DEPARTMENT OF COMMERCE
International Trade Administration

Development and Implementation of Cross-border Privacy Rules in the Asia Pacific Economic Cooperation Group (APEC)

Comments of the Electronic Privacy Information Center (EPIC), the Consumer Federation of America, the National Consumers League, the Privacy Rights Clearinghouse, the Privacy Times, the U.S. Public Interest Research Group and the World Privacy Forum on Behalf of U.S. Civil Society Organizations

FEDERAL RULEMAKING

Pursuant to a notice published in the Federal Register on May 22, 2006, the Office of Technology and Electronic Commerce solicited comments on the development and implementation on "cross-border privacy rules" in the Asia Pacific Economic Cooperation Group (APEC).[1] The Electronic Privacy Information Center (EPIC), the Consumer Federation of America, the National Consumers League, Privacy Rights Clearinghouse, the Privacy Times, the U.S. Public Interest Research Group (U.S. PIRG), and the World Privacy Forum submit comments on behalf of civil society organizations (CSO) in the United States concerned about privacy to urge the strengthening of privacy rules in the Asia Pacific Economic Cooperation Group so as to ensure the protection of consumer information that travels across national borders. We appreciate the opportunity provided by the Department of Commerce for the Public Voice to be heard on this important issue.

INTRODUCTION

The APEC Privacy Framework recognizes the "importance of protecting information and maintaining information flows among economies in the Asia Pacific region and among their trading partners."[2] The Framework also acknowledges the growing importance of new technologies for social and economic benefit, but cautions:

> [W]hile these technologies make it easier and cheaper to collect, link, and use large quantities of information, they also make these activities undetectable to individuals. Consequently, it can be more difficult for individual to retain a measure of control over their personal information. As a result, individuals have become concerned about the harmful

[1] Development and Implementation of Cross-border Privacy Rules in the Asia Pacific Cooperation Group, 71 Fed. Reg. 29,315 (May 22, 2006).
[2] Asia-Pac. Econ. Cooperation [APEC], *APEC Privacy Framework*, at 2 (Oct. 29, 2004) (Part I: Preamble, Point 1), *reprinted in* MARC ROTENBERG, THE PRIVACY LAW SOURCEBOOK 2004: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS 508 (EPIC 2004) (hereinafter "PRIVACY LAW SOURCEBOOK 2004")

> consequences that may arise from the misuse of personal information. Therefore, there is a need to promote and enforce ethical and trustworthy information practices in on- and off-line contexts to bolster the confidence of individuals and organizations.[3]

Privacy, as set out in the Universal Declaration of Human Rights of the United Nations, is a fundamental right.[4] That nearly all APEC economies are members of the United Nations[5] indicates privacy "is not a culture-bound value only relevant to advanced Western democracies . . . . [T]he core value [of privacy] is the same [because] . . . [i]t inheres in the dignity of each individual human being."[6]

The privacy principles in the Organisation for Economic Co-operation and Development (OECD) 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[7] are universally applicable. APEC member economies Japan, Australia, New Zealand, Canada and the United States were members of the OECD at the time the Guidelines were issued in 1980, and South Korea joined the OECD in 1996. The development of the OEC Privacy Guidelines, with the participation of countries from North America, Europe, and Asia, indicate that the privacy principles span multiple cultures. Furthermore, the Hong Kong Privacy Commissioner acknowledges that many Asian jurisdictions have examined the merits and features of the OECD in developing their own privacy systems, and that the OECD "set the benchmark in several Asian jurisdictions that have had strong historical ties with Europe."[8] However, the Hong Kong Commissioner also emphasizes that Asian economies have done more than merely abstracting the OECD privacy traditions into their own privacy systems. He describes Hong Kong's privacy regimen, which enshrines both the letter and spirit of the OECD principles and upgrades privacy protection to new levels in the region, as "European inspired but locally oriented, rather than simply a direct copy of what has gone before."[9] This demonstrates that the OECD

---

[3] Id.

[4] G.A. Res. 217 A (III), ¶ 12, U.N. DOC. A/ (Dec. 10, 1948) (Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.").

[5] Hong Kong and Chinese Taipei are the only APEC economies that are not members of the United Nations. This is because Hong Kong is a special administrative region of China and Chinese Taipei's political status as an independent nation is contested. However, both economies embrace the ideology and founding instruments of the United Nations – Hong Kong as a part of China, and Taiwan through its multiple attempts to rejoin the United Nations as the Republic of China.

[6] David Loukidelis, Info. and Privacy Comm'r for B.C., Transborder Data Flows & Privacy – An Update on Work in Progress at the 7th Annual Privacy & Security Conference (Feb. 10, 2006). See generally, EPIC and Privacy International, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS (EPIC 2004).

[7] Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980), *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html, *reprinted in* PRIVACY LAW SOURCEBOOK 2004 AT 395.

[8] Raymond Tang, Hong Kong Privacy Comm'r for Personal Data, Keynote Address at the 4th IAPP Privacy and Data Sec. Summit and Expo (Feb. 19, 2004).

[9] *Id.*

Guidelines are sensitive and flexible to "cultural and other diversities that exist within [APEC] member economies."[10]

The OECD Privacy Guidelines "have had a significant impact on the development of national law in North America, Europe, and East Asia . . ."[11] APEC member economies are among the countries that have extensively borrowed and incorporated aspects of the Guidelines into their own privacy systems. Australia's 1988 Privacy Act and New Zealand's 1993 Privacy Act adopt eleven and twelve privacy principles based on the OECD Guidelines, respectively.[12] Japan's act regulating electronic personal information maintained by the government also

> adopts many of the OECD Guidelines, including the collection limitation principle, the purpose specification principle, and the openness principle. [Similarly,] South Korea's Act on the Protection of Personal Information Managed by Public Agencies of 1994, which regulates electronic personal data maintained by the government, follows a number of OECD Guidelines such as the collection limitation principle, the data quality principle, the openness principle, and the purpose specification principle.[13]

The OECD Privacy Guidelines should be used as a benchmark in the evaluation of the Cross-Border Privacy Rules (CBPRs). The OECD Guidelines present a successful multinational standard for cross-border data transfer,[14] and the preamble to APEC's Privacy Framework itself asserts consistency with the core values of the OECD Guidelines.[15] Because the Framework endorses accountability as a means of implementing the privacy rules, its principles are enshrined as goals rather than laws for its members. In order to achieve meaningful information privacy protection, the CBPRs must clearly support and advance privacy protection. Accordingly, the OECD Privacy Guidelines set a standard for the CBPRs to follow.

Further, APEC is comprised of member economies – some of which are nations, others which are special administrative regions of other nations. "[A] large collection of governments and localized industries like the EU [already] harbors vast differences in 'rights, powers, and incentives between governments and the private sector.'"[16] Stronger CBPRs are necessary to reconcile the differences among APEC members – 21

---

[10] APEC Privacy Framework, *supra* note 2, at 3 (Part I: Preamble, Point 6), *reprinted in* PRIVACY LAW SOURCEBOOK 2004 at 509.
[11] DANIEL J. SOLOVE, MARC ROTENBERG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 872-73 (2nd ed. 2006).
[12] *Id.*
[13] *Id.*
[14] *See* MacDonnell, John. *Exporting Trust: Does E-commerce Need a Canadian Privacy Seal of Approval?*, 39 Alta. L. Rev. 346, 378 (2001) ("Regarding data-protection standards, international momentum has swung decidedly toward comprehensive data-protection frameworks modeled on the EU's breakthrough effort.").
[15] APEC Privacy Framework, *supra* note 2, at 3 (Part I: Preamble, Point 5), *reprinted in* Marc Rotenberg, 509.
[16] MacDonnell, *supra* note 14, at 370.

countries which span three continents. Harmonization of data protection practices to an international standard similar to the OECD Privacy Guidelines is vital to the creation of compatible data transfer systems and therefore to the Framework's additional objective of facilitating e-commerce and business transactions.

Given the need for privacy protection for consumers personal information and the fact that some APEC members lack domestic privacy protection laws, the APEC Framework and member economies require an approach that maximizes compliance with clear privacy standards. Effective means of implementing and enforcing the CBPRs are important for this reason. As such, EPIC, the Consumer Federation of America, the National Consumers League, the Privacy Rights Clearinghouse, the Privacy Times, U.S. PIRG, and the World Privacy Forum make the following recommendations:

1. Build on current privacy law and data protection institutions that have already been established to safeguard personal information in the region.

2. Encourage APEC members to enact the CBPRs themselves as law or to create and adopt even stronger information privacy systems.

3. Persuade member economies to either suspend data transfer operations or increase the liability of organizations that seek to transfer data to an economy with weaker data protection laws without:

    a. undertaking contractual mechanisms to ensure that the protection travels across borders with the data, *and*
    b. creating a process for time bound dispute resolution in the absence of an administrative or legal process in the data source's economy.

4. Encourage APEC members to enact whistle-blowing laws protecting employees from retaliatory action for disclosing privacy violations.

5. Create a monitoring committee that tracks when an organization violates CBPRs and/or any APEC member's data protection laws, issues warnings to offending organizations, publishes lists of violators, and makes recommendations on enforcement to the Privacy Commissioners or relevant government officials of the APEC members to which the involved individuals belong.

6. Encourage making the maximum legal data protection a standard. In any transaction in which an organization transfers data from one or more origination economy to one or more destination economy, the strongest data protection laws of any involved member economy should apply to all of the transferred data.

7. Encourage organizations to distinguish between "sensitive information" and ordinary personal information and to provide upgraded protection for the former.

8. Adopt an opt-in approach, as opposed to an opt-out approach, with regard to the collection, access, transfer, and use of sensitive personal information data.

9. Adopt a Purpose Specification Principle equivalent to the OECD's and thus require organizations to publicize and adhere to the expressed purpose for which the data was gathered.

10. Insert a Deletion Principle that encourages organizations to make provisions for the deletion of all data retained in any member economy that is no longer necessary for the organization's operations.

11. Insert an Openness Principle equivalent to the OECD's to ensure overall public awareness of the privacy practices and policies of members' surveillance systems.

12. Remove the burden of translation costs from individuals.

13. Adopt a non-binding equivalent version of the EU Directive's automated processing principle.[17]

14. Provide every individual with the right to access and correct his or her personal data even when that data is classified as confidential commercial information.

15. Presume the existence of harm whenever the CBPRs are violated and/or a breach occurs.

In the discussion that follows, it is assumed that the global organization is the personal information controller.

Recommendation 1 – in general

The preamble to the APEC Framework on information privacy protection states that the Framework was:

> developed in recognition of the importance of: developing appropriate privacy protections for personal information, particularly from the harmful consequences of unwanted intrusions and the misuse of personal

[17] Council Directive 95/46, art. 51, 1995 O.J. (L 281) 31 (EC).

> information; . . . [and] . . . [e]nabling enforcement agencies to fulfill their mandate to protect information privacy; and [a]dvancing international mechanisms to promote and enforce information privacy and to maintain the continuity of information flows among APEC economies and with their trading partners.[18]

CSO recommend: As the purpose of the CBPRs is to ensure the protection of privacy as personal information crosses national borders, it is important that high level, uniform privacy standards be established. Specifically, these standards should ensure that "personal information . . . [is] collected, held, processed, used, transferred, and disclose din a manner that protects individual information privacy . . . within and across borders."[19]

Recommendations 2 - 5 in relation to Principle IX on Accountability

The APEC Principles "recognize[] that individuals who entrust their information to another are entitled to expect that their information will be protected with reasonable safeguards."[20] Some form of enforcement is necessary in order to ensure that these expectations are met.

Although accountability is the preferred means of enforcement in the APEC Principles, Principle IX on Accountability undermines its own usefulness because it leaves open the possibility that a data subject may be left:

> without a remedy against any party where the exporter has exercised due diligence but the importer has nevertheless breached an IPP [information privacy principle]. There is no remedy against the exporter, and none against the importer if it is in a jurisdiction without applicable privacy laws, unless there is a contractual clause requiring APEC compliance in a jurisdiction where consumers can enforce such clauses benefiting third parties . . . .[21]

While it is the preferred means of enforcement, accountability does not have to be the only means of enforcement of the CBPRs. Instead of relying solely on accountability, regimes such as the OECD have been made directly binding on their members. Such regimes also promote the strengthening of their members' data protection laws.

---

[18] APEC Privacy Framework, *supra* note 2, at 4 (Part I: Preamble, Point 8), *reprinted in* PRIVACY LAW SOURCEBOOK 2004 at 509.
[19] APEC Privacy Framework, *supra* note 2, at 30 (Part IV: Implementation, Point 29), *reprinted in* PRIVACY LAW SOURCEBOOK 2004 at 520.
[20] APEC Privacy Framework, *supra* note 2, at 28 (Part III, Point 22), *reprinted in* PRIVACY LAW SOURCEBOOK 2004 at 509.
[21] Graham Greenleaf, The Global Contexts of Privacy Rights Policies in the Digital Age: Prospects and Present Situation (Sept. 27-29, 2005), Keynote Presentation at the UNESCO International Forum on Privacy Rights in the Digital Age, http://www2.austlii.edu.au/%7Egraham/publications/2005/UNESCO_Privacy.html#Heading62.

Purely private means of insuring compliance, including self-policing or industry policing through techniques like trustmarks, are inadequate means of enforcement. Trustmarks in general put individuals' privacy rights in the hands of corporations that have conflicts of interest between protecting individual privacy and maintaining good relationships with the corporations they evaluate. Unsurprisingly, many of the trustmark providers fail to require adherence even to generally accepted international privacy standards.[22] Specifically regarding the industry-run privacy compliance certification known as Web seals, APEC's consultants have noted that, "without objective standards on which to evaluate these seals, their relative merits remain open to debate. The public requires a greater degree of certainty regarding the claims that a company, especially one unknown to them, bearing a Web privacy seal will in fact protect one's privacy."[23]

CS0 recommend: The CBPRs should encourage the uniform adoption of stronger data protection laws. Additional accountability mechanisms should also be introduced in order to promote compliance with the CBPRs.

- *Recommendation 2*. CBPRs should encourage APEC members to enact the CBPRs themselves as law or to create and adopt even **stronger informational privacy laws**.

- *Recommendation 3(a)*. Both **suspension of data transfer privileges** and **increased sanctions or fines** are powerful mechanisms that ensure that organizations implement safeguards (i.e. contracts[24]) to maintain at least the existing protection that attaches to data at the time of its collection before transferring that data to places with weaker data protection systems.

  Despite the non-binding nature of APEC, CBPRs would be effectively enforced by upgrading sanctions or fines or by suspending organizations that transfer

[22] Andrew Shen, EPIC, Online Profiling Project – Comment 32 (November 8, 1999), http://www.epic.org/privacy/internet/Online_Profiling_Workshop.PDF (noting that trustmark provider TRUSTe "do[es] not even presume that users should have control over the use of their information," and pointing out that the United States government removed a TRUSTe seal from its website because TRUSTe itself failed to comply with United States privacy laws).

[23] The Office of the Info. and Privacy Comm'r/Ont. and The Office of the Fed. Privacy Comm'r of Austl., *Web Seals: A Review of Online Privacy Programs* (September 2000) [hereinafter *Web Seals*], *available at* http://www.privacy.gov.au/publications/seals.html (published at the 22nd International Conference on Privacy and Personal Data Protection in 2001, and presented at APEC's 2nd Technical Assistance Seminar on Implementation of APEC Privacy Framework: International Implementation Issues, in Gyeongju, Korea, Sept. 5-6, 2005).

[24] The contracts can be modeled after the EU Directive or the Hong Kong Rule 33 provision with liability, indemnity, and dispute resolution clauses. *See* Margaret P. Eisenhauer, *A Survey of International Data Transfer Provisions in Existing Data Protection Legislation* 22 (ASIA-PACIFIC ECONOMIC COOPERATION PAPER, Aug. 20, 2005), *available at* http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0075.File.v1.1.

personal information data to destinations with weaker data privacy protection laws without additional contractual mechanisms.

For instance, suppose Organization X collects personal information data in Korea, and then transfers it to Organization Y in Papua New Guinea, which has substantially weaker data privacy protection laws. Such a CBPR would mandate that Organization X be susceptible to larger civil and/or criminal penalties and/or to greater damage compensation payouts under Korea's Data Protection Act.[25]

Organizations would thus have incentives to comply with strong privacy standards that guard data privacy from being downgraded by a data transfer to a regime with less protection. Without restricting data flow to other economies, protection is therefore ensured "regardless of where the data is processed."[26] Exposing organizations to the possibility of the suspension of data transfer privileges (which often translates into suspension of normal operations) or greater financial liability is also consistent with Principle I on Preventing Harm. This is because the likelihood and severity of the harm posed to the individual is magnified by transfer of the data to a jurisdiction with weaker or non-existent data protection laws. Such a transfer amplifies the difficulties of access and correction and of use of legal remedies to which an individual is entitled. These mechanisms constitute "remedial measures" that are proportional to the likelihood and significance of harm.

- *Recommendation 3(b).* In conjunction with the above recommendation, it is equally important that a **process for time bound dispute resolution** be available if the APEC member in which the data originates (is collected or generated) lacks sufficient administrative or legal process for resolution of privacy disputes. Contractual privacy safeguards are only meaningful when the less sophisticated party (such as the data subject) has the opportunity to raise and resolve contractual conflicts about privacy protection. Korea's special privacy dispute mediation committee, the Personal Information Dispute Mediation Committee, is a good model.[27]

- *Recommendation 4.* Member economies should be encouraged to adopt **whistle-blower laws** that shield employees who report on data privacy violations by any organization, or agents or subsidiaries thereof, from retaliatory reaction. A CBPR promoting this goal could point to the redress provision of Canada's system as an example.

- *Recommendation 5.* APEC should establish a single independent watchdog committee similar to the European Data Protection Supervisor. This supervisory committee would be responsible for monitoring data transfer

[25] Eisenhauer, *supra* note 24, at 27.
[26] Eisenhauer, *supra* note 24, at 22.
[27] *Id.*

practices in all the member economies and sounding alarms about violations, both to organizations and to member economy privacy authorities. This watchdog group should also publish a list of organizations which violate CBPRs and/or any APEC member's data protection laws. An annual report would provide the basis for an ongoing evaluation of the APEC Privacy Framework. These actions would significantly bolster compliance with the CBPRs and promote uniformity of privacy standards.

Recommendation 6

The general purpose of the APEC CBPRs is to ensure the protection of privacy as personal information crosses national borders. "When transferring information, personal information controllers should be accountable for ensuring that the recipient will protect the information consistently with these Principles . . . ."[28] This can only be achieved if individuals' personal data is protected as it is transferred among economies with differing privacy protections. The CBPRs' additional purpose of promoting commerce would be promoted by the harmonization of member economies' privacy regimes.

CSO recommend: In any transaction in which data is transferred from one or more origination economies to one or more destination economies, the strongest data protection laws of any APEC member should apply to all of the transferred data.

Applying the strongest data protection laws of the APEC members involved in the given trans-border data transaction would help the privacy regimes of APEC members converge in practice, while providing maximum protection to individuals' privacy rights.

Recommendations 7 and 8 in relation to Principle II on Notice, Principle IV on Uses of Personal Information, Principle V on Choice

Businesses favor opt-out methods of data collection and use because the requirement of an affirmative act to deny authorization restricts the amount of data available to data managers and business firms.[29] On the other hand, opt-out methods may be designed to have confusing and difficult requirements that impose costs on individuals as compared to generally quick and easy opt-in mechanisms.[30] In multiple cases, consumers' attempts to opt out have simply been ignored.[31] Thus, even non-

[28] APEC Privacy Framework, *supra* note 2, at 28 (Part III, Point 26), *reprinted in* Marc Rotenberg, 509.
[29] Shubhankar Dam, *Article: Remedying a Technological Challenge: Individual Privacy and Market Efficiency; Issues and Perspectives on the Law Relating to Data Protection*, 15 Alb. L.J. Sci. & Tech. 337, 346 (2005).
[30] *Id.*
[31] EPIC Reply Comments to the Fed. Commc'n Comm'n In the Matter of Telecomm. Carriers' Use of Customer Proprietary Network Info. (Nov. 16, 2001), *available at* http://www.epic.org/privacy/cpni/CPNI_Reply_Comments.html (explaining that "not only is the burden on the customer to pay for and return their opt-out notice, such notices are vague, incoherent, and often concealed . . . Opt-out notices mailed out by financial institutions . . . were unintelligible and couched in

APEC economies such as India, in considering the introduction of their own information privacy principles, recognize that the need to "discriminate between the kinds of information is potentially significant."[32]

CSO recommend: CBPRs should adopt the EU's distinction between "data" and "sensitive data"[33] and encourage APEC members to favor "opt-in" privacy safeguards..

- *Recommendation 7.* **Sensitive information** should include sex, health, or gender-related data; racial or ethnic origin; political opinions; religious beliefs; and trade-union membership.

- *Recommendation 8.* **Sensitive information** should only be collected through an **explicit opt-in method**, except in the cases of law enforcement, state emergency, or security laws. The Framework specifically requires exceptions "relating to national sovereignty, national security, public safety and public policy . . . [to] be: a) limited and proportional to meeting the objectives to which the exceptions relate; and, b) (i) made known to the public; or, (ii) in accordance with law."[34] With regards to other, non-sensitive personal data, an opt-out approach should be the minimum standard for data collection, and it is appropriate to give every affected individual notice about any such approach and about his or her means of access and control of the collected data, not later than when the information is collected.

  This provides individuals with two levels of choice under Principle V, since personal data can be collected and processed if the data subject consents tacitly, while sensitive data can only be collected and processed once the data subject's explicit consent has been secured.[35] Under economic analysis, the approach maximizes free information by providing two levels of consent because "with the possibility of providing personal data but withholding 'sensitive' information, individuals may be more forthcoming in providing consent for the collection of personal data."[36]

Recommendations 9 through 12 in relation to Principle II on Notice, and Principle III on Collection Limitation, Principle VI on Integrity of Personal Information, and Principle VIII on Access and Correction

---

language several . . . levels above the reading capacity . . . of the general public . . . Expert studies illustrate that, in fact, few consumers recall seeing notices even when the [opt-out] notices are required to be clear and conspicuous, which suggest that when businesses do not want consumers to see a notice, consumers will not.").

[32] Dam, *supra* note 29, at 365

[33] Council Directive 95/46, art. 8, 1995 O.J. (L 281) 31 (EC).

[34] APEC Privacy Framework, *supra* note 2, at 8 (Part II: Scope, Point 13), *reprinted in* PRIVACY :LAW SOURCEBOOK 2004 at 511.

[35] Dam, *supra* note 29, at 357.

[36] *Id.* at 358.

The APEC Privacy Framework recognizes that individuals have interests in the control of their personal information. For that reason, organizations should collect and use personal information only to the extent that it serves valid organizational purposes.

Information is also more likely to be disclosed if privacy is protected. Thus, continuous control "over PID [personal information data] is crucial for encouraging individuals to share their information. Without any such control, or at least inexpensive control, individuals may be hesitant in providing information."[37]

CSO recommend: CBPRs should refine the current Notice Principle, introduce Openness and Deletion Principles, and shift the costs of translation from individuals to organizations in order to achieve transparency and access.

- *Recommendation 9.* CBPRs should encourage organizations to publicize a "**purpose specification**" listing all the potential purposes for which the personal information is collected and to commit to using the information only for the enumerated purposes. "The information should be relevant to such purposes, and proportionality to the fulfillment of such purposes may be a factor in determining what is relevant."[38]

- *Recommendation 10.* CBPRs should provide for the permanent **deletion** of all data that has expired -- i.e. data that no longer serves any of the purposes listed in the purpose specification -- but is retained by an organization operating in any of the member economies.

- *Recommendation 11.* CBPRs should commit to an **openness principle** so that the data collection, processing, use, and transfer processes and policies of organizations are transparent to impacted individuals and entities. This is important so that the individual or entity can make an informed decision about whether to consent to submitting information. One example is Recommendation 7's notice of an opt-out method at the time of or before data collection.

- *Recommendation 12.* Currently, an organization will charge an individual the cost of translation if it holds the information in a language other than the language of original collection. This is an impediment to an individual's assurance of the integrity of his or her personal information and to his or her choice of mechanisms for data access and correction since it may impede an individual's ability to monitor his collected data. CBPRs should push for a **relaxation of Principle VIII's translation requirements** so as to ensure ease of access for every individual to his or her own data. Specifically, the

[37] *Id.* at 359.
[38] APEC Privacy Framework, *supra* note 2, at 8 (Part III: Scope, Point 18), *reprinted in* PRIVACY LAW SOURCEBOOK 2004 at 511.

organization should be responsible for the costs, including timely provision, of all translation requests from data subjects in member economies.

Recommendation 13 in relation to Principle II on Notice, Principle VIII on Access and Correction, and Principle IX on Accountability

Perhaps the most prominent example of automated processing is the Internet "cookie." Commentary to Principle II uses the cookie to illustrate that giving notice at or before the time of information collection is impractical when electronic technology that automatically collects information is triggered by individual action (i.e. a mouse click).

CSO recommend: Currently, CBPRs make notice of such automated processing technologies the exception, rather than the general practice. Since notices rarely provide any meaningful choice to consumers, automatic data-collecting techniques require the adoption of opt-in requirements.

Further, APEC should emulate Article 15 of the EU Directive,[39] which provides that an organization should not "make a decision adverse to an individual based on automated processing without a prior review of that decision by a human . . . ."[40] This serves both to minimize the chance of errors by the automated process and to hold an agent of the information gathering organization responsible for the decision.

Recommendation 14 in relation to Principle VIII on Access and Correction

Currently, if personal information is classified as "confidential commercial information" (i.e. as a trade secret), the Framework relieves personal information controllers from due diligence and consent obligations in granting access to data subjects.

CSO recommend: CBPRs should mandate that organizations provide individual access and correction regardless of whether the personal information gathered comprises commercial information or not. Individualized access and correction by data subjects will not jeopardize an organization's confidential commercial information since personal information is valuable to an organization as a collection, in the aggregate. While a collection of personal information records may constitute a trade secret, a single record of personal information cannot be proprietary commercial information.

Recommendation 15 in relation to Principle I on Preventing Harm

Since APEC introduced a Principle on Preventing Harm, a number of information privacy and security breaches have demonstrated the extent and frequency of harm which arises when proper privacy protections are not followed. In just the past

[39] *See* Council Directive 95/46, art. 51, 1995 O.J. (L 281) 31 (EC).
[40] Greenleaf, *supra* note 21.

month, nineteen data breaches were reported in the United States.[41] Among them, data which was supposed to be destroyed was instead retained and subsequently stolen from the University of Michigan Credit Union; the University of Kentucky inadvertently made former employees' personal information available online; and a violation of proper security protocol at the United States Department of Veterans Affairs led to the theft of over 28.6 million individuals' personal data, including the personal data of over one million active-duty members.[42] The Privacy Rights Clearinghouse has documented well over one hundred incidents, affecting over 84 million individuals, counting only Americans, in just the past year and a half.[43] Nor are these problems limited to the United States. APEC's consultants have also noted "high profile breaches of public trust at several brand name Web sites, as well as examples of the vulnerability of Web sites to attacks from hackers."[44] In Japan, a file sharing computer virus named Antinny has recently caused leaks of private data including customer information.[45]

Even before other tangible harms arise from these failures, an affected individual must expend substantial time, effort, and money to mitigate further damage. For instance, the United States Federal Trade Commission advises an individual whose personal information has been lost or stolen to "[c]lose accounts, like credit cards and bank accounts, immediately . . . ," "place an initial fraud alert on [his or her] credit reports . . . ," and cancel and replace his or her driver's licenses and/or other government-issued identification.[46] Additional steps are recommended if actual identity theft occurs, and in either case heightened vigilance becomes necessary.[47]

CSO recommend: In light of recent events, the existence of harm should be presumed whenever a breach of data security and/or privacy occurs, as well as in any other case when an individual's private data has been misused.

CONCLUSION

The ability of organizations using modern technology to collect and store vast quantities of data about significant numbers of individuals poses serious threats to privacy rights. To protect against these dangers, the 2004 APEC Privacy Framework set out important principles to safeguard personal information that travels across national borders. Effective implementation and enforcement of these principles will be critical to ensure the protection of privacy in the APEC region..

---

[41] Privacy Rights Clearinghouse, *A Chronology of Data Breaches Reported Since the ChoicePoint Incident*, Jun. 11, 2006, http://www.privacyrights.org/ar/ChronDataBreaches.htm.
[42] *Id.*
[43] *Id.*
[44] *Web seals*, *supra* note 23.
[45] Carl Freire, *Virus Spreads Data, Scandal Over Winny*, WASH. POST, June 12, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200817.html.
[46] FEDERAL TRADE COMMISSION, TAKE CHARGE: FIGHTING BACK AGAINST IDENTITY THEFT, http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm (Feb. 2005) (emphasis removed).
[47] *Id.*

Respectfully submitted,

Marc Rotenberg, Executive Director
Sunni Yuen, IPIOP Clerk
Anthony Ritz, IPIOP Clerk
Electronic Privacy Information Center (EPIC)

Jean Ann Fox
Consumer Federation of America

Susan Grant
National Consumers League

Beth Givens
Privacy Rights Clearinghouse

Evan Hendricks
Privacy Times

Ed Mierzwinski
US Public Interest Research Group

Pam Dixon
World Privacy Forum