Frank Pasquale, "Data and Power: From Individual Consent to Societal Transparency," Yale Information Society Project, *available at* http://www.law.yale.edu/documents/pdf/ISP/PasqualeReciprocalTransparency.pdf (describing a "broken market" for privacy, leading to the conclusion that "given these patterns of industry practice and consumer behavior, regulation will be more effective than waiting for markets to provide varied privacy options…given the frequently abstract 'benefits' that privacy…affords, they are often traded away for competitive economic advantage.").

individuals to share personal information with friends and family. Privacy protection made possible the adoption of email. Privacy protection will be critical to the success of the President's plan to place electronic health records on the Internet.[52]

It is worth noting that in the related field of alternative energy, regulation has played a critical role in promoting new cleaner technologies and growing successful new industries,[53] and those countries that have managed to make the clearest commitment through regulatory structures and incentives are the ones now capturing the hi-tech markets of the 21st century.

On this central point concerning the relationship between regulation and innovation, the Commerce Report draws exactly the wrong conclusion.

Conclusion

For the foregoing reason, the EPIC recommends that the Department of Commerce work to establish an independent US privacy agency, comprehensive federal privacy laws based on Fair Information Practices, and a strong international framework for privacy protection that does not rely on Safe Harbor" agreements. This Report contains some of the elements of an Administration plan for privacy protection, but until the government's focus shifts from self-regulation to enforcement, it will be impossible to achieve meaningful privacy protection for American consumers and users of Internet-based services.

---

[52] *See generally,* Sharona Hoffman, "Privacy and E-Health Innovation," Yale Information Society Project, *available at* http://www.law.yale.edu/documents/pdf/ISP/Hoffman_Yale_EHR.pdf.

[53] *See generally,* Matt Leibowitz, "Government Regulations Needed to Solve Online Privacy Battle," Security News Daily, January 24, 2011, *available at* http://www.securitynewsdaily.com/government-regulations-needed-to-solve-online-privacy-battle--0443/; National Highway Traffic Safety Administration, "Corporate Average Fuel Economy (CAFE) Overview," *available at* http://www.nhtsa.gov/cars/rules/cafe/overview.htm.

Marc Rotenberg
EPIC President

Sharon Goott Nissim
EPIC Consumer Protection Fellow