

First Supplement to *International Data Privacy Laws and Application to the Use of Biometrics in the United States**

Introduction

Numerous international/intergovernmental organizations and their member states have chosen to make personal data protection an issue of global importance. New laws and regulations have been implemented and working groups and public policy think tanks have been founded and continue to work within the context of international law to protect personal information. Arguments for privacy are not new; rather, they are continuations of age-old civil liberties questions.

U.S. Supreme Court Justice Louis Brandeis said, “the right to be let alone is the most comprehensive of rights and the right most valued by civilized men.”¹ Brandeis’ modern supporters have expanded the right of privacy further. Now privacy “recognizes the human desire to restrict one’s thoughts, actions and information to oneself, and regards any intrusion as an affront to the most fundamental values of life.”² The increasing human expectations to privacy present the field of biometrics with a unique set of challenges and opportunities.

First, biometrics supporters will inevitably need to engage in public debate about privacy concerns. Ultimately, the debate will be framed with biometrics as privacy protector versus biometrics as a tool for “Big Brother.”³ Biometrics, though, have proved quite valuable and successful in thwarting instances of identity theft, while functioning as a gatekeeper to personal information and restricted areas.

Experts in the field have argued that the “irreversibility of the biometric templates stored in some systems should be considered a privacy enhancement rather than detriment.”⁴ These templates are used for matching rather than reproduction—making it nearly impossible to reconstruct a person’s biometrics from the template. And, even if a person could access the template, there is relatively little fraud that can be perpetrated. That cannot be said for a stolen credit card or Social Security number.

People who see biometrics as a threat are mainly concerned about a slippery slope in the decline of privacy rights. Their argument is that without legal or, at least, voluntary regulation—through trade organizations, for instance—there will be a free flow of biometric data. To them, “the era of Big Brother might exceed even Orwellian proportions,” if biometrics and related

* Supplement compiled by Biometric Services International, LLC. in Morgantown, West Virginia, beginning June 15, 2008 and completed July 17, 2008. Information is current through the completion date.

¹ MIT Faculty Web Site, “The Right to Privacy: Warren and Brandeis,” http://www-swiss.ai.mit.edu/6805/articles/privacy/Privacy_brand_warr2.html.

² Dam Shubhankar. “Remedying a Technological Challenge: Individual Privacy and Market Efficiency; Issues and Perspectives on the Law Relating to Data Protection,” *Albany Law Journal of Science & Technology* 15 (2005), <http://www.libraries.wvu.edu>.

³ Leader of the totalitarian society in George Orwell’s novel *1984*. *Everyone* is under surveillance by the authorities, mainly by telescreens. In the novel, people are constantly reminded of this by the phrase “Big Brother is watching you.”

⁴ Jeff Langenderder and Stefan Linnhoff, “The Emergence of Biometrics and Its Effect on Consumers,” *The Journal of Consumer Affairs* 39 (2005): 325.

technologies are left unchecked.⁵ Biometric opponents also have reasonable fears of “mission creep,” where a certain technology or project created for one purpose gradually becomes a party to different applications.⁶ Mission creep provides ample opportunity for misuse of biometric information, as in the United Kingdom’s case.

In January 2008, *The Independent* (UK) reported the United Kingdom’s plans to implant select prisoners with under-the-skin microchips as part of an electronic tagging scheme designed to create more space in British jails. These chips, known as radio frequency identification (RFID) tags, will replace more commonly worn electronic ankle monitor bracelets. The RFIDs are about the length of two grains of rice and can carry scannable personal information—including the person’s address, identity and criminal record.⁷ For an opponent of biometrics, it would not be difficult to see the RFID technology carryover to the general population—perhaps, if not usually, under the guise of national security or as a heralded innovation for protecting privacy.

The purpose of this supplement is to update and expand the original International Data Privacy Laws and Application to the use of Biometrics in the United States report published in 2005 by the National Biometric Security Project. Following this introduction are two sections: *New Analysis and Initiatives Since the Original Report* and *Updates on Key Areas of the Original Report*.

New Analysis and Initiatives

U.S. Concept of Privacy: A Tradeoff with National Security

The United States continues to view personal privacy and ipso facto, personal data, in negative correlation with national security interests. That is, as national security concerns increase, the right to, or expectation of privacy decreases. Studies show that Americans tacitly support that arrangement. Indeed, as threat perception rises, Americans tend to support civil liberties less, including free speech and privacy. But even the horrible events of September 11, 2001, have not fully eliminated American’s expectations of civil liberties.

Americans generally take a more moderate position on civil liberties during national security crises—making them “reluctant defenders of constitutional rights across the political spectrum....”⁸ Yet, surveys in the immediate wake of the September 11 terrorist attacks show that most Americans supported many government practices that—during peaceful times—would be considered invasions of privacy (See Table 1 in appendix).

The curtailment of civil liberties during crisis is partly a “rally round the flag” effect, where presidents see a substantial boost in approval ratings after a crisis (See Table 2 in appendix). This newfound approval translates into political capital for the president that can be used to guide legislation through Congress, such as the 2001 USA PATRIOT Act, or to restructure a

⁵ Ibid., 329.

⁶ Katina Michael and M.G. Michael, “Historical Lessons on ID Technology and the Consequences of an Unchecked Trajectory,” *Prometheus* 24 (2006): 365.

⁷ Brian Brady, “Prisoners ‘to be chipped like dogs,’ ” *The Independent*, January 13, 2008, <http://www.independent.co.uk/news/uk/politics/prisoners-to-be-chipped-like-dogs-769977.html>.

⁸ Darren W. Davis and Brian D. Silver, “Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America,” *American Journal of Political Science* 48 (2004): 43.

portion of the federal bureaucracy, as President George W. Bush did in forming the Department of Homeland Security in 2003.⁹

It makes sense, then, to hypothesize that biometrics and related technologies—sometimes seen as privacy invading—would be more widely accepted during times of crisis, much like infringement on civil liberties. This is important to consider in today’s world climate of terrorism and violence. U.S. courts, however, have taken a decidedly incongruent approach on whether rights can be suspended or impinged upon during crisis. As biometric technologies and deployments proliferate, vendors and/or users/policymakers could find themselves subject to legal action. Thus, it is valuable to discuss how a court might decide a privacy case during times of unrest.

U.S. Courts: Impact on International Law and Policy

In a globalized world, what happens in one country has a profound, rippling effect on what happens in another. This holds true in more than just economics. The way U.S. courts interpret law and render decisions greatly influences international relations. Indeed, the impact on international law is ample, too. For example, *Hamdan v. Rumsfeld* (2006), a case that challenged the Bush administration’s policy of trying suspected terrorists in military tribunals, created an extensive policy debate over non-citizen’s rights on two issues:

1. Can the rights protected by the Geneva Convention be enforced in federal court through *habeas corpus* petitions?
2. Was the military commission established to try Salim Ahmed Hamdan and others for alleged war crimes in the War on Terror authorized by Congress or was it within powers inherent in the Presidency?

The Supreme Court found in favor of Hamdan by a vote of 5-3, with Chief Justice John Roberts recused because of hearing and deciding the case in a lower court. The Court held that the Bush administration (Executive) lacked constitutional authority to form a military commission, such as the one slated to try Hamdan without Congressional authorization, because it violated the Uniform Code of Military Justice and the Geneva Conventions.¹⁰ Moreover, “absent expressed authorization, a military commission had to comply with the ordinary laws of the United States and the laws of war.”¹¹ Congress eventually approved military commissions with the Military Commissions Act of 2006.¹² The passage of the law ignited a firestorm of criticism concerning the precepts of the *Hamdan* case and the existence of military commissions. *The New York Times*, for example, sees military commissions at Guantánamo Bay, Cuba, as a miscarriage of justice “...where hearsay and secret documents are admissible [evidence].”¹³ The newspaper also called the Military Commissions Act “one of the worse bits of lawmaking in American

⁹ Lee Epstein, Daniel E. Ho, Gary King, and Jeffrey A. Segal, “The Supreme Court During Crisis: How War Affects Only Non-War Cases,” *New York University Law Review* 80 (2005): 15.

¹⁰ Supreme Court of the United States. “No. 05-184 Salim Ahmed Hamdan, Petitioner v. Donald H. Rumsfeld, Secretary of Defense et al.,” <http://www.supremecourtus.gov/opinions/05pdf/05-184.pdf>.

¹¹ The Oyez Project, “Hamdan v. Rumsfeld,” http://www.oyez.org/cases/2000-2009/2005/2005_05_184/.

¹² 109th U.S. Congress, “An Act to authorize trial by military commission for violations of the law of war, and for other purposes,” http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?Dbname=109_cong_bills&docid=f:s3930enr.txt.pdf.

¹³ “Guilty as Ordered,” *The New York Times*, August 7, 2008, <http://www.nytimes.com/2008/08/07/opinion/07thu1.html>.

history.”¹⁴ On the other hand, Rhode Island Supreme Court Chief Justice Frank J. Williams has defended the existence of military tribunals and advocated, in certain instances, for the suspension of *habeas corpus*, because “...the Constitution permits the suspension of the writ in ‘cases of rebellion and when the public safety’ requires it.”¹⁵

In August 2008, a panel of six military officers convicted Hamdan of “providing material support for terrorism” and acquitted him on a conspiracy charge, the more serious of the two. Hamdan, a former driver for Osama bin Laden, became the first person tried by a military commission since the end of World War II. The six-person panel sentenced Hamdan to five and a half years in prison, with credit for time served at Guantánamo Bay after his November 2001 capture in Afghanistan by U.S. forces.¹⁶ He is required to serve five more months at Guantánamo Bay and can be released in early 2009. But his imprisonment might be longer, as “the Bush administration has long asserted that it could continue to hold detainees even if they were acquitted or given short sentences because they are designated enemy combatants...”¹⁷

The above propositions and the *Hamdan* case set the stage for a debate on U.S. courts and their support of civil liberties during times of conflict. This is an important concept for biometric advocates, as court decisions could impact the scope of technology deployment in the United States and abroad. Generally, there is no rule determining how a court might decide cases involving civil liberties, but two competing theories have formed on the issue. These two theories are known as *The Crisis Thesis* and *The Milligan Thesis*, but the latter theory has a greater degree of evidential support.

The Crisis Thesis

This theory operates on the Roman lawyer and philosopher Cicero’s pronouncement in *Pro Milone* that “Inter arma enim silent leges,” literally translated to mean “For among [times of] arms, the laws fall mute,” but popularly read as “In times of war, the law falls silent.”¹⁸ *The Crisis Thesis* view of courts, especially the Supreme Court, is so widely held that few scholars really question its validity anymore. The prevailing sentiment is that courts will *always* side with the government and approve curtailment of civil liberties during conflict. That belief is not fully founded, however, as empirical evidence is lacking to support the theory. Instead, anecdotal evidence gleaned from a few landmark Court cases is used to verify the theory.

Two relevant sets of responses exist during a crisis: those of the executive and legislative branches and those of the judicial branch. The former seeks to curtail rights and liberties during wartime, while the latter is more willing to uphold those curtailments than during peacetime.¹⁹ The most prominent example of this theory is *Korematsu v. United States*.

¹⁴ Ibid.

¹⁵ Frank J. Williams, “Abraham Lincoln and Civil Liberties in Wartime,” *Heritage Lectures* (Delivered April 20, 2004): 3.

¹⁶ Sixty-one months will be counted toward Hamdan’s sentence

¹⁷ “Panel Convicts bin Laden Driver in Split Verdict,” *The New York Times*, August 7, 2008, <http://www.nytimes.com/2008/08/07/washington/07gitmo.html?scp=1&sq=Panel%20Convicts%20bin%20Laden%20Driver%20in%20Split%20Verdict&st=cse> and “Bin Laden Driver Sentenced to a Short Term,” August 8, 2008, <http://www.nytimes.com/2008/08/08/washington/08gitmo.html?scp=2&sq=Panel%20Convicts%20bin%20Laden%20Driver%20in%20Split%20Verdict&st=cse>.

¹⁸ D. H. Berry, trans., *Cicero Defense Speeches* (Oxford University Press, 2001).

¹⁹ Epstein, Ho, King, and Segal, “The Supreme Court During Crisis...,” 10.

Korematsu questioned the constitutionality of interring people of Japanese ancestry—the majority were American citizens—during World War II. The practice was initiated by President Franklin D. Roosevelt in Executive Order 9066, while various statutes gave the military authority to relocate people of Japanese descent from areas deemed critical to national defense and potentially vulnerable to espionage.

The plaintiff, *Korematsu*, remained in San Leandro, California, and violated Civilian Exclusion Order No. 34 of the U.S. Army. The Supreme Court ruled, in that instance, the need to protect against espionage outweighed *Korematsu's* rights. Justice Hugo Black specifically argued for the relocation of people. He said, although constitutionally suspect, the procedure was justified during circumstances of "emergency and peril."²⁰

Nevertheless, recent research has shown that *The Crisis Thesis* is not valid in every application. To be sure, when crises threaten national security, the Supreme Court is more likely to curtail civil rights and liberties as the theory suggests. The difference, paradoxically, is that the justices are only willing to apply such a standard to cases unrelated to war or national security. The justices “instead of balancing rights and security in high stakes cases directly related to the war” seek to “ensur[e] the institutional checks of the democratic branches.”²¹ That behavior segues into the other theory of U.S. courts during periods of national security crisis.

The Milligan Thesis

This theory sees the courts as a guardian of civil liberties and rights during times of war. Instead, “during war the law speaks loudly,” a direct affront to Cicero’s opinion.²² It is named after the landmark Supreme Court case *Ex parte Milligan*, which addressed the authority of President Abraham Lincoln to suspend *habeas corpus*²³ during the Civil War. Justice David Davis said in the Court’s majority opinion in the case: “The importance of the main question presented by this record cannot be overstated; for it involves the very framework of the government and the fundamental principles of American liberty.”²⁴

Indisputably, the Supreme Court’s decision affirmed the right of Lincoln to suspend *habeas corpus* but only when regular civilian courts were not functioning. In sum, the Court ruled that military tribunals could not try civilians in areas where civil courts were open, even during times of war. Davis’ words were prophetic in determining the case’s impact on turmoil and war-time jurisprudence. Moreover, the decision concerns biometrics greatly, as a Court case concerning technology deployment may be decided differently during times of conflict than peacetime—or, even, within the scope of the War on Terrorism.

²⁰ The Oyez Project, “*Korematsu v. United States*” http://www.oyez.org/cases/1940-1949/1944/1944_22/.

²¹ Epstein, Ho, King, and Segal, “The Supreme Court During Crisis...,” 1.

²² *Ibid.*, 4.

²³ From Latin, literally meaning “[We command] that you have the body.” The right to habeas corpus is espoused in Amendment Five of the U.S. Constitution—stating “No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury...” That right cannot be suspended, “unless...in Cases of Rebellion or Invasion [that] the public Safety may require it,” as outlined in Article I, Section of the U.S. Constitution.

²⁴ The University of Chicago Law School, “*Ex parte Milligan* 71 U.S. 2 (1866),” <http://www.law.uchicago.edu/tribunals/docs/milligan.pdf>.

Application to Biometrics

In Epstein, Ho, King and Segal’s seminal work on the Supreme Court in wartime, they found that there exists a “crisis jurisprudence”—that “justices are...significantly more likely to curtail rights and liberties during times of war and other international threats.”²⁵ Also, the scholars found that, contrary to *The Crisis Thesis*, “there is no evidence that the presence of war affects cases directly related to war.” Therefore, this finding should be interpreted to mean that a case involving biometrics as a privacy concern during a crisis could be decided unfavorably based on empirical evidence. This is important information to consider when initiating a wide-scale deployment of new or reasonably new biometric technologies.

Exemptions to the Privacy Act of 1974: Passenger Name Record Program and Arrival and Departure Information System

The Privacy Act of 1974 declares that no federal agency—unless exempted—can disclose or communicate personal information or data to another federal agency or person without prior written authorization. That authorization must come from the person about whom the information pertains. Under the law, federal agencies are allowed to request an exemption, if they are involved in law enforcement or national security defense, generally. The Central Intelligence Agency, for example, is expressly exempt from the law.²⁶

In August 2007, the Department of Homeland Security (DHS) requested an exemption from the law for its Arrival and Departure Information System (ADIS).²⁷ ADIS is a way of compiling data on aliens²⁸ flying into the United States who could be national security threats. DHS then shares the information with law enforcement, immigration controllers, intelligence officers and other concerned constituencies.²⁹ ADIS stores biographic, biometric indicator and encounter data on aliens who have applied for entry, entered or departed the United States. Primarily and specifically, the system was developed to investigate individuals who might have violated their immigration status by staying in the United States longer than authorized.³⁰

The proposed rules change filed and reported in the Federal Register explains the need for the exemption(s):

1. To preclude subjects of these activities [terrorism, et al.] from frustrating these processes;
2. To avoid disclosure of activity techniques;
3. To protect the identities and physical safety of confidential informants and of immigration and border management and law enforcement personnel;
4. To ensure DHS’s ability to obtain information from third parties and other sources;

²⁵ Epstein, Ho, King, and Segal, “The Supreme Court During Crisis...,” 9.

²⁶ U.S. Department of Justice, “The Privacy Act of 1974: 5 U.S.C. § 552a,” <http://www.usdoj.gov/oip/privstat.htm/>.

²⁷ U.S. Government Printing Office, “Privacy Act of 1974: Implementation of Exemptions,” <http://edocket.access.gpo.gov/2007/E7-16461.htm>.

²⁸ An “alien” is defined by the Immigration and Nationality Act as anyone who is not a citizen or national of the United States. 8 U.S.C. § 1101 (a)(3).

²⁹ U.S. Department of Homeland Security, “Privacy Impact Assessment for the Arrival and Departure Information System (ADIS): August 1, 2007,” http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_adis_2007.pdf.

³⁰ *Ibid.*

5. To protect the privacy of third parties and
6. To safeguard classified information.³¹

ADIS will supplement the Passenger Name Record Program (PNRP), a privately developed partnership between airlines to track and screen their passengers. The International Air Transport Association, an international trade group of airlines, standardized what information would be collected and the layout of PNRP. On May 28, 2004, an international agreement was signed between the United States and European Union concerning PNRP and the usage of the information. PNRP is shared between the United States and EU, if privacy practices are upheld—specifically *Directive 95/46/EC of the EU*,³² commonly known as the *Data Protection Directive*, and the *Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.³³

As noted in the original report, Europeans generally take privacy rights more seriously than Americans. Indeed, in the *Data Protection Directive*, privacy is declared as a human right, not some tacit privilege, as it is normally viewed in the United States: “[data processing systems] must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy...”³⁴ As previously noted, U.S. policies and laws generally view privacy rights of non-citizens to be lesser than those afforded to citizens (see *Hamdan* case and ADIS system). This reality should be further explored, as it could have a major impact on who might be obligated to use biometric devices or submit samples and under what or whose authority.

In July 2007, the U.S. Department of Homeland Security and the European Union entered into an agreement concerning the transfer and sharing of PNRP data. Under the terms of the agreement, DHS agreed to certain undisclosed privacy assurances but at least adhering to the EU *Data Protection Directive* and the *OECD Guidelines*. In return, the EU will ensure that air carriers operating flights to the United States will make their PNRP data available to DHS.³⁵

On the European front, the European Union announced in November 2007 plans for a framework using PNRP data among its member states. The proposal requires air carriers to make PNRP data available to law enforcement authorities in EU member states to help combat and prevent organized crime and terrorism. Under the proposal, air carriers must furnish 19 PNRP data elements, but only for flights between two EU member states (for example, a flight from Italy to Spain).³⁶ PNRP data could include biometric materials, especially with the advent of biometric passports and as more countries, such as the United Kingdom, require biometric samples be given for visas.

³¹ U.S. Government Printing Office, “Privacy Act of 1974: Implementation of Exemptions...”

³² Official Journal of the European Communities, “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,” http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

³³ OECD Directorate for Science, Technology and Industry, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

³⁴ Official Journal of the European Communities, “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,” http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

³⁵ U.S. Department of Homeland Security, “Agreement Between the United States of America and the European Union on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS),” <http://www.dhs.gov/xlibrary/assets/pnr-2007agreement-usversion.pdf>.

³⁶ European Union Press Releases, “Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes,” <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/449&format=HTML&aged=0&language=EN&guiLanguage=en>.

Updates to Previous Analysis and Initiatives

The Appending and Amending of an Important Executive Order

Executive Order 12333

President Ronald Reagan signed Executive Order 12333 on December 4, 1981, with the intent “to control and provide direction and guidance to the Intelligence Community.” Explicitly, the order obligated the U.S. intelligence community to provide the president and the National Security Council with information to make decisions concerning defense, economic and foreign policy and for the protection of national security interests. The order also addressed the underlying problem of intelligence collection—personal data management—but only tacitly.³⁷

The order mandates that “information is a priority objective and will be pursued in a vigorous, innovative and responsible manner that is consistent with the Constitution and applicable law...”³⁸ It also explains that information can be collected, disseminated and retained only by procedures set forth by the head of the federal agency in question. Those must be approved by the attorney general, after being vetted against the outline for collecting information:

Permitted by the order (appended and amended)

- Publicly available information, or information collected with the consent of the person involved;
- Information needed to protect the safety of any persons or organizations, including those who are targets, victims or hostages of international terrorist organizations;
- Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws;
- Information for administrative purposes.³⁹

The guidelines above concerning what information may or may not be collected, disseminated and retained are ambiguous. Numerous interpretations of the permissions listed provide the opportunity for privacy abuses, even though the order attempts to mitigate them with specific wording. This has an enormous impact on biometric data, because it could—in theory—be utilized in intelligence activities inadvertently. Therefore, the process by which biometric samples are taken and the security of their storage is of the utmost importance.

Executive Order 13355

President Bush signed Executive Order 13355 on August 27, 2004, “to further strengthen” U.S. intelligence activities for the sake of national defense against terrorism. The order bolstered the role of the Director of Central Intelligence (CIA) by mandating that he or she

³⁷ The U.S. National Archives & Records Administration, “The Provisions of Executive Order 12333 of Dec. 4, 1981,” <http://www.archives.gov/federal-register/codification/executive-order/12333.html?template=print>.

³⁸ *Ibid.*, Section 2.1 under Conduct of Intelligence Activities.

³⁹ *Ibid.*, Section 2.3 under Conduct of Intelligence Activities.

act as the principal adviser to the president and National Security Council for intelligence matters concerning national security. Subsection 1.5 of Executive Order 12333 was also greatly changed—allowing for greater free flow of intelligence: “...the fullest and most prompt sharing of information practicable, assigning the highest priority to detecting, preventing, preempting, and disrupting terrorist threats against our homeland, our people, our allies, and our interests...” Perhaps most important, though, is the proclamation that fighting terrorism is the “highest national security priority.”⁴⁰ This order amended some aspects of Executive Order 12333, but the latter is still valid—subject to the changes of the new order and future ones.

Importance of the Organisation for Economic Co-operation and Development for Privacy Standards and Biometric Deployment

The Organisation for Economic Co-operation and Development (OECD) is an intergovernmental organization composed of 30 market-based, democratic countries that seeks to address economic, governmental and social concerns relating to globalization and reap the benefits. The only requirement to be a member of OECD is a “commitment to a market economy and a pluralistic democracy.” Its 30 current members produce nearly 60 percent of the world’s goods and services. But non-member countries are also invited to participate in OECD initiatives by becoming parties to agreements and treaties and engaging in global discussions. Currently, OECD operates on a budget of about \$537 million, 25 percent (about \$134 million) of which is funded by the United States.⁴¹

Because of OECD’s unique role in the global community, it is an excellent outlet for discussing biometrics and the ensuing privacy concerns. Indeed, this is why *The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) are invaluable to any discussion of data privacy, nearly 30 years after their adoption. Although the privacy protections contained in the document may be outdated, the underlying themes are still being discussed by OECD countries and non-members through working groups. This is an encouraging step toward a more universal definition of privacy, which will greatly benefit the biometric community by clearly defining the rules of operation and providing direction for storage of personal or sensitive data.

The OECD Working Party on Information Security and Privacy (WPISP), under the purview of the Directorate for Science, Technology and Industry, was created in October 1995 with a set of goals and a specific yet amendable mandate. Most relevant to biometrics, among WPISP’s responsibilities, is: “To monitor and analyse developments and trends in security of information systems and networks, and protection of personal data and privacy in the Digital economy/Global information society, in member countries and non-member economies...”⁴² Of the countries highlighted in this report, Australia, Canada, Japan, the United Kingdom and the United States are in the working group. Mr. Keith Besgrove from Australia chairs the group, while the four previously mentioned countries serve as vice chairs. Still, the group is set to disband on December 31, 2008. No successor group has been named.

⁴⁰ The U.S. National Archives & Records Administration, “Executive Order 13355 of August 27, 2004, Strengthened Management of the Intelligence Community,” <http://www.archives.gov/federal-register/executive-orders/2004.html>.

⁴¹ The Organisation for Economic Co-operation and Development, “The OECD Brochure,” <http://www.oecd.org/Dataoecd/15/33/34011915.pdf>.

⁴² On-Line Guide to OECD Intergovernmental Activity, “Working Party on Information Security and Privacy (WPISP),” http://webnet3.oecd.org/OECDgroups/Bodies.asp?body_id=1840&lng=E.

In the marketplace, biometric technologies are expected to have widespread deployment and fill various niches where older technologies may not evolve with privacy norms. Making the *OECD Guidelines* even more important is the fact that biometrics are seen a “silver bullet” for reducing the cost and risk of transactions online and creating more trust.⁴³ Imagine using biometrics to identify and verify eBay buyers or sellers, for instance, or using biometrics to deter fraudulent credit card usage and identity theft. Those innovations are at least years away or may never occur, but they do present challenges concerning privacy and data security. The concept of risk (privacy threat and data security) and reward (protection of identity and stronger verification methods) must be fully considered in every application of biometric technologies, especially within the scope of law.

First, the *OECD Guidelines*, written in 1980, are too old to consider biometric technology and their related applications. Therefore, an overhaul of the agreement is necessary to meet the needs of today’s technologically advanced world. Next, adherence to the new set of guidelines must be enforced by an outside group or auditor to determine adherence to the agreement. Such inspections will ensure mutual trust among countries and provide a stable environment for biometric technology deployment.⁴⁴

Currently, there is no incentive for countries to follow the *OECD Guidelines*, while there is, for example, with the U.S. Department of Commerce development of the Safe Harbor program to comply with European Union privacy directives. Yet, WPISP found in a comparative study of privacy and defense of critical information policies in Canada, South Korea, the United Kingdom and the United States that there is an emerging norm for “countries [to] have clear policies and objectives with approaches that are consistent with their individual culture.” This bodes well for the future of data privacy and biometrics deployment, as uniform laws among countries would increase the range of deployment for devices, as well as boost interoperability.⁴⁵

The OECD Directorate for Science, Technology and Industry also commissions various reports and working papers. One such paper provides an interesting background for privacy development and what role biometrics might play. The report highlights user insensitivity to low-level security threats and people’s affinity for this arrangement because of convenience and ease. There exists, then, a constant balancing act between *Security and Privacy v. Convenience and Use*. Biometrics, thankfully, may solve that problem by functioning as a noninvasive way of protecting people and maintaining their personal information. Ultimately, the verdict is still to be rendered on biometrics as privacy defender versus offender.⁴⁶

Assessing the European Union’s Attempts at Privacy

Directive 95/46/EC is the European Union’s most recent attempt to cement privacy as a right for all Europeans. But its predecessor, *(EC) 45/2001*, which will be called *Directive 45* for short, initiated privacy policies and data protection schemes in various bureaucracies and mem-

⁴³ Virginia Franke Kleist, “Building Technologically Based Online Trust: Can the Biometric Industry Deliver the Online Trust Silver Bullet?,” *Information Systems Management* 24 (2007): 328.

⁴⁴ OECD Directorate for Science, Technology and Industry, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data...”

⁴⁵ OECD Directorate for Science, Technology and Industry, “Working Party on Information Security and Privacy: The Development of Policies for the Protection of Critical Information Infrastructure (CII),” [http://www.oalis.oecd.org/oalis/2006doc.nsf/LinkTo/NT00007766/\\$FILE/JT03221273.PDF](http://www.oalis.oecd.org/oalis/2006doc.nsf/LinkTo/NT00007766/$FILE/JT03221273.PDF).

⁴⁶ OECD Directorate for Science, Technology and Industry, “At a Crossroads: ‘Personhood’ and Digital Identity in the Information Society,” <http://www.oecd.org/dataoecd/31/6/40204773.doc>.

ber states. A May 2008 compliance audit—nicknamed “Spring 2007”—of the regulation was completed with surprising and inspiring results for privacy proponents.

Directive 45 provided for a data protection officer (DPO). The time of the appointment provided a way to classify agencies in privacy level categories—one through three, with one being the lowest level and three the highest. Category 1 agencies had no DPO during the audit, Category 2 agencies had an officer in place for less than two years and Category 3 agencies had an officer in place for more than two years. What was consistent, however, is that in nearly every agency the DPO only serves in that capacity on a part-time basis, while he or she performs other functions, such as legal counsel.⁴⁷

In some agencies, the DPO only spends about 10 to 20 percent of their work time dedicated to data and privacy protection. But the office of the European Data Protection Supervisor (EDPS) suggests appointing a DPO full-time for a set period to perform his or her duties to create greater independence. The three principal organs of the European Union—the Commission, Council and Parliament—all have a full-time DPO.⁴⁸

The ultimate consequence of “Spring 2007” was greater compliance with *Directive 45*, because “it has encouraged the appointment of a DPO in every institution and operational agency.” Additionally, the audit provoked most institutions and agencies to develop an inventory of operations concerning personal data. Negatively, the EDPS found a low level of notification in most of the agencies with the DPO.⁴⁹

Continuation of the Safe Harbor Program

Directive 95/46/EC (Directive) was enacted in October 1998 to prohibit the transfer of personal data to non-European Union countries that do not meet an “adequacy” standard for privacy protection. The U.S. Department of Commerce, in consultation with the European Commission, developed the Safe Harbor Program to allow companies and organizations to certify that they maintain the necessary privacy protection standards as mandated by the *Directive*.⁵⁰

The Safe Harbor Program provides U.S. and EU firms with numerous benefits. The most significant accruing specifically to the United States are:

1. All 27 Member States of the European Union will be bound by the European Commission’s finding of adequacy
2. Companies participating in the safe harbor program will be deemed adequate and data flows to those companies will continue;
3. Member State requirements for prior approval of data transfers either will be waived or approval will be automatically granted; and

⁴⁷ European Data Protection Supervisor, “Measuring Compliance with Regulation (EC) 45/2001 in EU Institutions and Bodies (“Spring 2007”),” http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Inquiries/2008/08-05-14_Report_Spring_2007.pdf.

⁴⁸ *Ibid.*, 5.

⁴⁹ *Ibid.*, 10.

⁵⁰ The U.S. Department of Commerce’s International Trade Administration, “Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000,” http://www.export.gov/safeharbor/SH_Privacy.asp.

4. Claims brought by European citizens against U.S. companies will be heard in the United States subject to limited exceptions.⁵¹

U.S. companies and organizations must agree to follow the seven principles on data security and privacy as outlined in the *Directive* (See List 1 in appendix). Thousands of companies and organizations are Safe Harbor-certified. They must undergo a recertification annually by either performing a self-assessment of adherence to the seven principles on data security and privacy principles or hire a third-party to perform the assessment.

The Safe Harbor Program has received a fair amount of criticism for being a weak protector of privacy, because the program does not take into account state, national and other international laws. Moreover, since the European Union passed a directive and not a regulation, for it to be effective, member states must implement national laws—causing delays and sometimes confusion and contradiction with existing laws and procedures. Wells, Courtney and Vogel explain that, while a U.S.-based corporation or entity without any assets in Europe would be safe simply relying on the Safe Harbor Principles, those that have assets inside of Europe will be subject to further national legislation, which could be stricter than the *Directive*.⁵²

1. Eurodac and Other Centralized Databases

In 2002, a system known as “Eurodac” was established to assist in determining which member states are competent for asylum applications, to prevent forum shopping, and to facilitate the application of the Dublin Convention.⁵³ The principle area of concern was the establishment of a central database, however it was noted that the need for central storage of biometric data essential for the use of biometrics for identification purposes is balanced with a number of special safeguards on data protection, in order to compensate for the additional risks inherent in such model. Today the Eurodac is fully operational and has undergone numerous reviews in recent years. The fourth annual report on the system satisfied the European Commission’s misgivings about the Central Unit of Eurodac, but it did highlight some of the delays in disseminating biometric and other information among EU member states. In some countries, for example, it can take more than 30 days to send a single set of fingerprints.⁵⁴

A spring 2007 Supervision Coordination Group inspection of the Eurodac system focused on three areas with potential problems: special searches,⁵⁵ further use and data quality.⁵⁶ At the

⁵¹ The U.S. Department of Commerce’s International Trade Administration, “Safe Harbor Overview,” http://www.export.gov/safeharbor/SH_Overview.asp.

⁵² Steven A. Wells, Mark Courtney and Peter Vogel . “UnSafe Harbor: No Common Denominator in Privacy Compliance,” *Computer Law Review & Technology Journal* 9, no. 1 (2004), <http://www.libraries.wvu.edu>.

⁵³ Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of “Eurodac” for the comparison of fingerprints for the effective application of the Dublin Convention, 2000 O.J. (L 316) 1[*hereinafter* Eurodac]. Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities-Dublin Convention, 1997 O.J. (C 254) 1. Interestingly, Denmark opted not to participate or be bound by the regulation establishing Eurodac.

⁵⁴ Europa: Activities of the European Union, “ ‘Eurodac System,’ ” <http://europa.eu/scadplus/leg/en/lvb/l33081.htm>.

⁵⁵ Special searches are queries made to Eurodac that are legally limited to requests for personal data made by individuals.

⁵⁶ Secretariat of the Eurodac Supervision Coordination Group, “Coordinated Supervision of Eurodac: Activity Report 2005-2007,” http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/08-04-21_Eurodac_activity_report_2005-2007_EN.pdf.

onset of Eurodac, special searches were conducted inappropriately, but that problem has since been corrected. That area will be monitored in the future and users will be trained on how to avoid possible abuse, errors and educated on the data subjects' privacy rights. Eurodac fingerprints cannot be used to identify a person's country of origin for an asylum application, and there were no abuses of this rule—despite increased use of the system by police and other law enforcement entities. The largest issues concerning Eurodac, however, stems from the quality of fingerprint images. About six percent of the fingerprint images submitted to Eurodac are unusable because of poor quality, which creates difficulties for the data subject and the Eurodac users.⁵⁷

Laws relating to Travel Documents

The original **Schengen Information System (SIS)** was set up in the 1980's to allow police forces and consular agents from the Schengen countries⁵⁸ to access data on specific individuals (i.e. criminals wanted for arrest or extradition, missing persons, third-country nationals to be refused entry, etc.) and on goods which have been lost or stolen.⁵⁹ The development of a second-generation system known as "SIS II" was authorized pursuant to Council Regulation (EC) No 2424/2001 of December 6, 2001, which will include the inter-linking of alerts and the use of biometric information.⁶⁰ **The SIS II system**, scheduled to begin in December 2008, is experiencing numerous delays because of its technical complexity. Currently, the program is still being implemented. Likewise, the Visa Information System (VIS) is meeting similar difficulties and remains unimplemented on the large scale. Further negotiations between the European Council and Parliament concerning the regulation and passing relevant legislation are needed.⁶¹ The VIS legislation/regulation was passed in June 2007, though, "allowing consulates and other competent authorities to start using the system when processing visa applications and to check visas." This will allow police and law enforcement authorities to consult the data under certain conditions that should ensure a high level of data protection.⁶²

The Department of Homeland Security announced its **Electronic System for Travel Authorization (ESTA)** in 2008, allowing citizens from Visa Waiver Program (VWP) countries to submit applications beginning August 1 to enter the United States using a fully automated screening program. Currently, the ESTA program is optional, but it is expected to be mandatory

⁵⁷ Ibid.

⁵⁸ The term "Schengen" originates from a small town in Luxembourg. In June 1985, seven EU countries signed a treaty to end internal border checkpoints and controls. More countries have joined the treaty over the past years. At present, there are 15 Schengen countries, all in Europe. The 15 Schengen countries are: Austria, Belgium, Denmark, Finland, France, Germany, Iceland, Italy, Greece, Luxembourg, Netherlands, Norway, Portugal, Spain and Sweden. All these countries except Norway and Iceland are European Union members. What are the Schengen Countries?, <http://www.eurovisa.info/SchengenCountries.htm>. The Schengen Convention and related legislation (collectively referred to as the "Schengen aquis") abolished controls on people at the internal borders of the signatory countries and provide a common policy on visas and other security measures such as police and judicial cooperation, and to combat terror and organized crime. Ireland and the UK, although not Schengen countries, participate in certain aspects of the Schengen aquis that deal with cooperation between police forces and judiciaries, but have not ended border controls with other Schengen states. See Europa, Justice and Home Affairs, for information relating to Schengen at <http://europa.eu.int/scadplus/leg/en/lvb/l33020.htm>.

⁵⁹ *Id.*

⁶⁰ SIS II, *supra* note 152.

⁶¹ Bundesministerium des Innern, "Schengen and Visa Information System on Schedule," <http://www.statewatch.org/news/2007/apr/sis-and-vis-prel.pdf>.

⁶² European Digital Rights, "European Visa Information System Accepted by the EU Bodies," <http://www.edri.org/edrigram/number5.12/VIS-EU-adoption>.

for VWP travelers beginning January 12, 2009. All VWP travelers, regardless of age or type of passport, must present machine-readable passports to the appropriate authority and are bound by the following obligations, depending upon the issued date of a passport:

- Machine-readable passports issued or renewed/extended on or after October 26, 2006, require an integrated chip with information from the data page.
- Machine-readable passports issued or renewed/extended between October 26, 2005, and October 25, 2006, require a digital photograph printed on the data page or integrated chip with information from the data page.
- Machine-readable passports issued or renewed/extended before October 26, 2005, have no other requirements.

There are still 27 countries in the VWP, which allows travelers to stay in the United States for up to 90 days if the trip is for tourism or business. Otherwise, a visa is required for entry into the United States.⁶³

In July 2005, the **International Civil Aviation Organization (ICAO)** bound its 190 contracting states to issue machine-readable passports no later than April 1, 2010. About two-thirds of ICAO contracting states currently use machine-readable passports. For states not on the machine-readable system and lacking technological expertise or finances, ICAO developed a plan of action called *The Universal Implementation Machine Readable Travel Documents* and encouraged donor states and international financial institutions to help by providing funds.⁶⁴

Individual Countries⁶⁵

Canada

Like the United States' major privacy legislation, Canada's has not undergone an extensive review or change in decades. *The Privacy Act of 1982* remains the definitive law relating to data protection and other related matters. Another law, *The Personal Information Protection and Electronic Documents Act of 2000 (PIPEDA)*, provided some guidance on new technologies, but it still does not amend or update *The Privacy Act*.

In May 2008, the Office of the Privacy Commissioner of Canada released a statement for *10 Quick Fixes to The Privacy Act*. Boldly, the statement also said: "The 10 Quick Fix changes we are currently proposing to the Privacy Act are not meant to be the definitive statement on Privacy Act reform. *The Act is in desperate need of a complete overhaul* [emphasis added]." The 10 Quick Fixes are listed in the appendix under List 2. Little else has changed in Canada concerning biometrics or data protection and privacy.

⁶³ U.S. State Department Bureau of Consular Affairs, "Visa Waiver Program (VWP)," http://travel.state.gov/visa/temp/without/without_1990.html.

⁶⁴ International Civil Aviation Organization, "Machine Readable Passports to be Issued Worldwide by 2010," http://www.icao.int/icao/en/nr/2005/pio200507_e.pdf.

⁶⁵ New Zealand and Japan are omitted from the countries section, because nothing noteworthy has occurred on the biometric or data privacy fronts in the past two years.

Australia

In recent years, various proposals have been introduced in Australia to implement a national identification card, with the most recent attempt occurring in spring 2006. After a review of the costs and social impact of the policy, as ordered by former-Prime Minister John Howard, the plan was scrapped, although that did not stop the government from introducing a health and services “smartcard” as a means to prevent welfare fraud. The card replaces 17 other benefits cards and contains a large amount of personal information—including a digital photo, a number and signature with a scannable microchip holding an address, date of birth and details about dependents.⁶⁶

The Asia-Pacific Economic Cooperation (APEC) is an organization mirroring the OECD and World Trade Organization in that it promotes free and open trade within the context of various other goals. Collectively, the 21 APEC members account for half of the world’s gross domestic product and 47 percent of worldwide trade.⁶⁷ Although Japan and New Zealand are also members of APEC and party to the *APEC Privacy Framework*, Australia has touted the agreement more than the other two countries.

The Framework espouses nine principles concerning privacy: preventing harm, integrity of personal information, notice, security safeguards, collection limitations, access and correction, uses of personal information, accountability and choice (See List Three in appendix).⁶⁸ Although not as in-depth or widely accepted as the *OECD Guidelines*, *The Framework* provides another example of developing data privacy norms.

On the national level, *The Privacy Act of 1988* remains as the main privacy law governing Australia. The law considers biometric information sensitive, among other types of personal information, such as political opinions and religious beliefs. The Australian Law Reform Commission, on behalf of the attorney general, determined in a September 2007 report that biometrics require a special level of protection in some circumstances, because “the risk of revealing an individual’s cultural origins or providing information that can allow an individual to be impersonated.” The Commission also suggested, to ensure the *The Privacy Act’s* timeliness with new technology development, that the law should be drafted for “handling of information in any context, and should not refer to specific types of technology.”⁶⁹

⁶⁶ Margaret Jackson and Julian Ligerwood, “Identity Management: Is an Identity Card the Solution for Australia?,” *Prometheus* 24 (2006): 380-381.

⁶⁷ Asian-Pacific Economic Cooperation, “FAQs—Asia-Pacific Economic Cooperation,” <http://www.apec.org/apec/tools/faqs.html#>.

⁶⁸ Australian Government Attorney-General’s Office, “APEC Privacy Framework,” [http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/\(03995EABC73F94816C2AF4AA2645824B\)~APEC+Privacy+Framework.pdf/\\$file/APEC+Privacy+Framework.pdf](http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf).

⁶⁹ Australian Law Reform Commission, “Review of Australian Privacy Law: An Overview,” <http://www.austlii.edu.au/au/other/alrc/publications/dp/72/overview.pdf>

Appendix

*Table 1: Support of and Opposition to Anti-terrorist Actions Post-9/11 (in percent)*⁷⁰

Measure	Support	Oppose	Don't Know
Wiretap telephone	69	29	2
Intercept e-mail	72	23	5
Intercept ordinary mail	57	39	4
Examine Internet activity	82	15	3
Examine telephone records	82	17	1
Examine bank records	79	20	1
Track credit card purchases	75	21	4
Examine tax records	75	24	1

*Table 2: President's Rally Around the Flag Effect*⁷¹

President	Approval Boost (in points)	Event
Franklin D. Roosevelt	12	Japanese attack on Pearl Harbor
John F. Kennedy	13	Cuban Missile Crisis
George H.W. Bush	14	Iraq invasion of Kuwait; Gulf War
George W. Bush	35*	9/11 terrorist attacks

*The 35 point jump was the largest in recorded history, as Bush's approval rose from 51 percent on September 7, 2001, to 86 percent on September 14, 2001.

⁷⁰ Survey conducted by NPR, Kaiser Family Foundation and Kennedy School of Government from October 31, 2001, to November 12, 2001. Table amended and used from Epstein, Ho, King, and Segal, "The Supreme Court During Crisis..." 17.

⁷¹ Ibid. Table created from information listed in the article.

List 1: Principles of Directive 95/46/EC for the U.S. Safe Harbor Program

- **Notice**—Individuals must be informed that their data is being collected and about how it will be used.
- **Choice**—Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.
- **Onward Transfer**—Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
- **Security**—Reasonable efforts must be made to prevent loss of collected information.
- **Data Integrity**—Data must be relevant and reliable for the purpose it was collected for.
- **Access**—Individuals must be able to access information held about them and correct or delete it if it is inaccurate.
- **Enforcement**—There must be an effective means of enforcing these rules.⁷²

*List 2: 10 Quick Fixes to the Canadian Privacy Act of 1982*⁷³

Recommendation One: Create a legislative “necessity test” which would require government institutions to demonstrate the need for the personal information they collect.

Recommendation Two: Broaden the grounds for which an application for Court review under section 41 of the *Privacy Act* may be made to include the full array of privacy rights and protections under the *Privacy Act* and give the Federal Court the power to award damages against offending institutions.

Recommendation Three: Enshrine a requirement for heads of government institutions subject to *The Privacy Act* to assess the privacy impact of programs or systems prior to their implementation and to publicly report assessment results.

Recommendation Four: Amend the *Privacy Act* to provide the Office of the Privacy Commissioner of Canada with a clear public education mandate.

Recommendation Five: Provide greater discretion for the Office of the Privacy Commissioner of Canada to report publicly on the privacy management practices of government institutions.

Recommendation Six: Provide discretion for the Privacy Commissioner to refuse and/or discontinue complaints the investigation of which would serve little or no useful purpose, and would not be in the public interest to pursue.

Recommendation Seven: Amend the *Privacy Act* to align it with *PIPEDA* by eliminating the restriction that the *Privacy Act* applies to recorded information only.

Recommendation Eight: Strengthen the annual reporting requirements of government departments and agencies under section 72 of the *Privacy Act*, by requiring these institutions to report to Parliament on a broader spectrum of privacy-related activities.

⁷² Official Journal of the European Communities, “Directive 95/46/EC...”

⁷³ Office of the Privacy Commissioner of Canada, “Privacy Act Reform: 10 Quick Fixes,” http://www.privcom.gc.ca/legislation/pa/pa_reform_e.asp.

Recommendation Nine: Introduction of a provision requiring an ongoing five-year Parliamentary review of the *Privacy Act*.

Recommendation Ten: Strengthen the provisions governing the disclosure of personal information by the Canadian government to foreign states.

*List 3: Nine Principles of the APEC Privacy Framework*⁷⁴

Preventing Harm: Personal information protection should be designed to prevent the misuse of such information. The Preventing Harm Principle recognizes that one of the primary objectives of the *APEC Privacy Framework* is to prevent misuse of personal information and consequent harm to individuals. Therefore, privacy protections, including self-regulatory efforts, education and awareness campaigns, laws, regulations, and enforcement mechanisms, should be designed to prevent harm to individuals from the wrongful collection and misuse of their personal information.

Notice: Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include: a) the fact that personal information is being collected; b) the purposes for which personal information is collected; c) the types of persons or organizations to whom personal information might be disclosed; d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information; e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.

Collection Limitation: The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.

Uses of Personal Information: Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except: a) with the consent of the individual whose personal information is collected; b) when necessary to provide a service or product requested by the individual; and c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.

Choice: Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information. Determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes.

Integrity of Personal Information: Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.

⁷⁴ Australian Government Attorney-General's Office, "APEC Privacy Framework," [http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/\(03995EABC73F94816C2AF4AA2645824B\)~APEC+Privacy+Framework.pdf/\\$file/APEC+Privacy+Framework.pdf](http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf). Descriptions of the principles are shortened from the larger report.

Security Safeguards: Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. This principle recognizes that individuals who entrust their information to another are entitled to expect that their information be protected with reasonable security safeguards.

Access and Correction: Individuals should be able to: a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them; b) have communicated to them, after having provided sufficient proof of their identity, personal information about them; i. within a reasonable time; ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; iv. in a form that is generally understandable; and, c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.

Accountability: Personal information controllers should be accountable for complying with measures that give effect to the principles stated previously. When personal information is to be transferred to another person or organization, whether domestic or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these principles.