

Subject: Perspectives of the Center for Democracy and Technology
From: Ari Schwartz, Center for Democracy and Technology, 202-637-9800,
ari@cdt.org
To: Internet Caucus Advisory Committee

Briefing Materials on the European Union Directive on Data Protection

This material may be found online at: <http://www.cdt.org/privacy/eudirective/>

EU Documents

1. [Directive 95/46/EC](http://www.cdt.org/privacy/eudirective/EU_Directive_.html) on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data
http://www.cdt.org/privacy/eudirective/EU_Directive_.html
2. [News Release](http://europa.eu.int/comm/dg15/en/media/dataprot/news/925.htm): Directive on Data Protection Enters Into Effect
<http://europa.eu.int/comm/dg15/en/media/dataprot/news/925.htm>
3. [Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive](http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp12en.htm)
<http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp12en.htm>
4. [Working Document](http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp7en.htm): "Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?"
<http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp7en.htm>

Background

1. A generic [Code of Fair Information Principles](http://www.cdt.org/privacy/privacy/guide/basic/generic.html)
<http://www.cdt.org/privacy/privacy/guide/basic/generic.html>
2. [OECD Guidelines](http://www.cdt.org/privacy//privacy/survey/oecdguidelines.html)
<http://www.cdt.org/privacy//privacy/survey/oecdguidelines.html>
3. [Public Records: Access, Privacy, and Public Policy: A Discussion Paper Prepared by Robert Gellman](http://www.cdt.org/privacy//privacy/pubrecs/pubrec.html)
<http://www.cdt.org/privacy//privacy/pubrecs/pubrec.html>

International Responses

Canada

1. ["The Protection of Personal Information,"](http://strategis.ic.gc.ca/virtual_hosts/e-com/english/privacy/632d2.html) a joint report by the industry and justice ministries.
http://strategis.ic.gc.ca/virtual_hosts/e-com/english/privacy/632d2.html
2. "Canada's New Approach to Privacy Standards" by Robert Gellman [not available online]

United States

3. [Privacy Elements Paper,"](http://www.ntia.doc.gov/ntiahome/privacy/6_5_98fedreg.htm) a proposal by the National Telecommunications and Information Administration of the Department of Commerce
http://www.ntia.doc.gov/ntiahome/privacy/6_5_98fedreg.htm

4. ["Options for Promoting Privacy on the National Information Infrastructure,"](http://www.ntia.doc.gov/ntiahome/privwhitepaper.html) a report by the Information Policy Committee of the National Information Infrastructure Task Force
<http://www.ntia.doc.gov/ntiahome/privwhitepaper.html>
5. [Report to Congress: "Privacy Online,"](http://www.ftc.gov/reports/privacy3/index.htm) a report by the Federal Trade Commission, [executive summary and introduction](http://www.ftc.gov/reports/privacy3/index.htm)
<http://www.ftc.gov/reports/privacy3/index.htm>
<http://www.ftc.gov/reports/privacy3/exeintro.htm>
6. "Recycled Self-Regulation Stance of US May Only Irk Europeans" by Robert Gellman [not available online]

United Kingdom

7. ["Implementing the EU Data Protection Directive,"](http://www.open.gov.uk/dpr/impeudir.htm) a discussion by the Data Protection Registrar
<http://www.open.gov.uk/dpr/impeudir.htm>

Interpretations

1. ["Paper 6: Individuals' Rights,"](http://www.open.gov.uk/dpr/paper6.htm) a comparison of pre- and post-directive privacy regimes in the UK
<http://www.open.gov.uk/dpr/paper6.htm>
2. Irish "Consultation Paper," sections concerning data controllers' obligations individuals' rights under the directive

Documents Discussed at the Briefing

1. CSA Standard CAN/CSA-Q830-96, Model Code of the Protection of Personal Information, [principles in summary](http://www.gov.mb.ca/mihac/eng/csa.html) [full text available from the [CSA](http://www.csa.ca) for CAN\$22]
<http://www.gov.mb.ca/mihac/eng/csa.html>
<http://www.csa.ca>
2. [Council of Europe Convention](http://www.coe.fr/eng/legaltxt/108e.htm) for the Protection of Individuals with Regard for Automatic Processing of Personal Data (ETS No. 108)
<http://www.coe.fr/eng/legaltxt/108e.htm>
3. [Discussion Paper 2: "Information Privacy Principles,"](http://www.knowledge-basket.co.nz/privacy/discpp/discpr2.htm) part of the review of the (New Zealand) Privacy Act 1993 by the New Zealand Privacy Commissioner
<http://www.knowledge-basket.co.nz/privacy/discpp/discpr2.htm>
4. "Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions," by Robert Gellman. IV Software Law Journal 200 [not available online]

New Links [added January 10, 2000]

1. [Background Information on the European "Privacy" Directive](http://europa.eu.int/comm/dg15/en/media/dataprot/backinfo/info.htm)
<http://europa.eu.int/comm/dg15/en/media/dataprot/backinfo/info.htm>
2. European Commission (Directorate General XV) - [Data Protection Working Party : Recommendation 3/97 : Anonymity on the Internet \(3 December 1997\)](http://www.netcaucus.org)

<http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp6en.htm>

3. Data protection applied to the telecommunications sector : [Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector](#)
<http://www2.echo.lu/legal/en/dataprot/protection.html>
4. European Commission (Directorate General XV) - [Data Protection Working Party : Working Document : Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries \(22 April 1998\)](#)
<http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp9en.htm>
5. European Commission (Directorate General XV) - [Data Protection Working Party : Second Annual Report \(30 November 1998\)](#)
<http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp14en.htm>
6. European Commission (Directorate General XV) - [Data Protection Working Party : Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government \(26 January 1999\)](#)
<http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp15en.htm>
7. European Commission (Directorate General XV) - [Data Protection Working Party : Working Document: Processing of Personal Data on the Internet \(23 February 1999\)](#)
<http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp16en.htm>
8. European Commission (Directorate General XV) - [Data Protection Working Party : Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware \(23 February 1999\)](#)
<http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp17en.htm>
9. European Commission (Directorate General XV) - [Data Protection Working Party : Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce on 19th April 1999](#)
<http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp19en.htm>
10. European Commission (Directorate General XV) - [Data Protection Working Party : Opinion 4/99 on the Frequently Asked Questions to be issued by the US Department of Commerce in relation to the proposed "Safe Harbor Principles" on the Adequacy of the "International Safe Harbor Principles", \(7 June 1999\)](#)
<http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp21en.htm>
11. European Commission (Directorate General XV) - [Data Protection Working Party : Working document on the current state of play of the ongoing discussions between the European Commission and the United States Government concerning the "International Safe Harbor Principles" \(7 July 1999\)](#)

<http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp23en.htm>

12. European Commission (Directorate General XV) - [Data Protection Working Party : Opinion 7/99 on the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions \(FAQs\) and other related documents on 15 and 16 November 1999 by the US Department of Commerce \(3 December 1999\)](#)
<http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp27en.htm>
13. European Commission (Directorate General XV) - [Status of implementation of Directive 95/46 in the 15 countries of the European Union](#)
<http://www.europa.eu.int/comm/dg15/en/media/dataprot/law/impl.htm>

Online Privacy Part 5: How Do US Privacy Protections Compare to Privacy Protections in Other Countries?

Subj: Online Privacy: Perspectives of Progressive Policy Institute
From: Shane Ham, Policy Analyst, Progressive Policy Institute, 202-608-1284, sham@dlcpipi.org
To: Internet Caucus Advisory Committee

Excerpt from the PPI's On-Line Privacy Standard: The Case for a Limited Federal Role In a Self-Regulatory Regime

We have reached a pivotal period in the short history of the emerging digital economy. Constant innovations in ever-lower-cost information technologies, coupled with increasingly widespread access to the Internet, have begun to yield significant economic and social benefits, both in terms of tremendous value added and reduced costs for citizens and consumers, and extraordinary opportunities for businesses. But the same technologies and market forces driving the development of the World Wide Web and enabling the spread of “electronic commerce” (e-commerce) have also added to concerns in the public mind about individuals’ ability to maintain their personal privacy. On the Web, it has become easier than ever for businesses to gather consumer information and use it for marketing purposes without individual consumers’ knowledge or consent, which some argue is unfair and even invasive. Others have raised more serious concerns about the possibility that personal information compiled in databases could be used in discriminatory ways, for example, by insurance companies or employers.

Some of the marketing practices in question are every-day occurrences, but it is arguable whether or not those practices constitute actual harms to consumers. Meanwhile, many of the more serious concerns about the potential damage individuals could face in an unregulated environment are only based on hypothetical scenarios. Nonetheless, surveys have found that a large majority of Americans (over 80 percent) feel they have “lost all control” over how companies use their personal information, with over 60 percent saying they do not believe their rights to privacy as consumers are adequately protected by law or business practices. **Note 1** To the extent these privacy concerns undermine consumer confidence in the Internet and in electronic commerce, they could retard the growth of a critical driver of the New Economy.

Even though e-commerce is still in its infancy, pressure is mounting for government action. The stakes in the debate are high because overly restrictive federal intervention could have a devastating effect on innovation in the rapidly evolving online world. On one side of the issue are many who would adhere to the early industry consensus that in all Internet-related matters, government should lay off. From this point of view, even industry self-regulation through consumer privacy protection programs such as those offered by TRUSTe and the Better Business Bureau’s subsidiary, BBBOnline, would be a move in the wrong direction. **Note 2** On the other side are privacy advocates who favor a comprehensive, top-down regulatory regime that would define and protect individual privacy rights in the Information Age—which is the approach the European Union (EU) took last October when it enacted its Directive on Data Protection.

In reality, it is simply too early in the development of e-commerce to know how self-regulatory programs will evolve, what kinds of solutions and challenges technological innovation will provide, or how significant the risks to privacy will be. In the absence of this information, no compelling case can be made for a kind of EU-style regulatory regime. Conversely, no compelling case can be made at this point for concluding that government should never play a role in regulating privacy on the Internet.

Ultimately, instead of an EU-style bureaucratic regulatory regime or a purely laissez faire approach, the Progressive Policy Institute (PPI) believes there can be a third way, providing more control over personal privacy for consumers while leaving businesses free to innovate and add value to the economy. The forces shaping the Web, by their very nature, allow (in fact, require) policy makers to take a more flexible approach to public policy challenges—to move beyond the false choice between all-out command-and-control models on the one hand and a complete lack of regulation on the other. In the case of privacy, technological innovation and market pressures effectively allow customized solutions to be developed to meet diverse individual preferences and needs. Thus, government can take a minimalist approach while supporting private sector self-regulation.

In PPI’s view:

— Congress should give self-regulation a chance to work. For now, Congress should not legislate consumer privacy protections in online transactions that don’t involve sensitive data like medical, financial, or

Online Privacy Part 5: How Do US Privacy Protections Compare to Privacy Protections in Other Countries?

children's information. It is simply too early in the development of e-commerce to risk creating a regulatory regime which could end up stifling innovation in the digital economy. Moreover, if privacy legislation were enacted now, it could potentially squelch the development and widespread adoption of privacy protection "best practices" in the private sector. For now, the proper role for government is to continue to investigate and prosecute deceptive business practices, while monitoring the development of e-commerce and thoroughly assessing the severity and pervasiveness of privacy abuses and actual harms to consumers.

– If after a significant trial period self-regulation is not adopted by a large share of Web sites engaged in e-commerce, if consumer concerns regarding privacy on the Internet do not diminish, and if a record of significant abuses emerges, then Congress should establish minimum privacy standards in transactions involving personal information. The right baseline standard to apply would be to require businesses to give consumers notice before gathering personal data by disclosing information practices in comprehensive privacy policy statements, and to require businesses to obtain consent by offering consumers the choice of opting out of any personal data transfers that aren't needed to complete a given transaction.

– Public policy should continue to encourage private sector leadership in consumer privacy protection. Any legislative approach should stipulate that participation in recognized self-regulatory programs would constitute full compliance with federally mandated minimum privacy standards. The purpose of minimum standards would be to allow consumers to expect consistency in their dealings with businesses and Web sites that don't participate in recognized self-regulatory programs.

Trade-Offs: Absolute Privacy vs. Free Markets

Thus far, the privacy debate has broken down primarily along bipolar lines, focusing on the implications of two very different types of solutions to personal privacy concerns: the consumer-focused, top-down regulatory model adopted in Europe under the European Union Directive on Data Protection; and the pure self-regulatory model favored by market advocates in the United States. The potential for a middle-ground alternative has been given considerably less attention. But an examination of the two extreme approaches reveals weaknesses with each, suggesting that a third way may in fact be the most appropriate course for public policy.

The EU Directive

The European Union began deliberations on the issue of personal data protection in the early 1990s—before the widespread use of the Internet—and finally adopted the Directive on Data Protection in October 1998. The directive is undeniably sweeping in scope, applying to all "processing" of "personal data," with only limited exceptions. **Note 13** "Personal data" is defined as any data that is identified with an individual (i.e., not including aggregated data), and "processing of personal data" includes essentially anything that can be done to, or with, the data.

The directive contains the following provisions:

– Personal data, in addition to being "processed fairly and lawfully," must only be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." Further, data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected." Data must be kept accurate and up to date, and must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected."

– Criteria for legitimate data processing are essentially as follows: personal data may only be processed if unambiguous consent is given, or if the processing is necessary for performance of a contract, if there is some other legal obligation, if it's "necessary in order to protect the vital interests of the data subject," or for the public interest, though individuals retain the right to object in such cases.

– Except in cases of similarly specific exceptions, all personal data relating to race, ethnicity, political opinions, religion, trade-union membership, health, or sex life are considered sensitive and are strictly protected.

– "Controllers" of data are to provide individuals access to their data "at reasonable intervals and without excessive delay or expense." Access includes queries as to whether data exist at all, if so what types records exist, what the data is being used for, by whom (i.e., third party recipients), the "logic" of any automatic data processing, and the ability to rectify errors not only with the primary controller but also with notification to any third parties the data may have been passed on to.

– Controllers of data are further required to take "appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network."

Online Privacy Part 5: How Do US Privacy Protections Compare to Privacy Protections in Other Countries?

— Privacy standards set under the directive are administered and enforced in the member states by governmental privacy bodies, which have investigative powers, powers of intervention, and power to engage in legal proceedings.

— Businesses or other organizations wanting to gather or process individually identifiable data are required to either first notify the government privacy authorities, specifying the purposes of the data processing, the categories of data subject, any third parties to whom the data will be disclosed; or they may appoint an internal data protection official to ensure compliance with the directive, and to keep a register of all data processing operations.

As matters of general principle, the dictates of the EU Directive are not entirely unlike the policies designed by some of the leading self-regulation programs in United States, which tend to stress notice, choice, access, and security in privacy policies for consumers, with recourse mechanisms for violations. But unlike the efforts of industry groups in the United States, the EU Directive is not voluntary; there is no opportunity for companies to avoid the system. And whereas in current U.S. law what constitutes “fair” practices in transactions involving personal data is somewhat ambiguous, standards are codified in each European Union member state.

In the United States, critics of the EU Directive have argued that it will be an enormous impediment to innovation in the rapidly evolving digital economy. They ask: How can you possibly expect companies operating in “Web years”—accountable to investors on a quarterly basis—to register and get approval from some government privacy authority for every new data processing practice they want to develop or implement? Intelligent self-regulation could more readily allow much-needed flexibility. Critics argue the EU Directive could potentially have severe consequences for some forms of electronic commerce, particularly business-to-consumer transactions over the Web when the Web site is located in the United States and the consumer is a citizen of an EU member state. **Note 14** Business-to-business and internal business transactions could also potentially be affected, including such mundane internal data transmissions as those involving human resource data in a U.S.-based multinational company with employees in Europe. **Note 15** In the end, when the line items are all added up (for the cost of organizational transition, paring down some operations, the hiring of experts, etc.), the cost of compliance could be quite substantial. **Note 16** The directive has not yet been fully implemented, however. So as is the case with many privacy advocates’ worst fears, many of the EU Directive’s critics’ concerns are hypothetical.

There is a fundamental distinction between the European view of privacy and the traditional American view that must be considered in the context of any policy discussion about privacy: America does not have the general presumption that data should be used only for the purposes for which they are gathered. **Note 17**

This is a particularly important distinction in the context of the new value proposition that drives a great deal of the innovation in the New Economy: businesses are often able to add value for consumers in unexpected ways, often largely as a function of the quality and quantity of consumer data at their disposal. Undue restrictions on data processing could therefore amount to a counterweight on economic progress. It is not hard to imagine, for example, the end result of a regulation like Article 18 of the EU Directive, requiring businesses to notify supervisory authorities before carrying out specific sorts of data processing: the process could slow or inhibit the development of innovative products, services, and business practices, thus stifling economic progress and depriving consumers and citizens of the benefits.

Perhaps the single most powerful argument against a uniform, top-down regulatory regime for privacy protection online is that the core forces driving the New Economy enable more flexibility. Technology and markets can offer customized solutions for individuals’ privacy needs.

Blanket solutions may have been all that were achievable in the old economy, but the New Economy offers solutions like Platform for Privacy Preferences (P3P) and Free-PC.com. P3P is an emerging technical standard for creating privacy on a customizable basis for consumers browsing the Web. **Note 18** In a nutshell, P3P software could allow users to ensure certain privacy standards in their online dealings by setting up their computers to negotiate privacy agreements with Web sites. **Note 19** Free-PC.com **Note 20** is a recently-launched enterprise with a core business model based on the information-for-value proposition made possible between businesses and consumers in the New Economy. Free-PC.com literally offers free computers for two-year periods in exchange for detailed personal information (including demographic data such as age, household income, family status, etc., and information about personal tastes and interests). The information is used to target advertising to a frame around the perimeter of the user’s computer screen. Some privacy advocates have misleadingly argued this is like putting a surveillance camera in someone’s den. But the truth is that the Free-PC.com

Online Privacy Part 5: How Do US Privacy Protections Compare to Privacy Protections in Other Countries?

business model simply offers consumers the choice to trade something of value (their personal information and preferences) for something else of value (a computer). As long as the terms of deals like these are clear, conspicuous, and unambiguous, they are great examples of how the market can provide different arrangements to suit individual privacy preferences, while helping spread access to the Internet.

The Clinton Administration Position and Industry-led Efforts in the United States

In 1980, five years before the National Science Foundation began connecting the major U.S. supercomputing sites together to form the original backbone of the Internet, the member countries of the Organization for Economic Cooperation and Development (OECD) drafted guidelines on the protection of privacy in transborder flows of personal data. **Note 21** The premise of the document was the realization that “the development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, had made it necessary to consider privacy protection in relation to personal data.” The OECD further recognized that it would be critical to reconcile “fundamental but competing values such as privacy and the free flow of information.” But it also recognized that domestic privacy protection legislation may hinder information flows in an economically counterproductive way. With that in mind, the OECD outlined a set of general principles to be used as a framework for minimum standards in privacy policy making. The Clinton Administration since has built on the OECD guidelines, emphasizing consumer awareness, choice, data security, consumer access, verification, and recourse mechanisms, but also stressing private sector leadership and self-regulation.

Today, industry groups have established a number of self-regulated privacy protection programs following the Administration’s precepts. One example is TRUSTe, **Note 22** a non-profit, corporate-sponsored seal program officially launched in June 1997, which requires participants to provide consumers with notice and disclosure of data collection practices; choice and consent over how their personal information is used and shared; data security and quality assurances; and access provisions to safeguard, update, and correct personally identifiable information. TRUSTe periodically reviews participating sites to ensure compliance with posted privacy practices and program requirements, and for any changes to privacy statements. Additionally, reviewers “seed” sites to test them for compliance, a process of submitting unique user information to monitor outcomes. Finally, in the event of consumer complaints or program participant misconduct, TRUSTe offers a dispute resolution process, which can include expulsion from the program and ultimately referral to federal authorities if necessary.

The Council of Better Business Bureaus launched another privacy program in March 1999 through its BBBOnline subsidiary. **Note 23** Like TRUSTe, BBBOnline offers a seal of approval to businesses that post online privacy policies that meet required “core” principles, such as disclosure, choice, and security. The two programs are each unique in a number of ways, but both are based on essentially the same idea: participating members display a seal on their Web sites to reassure consumers that their personal information will not be abused.

Participants in the BBBOnline program pay an annual fee ranging from \$150 for businesses with annual sales less than \$1 million, to \$3,000 for businesses with annual sales greater than \$2 billion. BBBOnline requires privacy policy statements to make certain disclosures depending on a company or organization’s information practices (for example, if a company merges personally identifiable information with data from third parties, BBBOnline would require the company to disclose that practice in its privacy policy), it verifies companies’ internal information practices to ensure compliance with the program’s standards, and it offers dispute settlement. And like TRUSTe, non-compliance on the part of program participants can result in withdrawal of the seal of approval, negative publicity, and referral to government enforcement agencies.

Privacy advocates and proponents of European-style regulation offer a number of criticisms of these types of programs, some of which are conspicuously weak. For example, the BBBOnline program was criticized for being ineffective even before its actual debut. Another criticism has been that in the first year and a half of TRUSTe’s existence, surveys have shown that consumers’ privacy concerns have risen. But here, again, it is important to note that TRUSTe, like BBBOnline, is a new program that is still signing up members. But that fact aside, consumers’ privacy concerns at this point can largely be attributed to a rapidly increasing first-time awareness coupled with a shallow understanding of the online world. It is important to remember that the Internet and all that it entails is all still very new; millions of people are just beginning to tune in and their confusion is understandable.

But this speaks more to the need for public education campaigns than a lack of effectiveness of new self-regulatory privacy protection programs. More needs to be done to educate consumers to look for Web sites with posted privacy policies—or better yet, to look for Web sites that display the seals of leading privacy

Online Privacy Part 5: How Do US Privacy Protections Compare to Privacy Protections in Other Countries?

protection programs—and to encourage them to use other sites with caution. For example, consumers should avoid giving sites without substantive privacy policies their credit card numbers, email addresses, or postal addresses. (And when they visit such sites, consumers can also set their browsers not to accept cookies.)

There is, however, one criticism of self-regulatory privacy protection programs that is inescapable. There is no denying that their chief shortcoming is the fact that they are voluntary. As long as that is the case, there will always be companies that choose not to participate. So what, if anything, should policy makers do about them?

Note 1. Louis Harris & Associates, Inc. and Dr. Alan F. Westin, *E-Commerce & Privacy: What Net Users Want* (Hackensack, NJ: Privacy & American Business and Price Waterhouse, LLP, June 1998).

Note 2. <http://www.cato.org/pubs/pas/pa-295es.html>.

Note 13 Peter Swire, "Of Elephants, Mice, and Privacy: International Choice of Law and the Internet," *The International Lawyer*, Vol. 32, no. 4 (winter, 1998), pp.991-1025.

Note 14 Peter P. Swire and Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Washington, DC: Brookings Institution Press, 1998).

Note 15 *Ibid.*

Note 16 Swire and Litan, *op cit.*

Note 17 Swire and Litan, *op cit.*

Note 18 <http://www.w3.org/P3P/Overview.html>.

Note 19 <http://www.w3.org/P3P/nutshell.html>.

Note 20 <http://www.Free-PC.com>.

Note 21 <http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM>.

Note 22 <http://www.truste.org>.

Note 23 <http://www.bbbonline.com>.

Online Privacy Part 5: How Do US Privacy Protections Compare to Privacy Protections in Other Countries?

Subj: Online Privacy: Perspectives of Privacy Right
From: Paul Sholtz, Chief Technology Officer, PrivacyRight Inc., c/o Amy Hanson, 703-299-9470
To: Internet Caucus Advisory Committee

How do US Privacy Protections (if any) compare to Privacy Protections in Other Countries?

In general, the EU has far more comprehensive data protection laws than the US. Most EU regulations are modeled on the Code of Fair Information Practices, which was in fact conceived of, although never adopted, in the US. The EU Directive is unique in that it restricts trade with countries like the US that do not diligently protect privacy. In 1999, this provision nearly led to the first trans-Atlantic Internet trade war. Both sides have tentatively agreed to a compromise solution, allowing US companies to continue operating in "safe-harbor" with the EU, while they adopt more comprehensive data protection policies.