OUTSOURCING PRIVACY:
Countries Processing U.S. Social Security Numbers, Health Information, Tax Records Lack Fundamental Privacy Safeguards

Including

International Rankings of Privacy Protections in 20 Countries and the European Union

---

A Staff Report
prepared at the request of
Edward J. Markey
U.S. House of Representatives
Revised September 2005

OUTSOURCING PRIVACY:

Countries Processing U.S. Social Security Numbers, Health Information, Tax Records Lack Fundamental Privacy Safeguards

Introduction

The *New York Times* recently suggested that 2005 might be viewed historically as "the year of the consumer privacy breach"[1] in recognition of the more than 50 million American consumers who have seen their personal information lost, stolen or sold to thieves by third parties. But this may only be the early tip of the iceberg of a problem that is going global. The telecommunications revolution now makes it possible to process U.S. data, read U.S. x-rays, or answer U.S. consumer complaints from low-wage foreign countries where privacy protections are weak or non-existent. This report reviews the relative strength of the privacy regimes in countries to which U.S.-based companies are now turning to maximize profits in a competitive global economy. It asks whether what is good for profits is also good for privacy. Americans would not travel to a country without first inoculating themselves against foreign diseases. Why then would Americans want their data going to a foreign country without the proper privacy protections? In the absence of such proper privacy protections, outsourcing sensitive data jeopardizes U.S. confidence in information outsourcing.

Modern electronic communication has collapsed geographical boundaries at the expense of personal privacy boundaries. American tax records, medical records, credit card information, and insurance data are no longer for American eyes only. Data handlers from Brazil to India now have access to Social Security numbers, credit histories, employees' records, bank investment information, and more. The low cost of labor, management, and infrastructure in Asia and Latin America has led to an increase in offshore business processing. Spending for global sourcing of computer services and information processing is expected to grow at a compound interest rate of almost 26%, from approximately $10 billion in 2003 to $31 billion in 2008.[2] More spending means more international data exchanges—exchanges which are, in many cases, insecure and vulnerable to theft, unauthorized access, and misuse.

In 2001, Indian workers at Ohio-based Heartland Information Services, threatened to release confidential medical records online unless they received a cash payment from the company.[3] In 2003, a Pakistani medical transcriber, subcontracting with the University of California at San Francisco (UCSF) medical center, threatened to do the same.[4] Neither

---

[1] Dash, Eric. "Europe Zips Lips; U.S Sells Zips." *New York Times.* Section 4, Page 1. August 7, 3005.

[2] Global Insight. "Executive Summary: The Impact of Offshore IT Software and Services Outsourcing on the U.S Economy and the IT Industry."

[3] Public Citizen. "Offshoring and Privacy Protection." http://www.citizen.org/trade/offshoring/privacy/index/cfm

[4] Lazarus, David. "A Tough Lesson on Medical Privacy." *San Francisco Chronicle.* October 22, 2003. Page A1.

India nor Pakistan has national data privacy laws compelling companies to implement basic data privacy safeguards. Indeed, of the 19 countries and one region to whom American companies predominantly offshore, thirteen offer *less* data privacy to consumers than the United States. And only six countries and one region (the EU) provide more data privacy to consumers than the United States. [5] More must be done to ensure that the data privacy protections American citizens enjoy do not end at our borders. American consumers must not be told, in effect, to "check your privacy at the shore."

Rationale

Consumers deserve not only to know where their personal information is going, but also to have confidence that their sensitive information is collected, used, and stored safely, wherever that may be. Moreover, regulators need to know whether their enforcement of privacy protections mandated here at home is being rendered futile by the trend to send data for business processing to countries with little or no privacy protection. In general, the principle of "Knowledge, Notice, Not My Info" should apply when it comes to transfer of American consumers' personal information:

- **Knowledge:** Consumers should be told that their financial, medical, credit or other personally-identifiable, sensitive information may be sent overseas.
- **Notice:** If their information is actually transmitted overseas, consumers should be notified.
- **Not My Info:** Consumers should have ability to block the transfer of their information, and they should not be penalized through higher charges or denial of service if they choose to have their information processed domestically.

This study examines data privacy and consumer protection laws in 19 countries and one region (the EU) and compares each country's statutory requirements with those in the United States. Such a comparison not only tells us where the United States stands with regard to the rigor and comprehensiveness of its data privacy laws, but more importantly, how the rest of the world fairs in comparison to the United States.

Methodological Overview

Consumers and government officials will only be able to make judgments about the adequacy of a particular country's privacy protection regime if we take steps to develop a method of ranking countries with respect to major data privacy principles. This report undertakes such a ranking by focusing on seven key tests of privacy protection: notice, choice, transborder transfer, access, security, integrity, and enforcement.

Country Selection

Countries were included in the study if U.S. companies currently offshore business processing to that location *or* if there is a high likelihood that such offshoring will occur in the future. Of the 19 countries studied, eleven were identified by the firm A.T. Kearney as being among the best candidates for offshore business processing, and not surprisingly,

[5] Revised from August 2005 version to reflect the addition of Hong Kong to the "adequate" data privacy regime list.

home to US-based affiliates.[6] The remaining eight countries are located in the Asia-Pacific region, a region experiencing substantial growth in the service industry. In a September 2005 Economist Intelligence Unit survey of 500 senior executives, Hong Kong, Singapore, Malaysia, and Thailand emerged as attractive offshoring locations. Bangladesh and Pakistan also received high rankings. Eighty-one of the 100 executives questioned in 2005 for a London-based TPI's survey said they will shift business to overseas countries in the next two to three years. About 75 percent of the executives questioned use India as an offshore destination, 28 percent use Central and Eastern Europe and a quarter use China, according to the report.

Principle Selection

The principles used to judge the adequacy of each country's privacy regime are taken from the EU Data Privacy Directive. The EU is generally regarded to have developed the most comprehensive and effective data protection model. Even the United States, through the adoption of the Safe Harbor Agreement, has agreed to the principles underlying the EU Directive. These principles define protected data as that which is obtained fairly and lawfully; used for a specified and limited purpose; adequate and relevant to that purpose; current and accurate; accessible to the data subject; stored securely; and destroyed once used.

Principles do little to protect consumers from data theft or misuse unless they are fully practiced and enforced. International guidelines—with the exception of the EU Directive—merely *recommend* how public and private organizations should handle personally identifiable information. The Organization for Economic Co-operation and Development's 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, signed by all member countries, were the first to outline collectively agreed upon data privacy principles. Principles of notice, security, data quality, and access were embraced. The EU Data Privacy Directive, revised in 2000, goes a step further. Principles of choice, third-party transfer, and enforcement are added. More importantly, the Directive *prohibits* the transfer of data to countries without adequate privacy laws and *mandates* enforcement through the establishment of an independent data privacy commission. Both the transfer and enforcement provisions have significantly shaped today's international data privacy landscape. Asian and Latin American countries, including Japan and Argentina, have utilized the EU model as a template when crafting national data privacy legislation. It makes sense, then, to turn the EU principles into a comparative metric. The seven EU principles include:

- **Notice** such that organizations inform individuals about the *purposes* for which it collects information about them; what an individual's *rights* are with regards to choice and access, and the types of *third parties* to which it discloses information.
- **Choice** such that organizations offer individuals the opportunity to opt-in, or at the very least opt-out, of data collection and storage.
- **Transborder Transfer** such that personal data is only transferred to countries with a similar or "*adequate"* level of privacy protection. Personal information is only disclosed to third parties consistent with the principles of *notice* and *choice.*

[6] The eleven countries include: India, Canada, Brazil, Mexico, Philippines, Hungary, Ireland, Australia, Czech Republic, Russia, and China.

- **Security** such that organizations take reasonable steps to prevent the loss, unauthorized access, destruction, use, modification, or disclosure of personal data.
- **Data Integrity** such that organizations take reasonable steps to ensure that data is accurate, complete and current.
- **Access** such that individuals have reasonable access to personal information about them that an organization holds and are able to correct or amend any inaccurate information.
- **Enforcement** such that an independent supervisory authority exists to ensure that organizations uphold the principles of notice, choice, transborder transfer, security, data integrity, and access. Individuals also have the right to file complaints and directly pursue litigation.

Finally, while the EU directive applies to both the public and private sector, not every country has enacted a comprehensive law. The seven principles will have a limited impact unless widely implemented. Thus we have included **comprehensive legislation** as an additional measure of adequate data protection.

Point System and Rankings

Country rankings were calculated by assigning points for national consumer protection and data privacy legislation aligned with the principles of **notice, choice, transborder transfer, access, security, integrity, and enforcement.** Countries with **comprehensive legislation**—legislation applicable to both the public and private sectors—received an additional point. This point system was structured according to the European Union's Directive on Data Privacy, the most detailed data privacy code to date. Countries could score a total of 17 points. Composite scores were subsequently translated into letter grades. Number scores of 0-3 were coded as the letter "F;" 4-7 as "D;" 8-11 as "C;" 12-14 as "B;" and 15-17 as "A." Laws from 19 countries, as well as from the United States and the EU, were compared against the seven selected principles. Countries were chosen based on the likelihood of US data transferal to that location. Research focused solely on each jurisdiction's legislative response, if any, to data privacy concerns. In other words, the study looked only at what is on paper and did not assess everyday practice.

In short, each country was ranked using the principles and the point system described above and summarized in the table below.

Principle	**Description**	**Assignable Points** ***Law(s) include language on:***
Notice	Organizations inform individuals about the *purposes* for which it collects information about them; what an individual's *rights* are with regards to choice and access, and the types of *third parties* to which it discloses information.	3: purpose, rights, and transfer 2: two of the above 1: one of the above 0: no language on notice
Choice	Organizations offer individuals the opportunity to opt-in, or at the very least opt-out, of data collection and storage.	3: opt-in only 2: both opt-in and opt-out 1: opt-out only 0: no language on choice
Transborder Transfer	Personal data only transfer to countries with a similar or "*adequate"* level of privacy protection. Personal information is only disclosed to third parties consistent with the principles of *notice* and *choice.*	3: adequacy req., notice, choice 2: two of the above 1: one of the above 0: no language on transfer

Security	Organizations take reasonable steps to prevent the loss, unauthorized access, destruction, use, modification, or disclosure of personal data.	2: protection from loss/misuse and unauthorized access 1: one of the above 0: no language on security
Data Integrity	Organizations must take reasonable steps to ensure that data is accurate, complete, and current.	1: accuracy expected 0: no language on integrity
Access	Individuals have reasonable access to personal information about them that an organization holds and are able to correct or amend any inaccurate information.	1: right to view/correct data 0: no language on access
Enforcement	An independent supervisory authority is established to ensure that organizations uphold the principles of notice, choice, transborder transfer, security, data integrity, and access. Individuals also have the right to file complaints and directly pursue litigation.	3: independent supervision *and* direct litigation 2: independent supervision *or* direct litigation 1: governmental oversight only 0: no language on enforcement
Comprehensive?	General law exists governing the collection, use, and dissemination of personal information by both the public and private sectors.	1: comprehensive legislation 0: no comprehensive legislation

Results

As shown below, the results of ranking countries by privacy protection regimes reveals the extreme vulnerability of U.S. citizens to privacy breaches when personally identifiable data is sent to foreign countries to be processed. In fact,

- **Of the twenty countries and regions examined, five--Australia, Canada, Czech Republic, Hungary and Japan--plus the European Union, have privacy regimes that are stronger than the U.S.**

INTENRATIONAL PRIVACY RANKINGS	
	COMPOSITE GRADE
Canada	**A**
EU	**A**
Hungary	**A**
Australia	**B**
Czech Republic	**B**
Japan	**B**
Hong Kong	**B**[7]
US	**C**
Korea	**C**
Taiwan	**D**
Thailand	**D**
India	**D**[8]
Singapore	**D**
Mexico	**F**
Brazil	**F**
Bangladesh	**F**

[7] Revised from August 2005 version to reflect Hong Kong's Personal Data Privacy Ordinance.
[8] Revised from August 2005 version to reflect India's recently passed Right to Information Act of 2005.

China	**F**
Malaysia	**F**
Pakistan	**F**
Philippines	**F**
Russia	**F**

**See Appendix 1 for Complete Ranking Chart*

- **Unlike the European Union, the United States has failed to authorize any governmental agency to promulgate a common set of privacy standards that protect consumers when companies decide to send personally-identifiable information and data to entities in foreign host countries for processing.**

- **Of the 11 countries identified by AT Kearney as the most attractive targets for US offshoring, 6 of them--India, Brazil, Mexico, Philippines, Russia and China--have privacy regimes that are either weak or non-existent.**

PRIVACY GRADES OF COUNTRIES TO WHICH U.S. COMPANIES ARE MOST LIKELY TO OFFSHORE	
	COMPOSITE GRADE
Canada	**A**
EU (Ireland)	**A**
Australia	**B**
Czech Republic	**B**
US	**C**
India	**D**
Mexico	**F**
Brazil	**F**
China	**F**
Philippines	**F**
Russia	**F**

Next Steps

As outsourcing trends continue so too will unprotected data transferal. To ensure adequate privacy protection, American companies need a convenient method for judging whether the privacy protections offered by a potential host are at least as strong as the privacy protections their customers enjoy at home. The principles of notice and choice must also apply to information shipped abroad. Consumers deserve to know where their data is going and to decide if they want their data going to that location, particularly if that location affords fewer privacy protections than the United States.

Using a ranking system such as the one used in this report, businesses are empowered to advise consumers that their personally identifiable information may be transmitted to foreign affiliates or subcontractors. If those affiliates and subcontractors reside in jurisdictions with adequate privacy protection, such notice should be sufficient. However, if affiliates and subcontractors are located in a country without adequate privacy protection, consumers will want and deserve the right to opt-in. This approach could be adopted

voluntarily by industry associations or particular companies choosing to lead in the area of privacy protection.

However, the depth and speed of outsourcing data processing to foreign countries from the U.S. suggests that legislation is needed to provide a level playing field and a common understanding of obligations and rights. Two members of Congress – Rep. Ed Markey (D-MA) and Sen. Hillary Clinton (D-NY) have proposed legislation to accomplish these purposes. The Safeguarding Americans from Exporting Identification Act (House bill H.R. 1653, Senate bill S. 810) would authorize the Federal Trade Commission to determine whether the consumer privacy protections in a potential offshore host were "adequate" or "inadequate." Data could be sent freely to host countries with "adequate" protections (the consumer could only opt out), but data transfer would be restricted to host countries with "inadequate" protections (the consumer could opt in.)

For more information, visit www.house.gov/Markey.

Sources

General

- A.T Kearney. "Selecting a Country for Offshore Business Processing." http://www.atkearney.com/shared_res/pdf/Where_to_Locate_S.pdf
- Greenleaf, Graham. "A Tentative Start to the Implementation of APEC's Privacy Framework." *Privacy Laws & Business: Data Protection and Privacy Information Worldwide.* Issue 78, June/July 2005.
- Fitzgerald, Jay. "Known Around the world; Private Records May Be at Risk." *Boston Herald.* November 30, 2003, p. 027.
- International Safe Harbor Principles. http://ita.doc.gov/td/ecom/shprin.html.
- Organization for Economic Co-Operation and Development. "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." http://www.oecd.org/documentprint/0,2744,en_2649_34255_1815186_1_1_1_1,00.html
- TPI. The Global Sourcing Advisors. Quarterly Sourcing Developments Index. http://www.tpi.net/pdf/2Q05%20TPI%20Index%20Presentation.pdf
- United States Department of Commerce. "International Data Protection Legislation." Provided by Jeff Rohlmeier, July 11, 2005.

Asia and the Pacific

- Caslon Analytics. "Privacy Guide: Asia." http://www.caslon.com.au/privacyguide6.htm
- G&A Management Consultants Limited. "Hong Kong Personal Data (Privacy) Ordinance." http://www.privacy.com.hk/privkita.html
- Office of the Privacy Commissioner for Personal Data, Hong Kong. "Chapter 486: Personal Data (Privacy) Ordinance." http://www.pco.org.hk/english/ordinance/section_19.html
- Jefferson Data Strategies, Privacy Council. "Regulatory Compliance-Japan's Personal Information Protection Act." http://www/privacycouncil.com/adSvs_japan.php
- Baker and McKenzie. "Japanese Personal Information Protection Law. May 23, 2003.
- Privacy International. "Privacy and Human Rights 2003: Republic of [South] Korea." http://www.privacyinternational.org/survey/phr2003/countries/southkorea.htm
- Privacy International. "Privacy and Human Rights 2003: Republic of China [Taiwan]." http://www.privacyinternational.org/survey/phr2003/countries/taiwan.htm
- Privacy Exchange. "Computer-Processed Personal Data Protection Law." http://www.privacyexchange.org/legal/nat/omni/taiwan.html. August 11, 2003.
- Privacy International. "Privacy and Human Rights 2003: Kingdom of Thailand." http://www.privacyinternational.org/survey/phr2003/countries/thailand.htm
- Official Information Commission's Office. "Chapter III: Personal Information." http://www.oic.thaigov.go.th/eng/statue/Statutedata.htm

Canada

- Caslon Analytics. "Privacy Guide: North American Legislation and Development." http://www.caslon.com.au/privacyguide7.htm
- Wilson, Patricia. "Privacy Law in Canada." Osler Publicans. http://www.osler.com/resources.aspx?id=8686. January 15, 2003.
- Canada Department of Justice. "Personal Information Protection and Electronics Act." http://laws.justice.gc.ca/en/p-8.6/93196.html August 31, 2004
-

Czech Republic

- Privacy International. "Privacy and Human Rights 2003: Czech Republic Summary." http://www.privacyinternational.org/survey/phr2003/countries/czech.htm '
- Office for Personal Data Protection. "Consolidated Version of the Personal Data Protection Act 101." http://www.uoou.cz/eng/101_2000.php3. April 4, 2000

European Union

- Caslon Analytics. "Privacy Guide: EU Law and Developments." http://www.caslon.com.au/privacyguide4.htm
- Official Journal of the European Communities. "Regulation (EC) No 45/2001 of the European Parliament and of the Council." December 18, 2000.
- Data Protection European Commission. "Overview of Third Countries, Press Releases." http://europa.eu.int/comm/justice_home/fsj/privacy/thirdcountries/index.html

Mexico

- Privacy International. "Privacy and Human Rights 2003: United Mexican States." http://www.privacyinternational.org/survey/phr2003/countries/mexico.htm

Russia

- Privacy International. "Privacy and Human Rights 2003: Russian Federation." http://www.privacyinternational.org/survey/phr2003/countries/russianfederation.htm

United States

- Privacy International. "PHR2004: The United States of America." http://www.privacyinternational.org/article.shtml?cmd[347]=x-3547-83512.
- United States Department of Justice. "The Privacy Act of 1974." http://www.usdoj.gov/04foia/privstat.htm