

Fall 9-15-2012

The International Review | 2012 Fall/Winter

Michael Rhee
New York Law School

Follow this and additional works at: https://digitalcommons.nyls.edu/international_review_newsletter



Part of the [International Law Commons](#)

Recommended Citation

Rhee, Michael, "The International Review | 2012 Fall/Winter" (2012). *The International Review Newsletter*.
3.
https://digitalcommons.nyls.edu/international_review_newsletter/3

This Article is brought to you for free and open access by the Center for International Law at DigitalCommons@NYLS. It has been accepted for inclusion in The International Review Newsletter by an authorized administrator of DigitalCommons@NYLS. For more information, please contact camille.broussard@nyls.edu, farrah.nagrampa@nyls.edu.

THE INTERNATIONAL REVIEW

CENTER FOR INTERNATIONAL LAW | NEW YORK LAW SCHOOL

FALL/WINTER 2012 | VOLUME 15, ISSUE 1

 **COMPARATIVE LAW**

Should nations regulate digital photo editing? PAGE 16

Virtually anyone with a computer can digitally alter photographs and other images. While many users make minor alterations, others carry out dramatic changes. Some argue that digitally altering photos is a harmless act, but many are calling for restrictions on or minimum standards for that practice. Do nations regulate digital photo alterations? Are they proposing new laws? And does international law address this issue?

 **INTERNATIONAL CIVIL LIBERTIES**

Protecting the privacy of biometric data: National and international efforts PAGE 29

As public and private sectors across the world increase their collection of people's biometric information, societies are debating whether the benefits of using such data will outweigh their costs, including their effects on the right to privacy. How exactly does the use of biometrics affect privacy? How do different regions of the world address the use of biometrics and its implications on privacy? Does international law play a role?

 **INTERNATIONAL BUSINESS LAW**

How do nations and international law address bribery? PAGE 29

Bribery, a form of corruption affecting every nation in the world, leads to environmental damage, a weakening of the rule of law, and even the loss of life, among other problems. Many believe that bribery occurs more often now than ever before. How do various nations around the world deal with bribery? Does international law address this problem, and does it do so effectively? What more can be done to curb bribery?



Protecting the privacy of biometric data: National and international efforts

Over the past several decades, the public and private sectors in many nations have been increasing their collection of people's biometric information by using new technologies. Proponents say that using biometric data can provide society with more convenience and also enhance its security. But others worry that the increasing use of biometrics could threaten fundamental rights such as the right to privacy.

What is a biometric? How do the public and private sectors collect and use such data? How exactly does the use of biometrics affect the right to privacy? Which laws in the United States currently address privacy? Do they deal specifically with biometrics, and are they considered effective in protecting the privacy of such data? And how does international law regulate this issue?

What is a biometric?

A biometric is a biological or behavioral feature of a person which can be recorded and analyzed by certain technologies. Some biological features include a person's DNA; blood samples;

Recent technological advances have allowed the public and private sectors to collect and process biometric data – such as a person's DNA, blood samples, the structure of his retina, and even his typing rhythm on a computer keyboard – much more quickly and use such data for many more purposes.

fingerprints; the color of his iris and the structure of his retina; the shape and placement of individual parts of his face; the size, shape, and surface area of his hands; and the pattern of blood vessels throughout his body, according to various analysts. Behavioral features include a person's voice and speech patterns, his typing rhythm on a computer keyboard, and even the way he walks.

Recent technological advances (such as the development of small but powerful microprocessors, high resolution cameras, and portable scanners) have allowed the private and public sectors to collect and process biometric data much more quickly and use such data for many more purposes. According to trade publication *IEEE Spectrum* magazine: "Industry forecasters say the market for biometric data-collection systems will double or triple in size over the next five years."

Public sector uses of biometric data and technology

Law enforcement organizations have long collected biometric data – such as DNA samples, facial images, and fingerprints from detained individuals, criminal suspects, and prisoners – to see whether the collected information matches that already stored in large databases. Government agencies use face, iris, and hand scanning devices to verify their employees' identities before allowing them to enter restricted areas or view sensitive data. As

technological progress advances every year, governments are now using biometric data for a growing list of purposes.

Border crossings and passports: Many nations use biometric technologies to facilitate and record the entry of all foreign visitors, and screen out individuals such as criminals and terrorists. For example:

- In 2004, the European Union passed a regulation (No. 2252/2004) requiring its 27 member nations to issue passports and travel documents which contain both a person's facial and fingerprint images.
- Since 2007, all passports issued by the United States have electronic chips containing a person's information already printed on his passport along with his digital photograph which is compatible with facial recognition technology, according to the U.S. Department of State.
- Many nations – such as Australia, Japan, South Korea, the United Arab Emirates, and EU member states – are collecting

biometric information of visitors who arrive at their borders, reported *CNET.com*, a technology news webpage.

- Since 2004, the U.S. Department of Homeland Security has been administering one of the world's largest biometric collection efforts called the U.S. Visitor and Immigrant Status Indicator Technology (or US-VISIT) Program where border officials scan and store the fingerprints and facial images of nearly every person arriving at over 100 airports and 15 seaports and then compare the biometric data with information contained in existing databases, said a report issued by the National Biometric Security Project, a nonprofit research organization.

Expanded law enforcement and military applications: Technological advances are allowing governments to collect and incorporate biometric data into already existing databases while allowing them to use such data for military purposes. Recent examples include the following:

- In 2009, the Federal Bureau of Investigation (or FBI) announced that it would incrementally replace its Integrated Automated Fingerprint Identification System – which has been described by the FBI as the "largest biometric database in the world" containing the fingerprints, mug shots, and criminal histories of over 70 million people – with what is called the Next Generation Identification (or NGI) system. The NGI system will add more

biometric information to existing criminal histories, including palm prints, iris scans, and digital facial images.

- In 2011, *The New York Times* reported that the government of Afghanistan (which is battling an insurgency composed of the Taliban and foreign terrorist fighters) had a goal to “fingerprint, photograph, and scan the irises of every living Afghan.” One U.S. official said that the military will use this information to identify and track thousands of terrorist and insurgent suspects.

National ID cards: Many countries have long issued standard national identity cards which contain basic information about its holder such as his name, photo, and date of birth. They are now in the process of adding people’s biometric data. For instance:

- In 2004, India began a mandatory program – called the National Population Register – to create a “comprehensive identity database” containing the biometric information of its entire population of 1.2 billion people. According to digital rights advocacy group Electronic Frontier Foundation, officials are visiting villages throughout India where they set up a “processing center” to scan every person’s fingerprints, irises, and faces.
- The parliament in Israel (called the Knesset) passed a law in December 2009 which calls on the government to scan the fingerprints and facial images of all Israeli citizens – through a series of pilot programs – in preparation for a new biometric ID card, reported the *Jerusalem Post*.
- In January 2012, Argentina implemented a presidential decree to create what the Electronic Frontier Foundation described as a “new centralized, nationwide biometric ID service” (called the “Federal System of Biometric Identification”) which will allow the government to put a person’s biometric information – such as fingerprint and facial scans – on the national ID card.

Voter registration: To curb voter fraud and other irregularities, governments are carrying out voter registration drives where they collect biometric data from eligible voters:

- Many African nations – including Burkina Faso, Kenya, Nigeria, Sierra Leone, and Tanzania, among others – are registering eligible voters using biometric technology, said the Ghana Center for Democratic Development.
- Since 2008, Brazil began using biometric technology to verify the identity and eligibility of voters during an election. News site *Txchnologist.com* noted that “Brazil plans to make its entire election process biometric by 2018.”

Private sector uses of biometric data and technology

Along with governments, the private sector uses biometric data. Many banks, for instance, use such data in place of, say, ATM cards. In the late 1990s, Bank United in Texas (now called Bank United Corp.) began to install ATM machines which scan the irises of participating customers before allowing them to carry out a transaction. Industry analysts report that other businesses let customers register images of their fingerprints so that they can pay for their merchandise using a finger scanner, which, in turn, withdraws money from a bank account or places a charge on a credit card.

Examples of the most recent uses of people’s biometric information in the private sector include the following:

- In June 2012, Facebook announced that it had acquired Face.com, a company whose facial recognition software identifies

people in online photos. “Our facial recognition analytics are able to identify faces well, despite difficult circumstances like poor lighting, poor focus, subjects wearing eyeglasses, facial hair, and even Halloween costumes,” said a Face.com spokesperson. Analysts say that the software will allow Facebook users to identify people in the photo albums of other users.

- Bars in cities such as Chicago and San Francisco are using cameras with facial detection software developed by Texas-based Scene Tap, LLC, to broadcast real-time information on the number of people in their establishments, their ages and gender, and the ratio of men to women, which users can use to decide which bar to visit.
- South Korea-based SK Holdings Co. manufactures information kiosks which use cameras installed with facial identity software to determine the gender and age of the people who stop to use them, according to the *Wall Street Journal* which calls them, “one of the first in the world.” The kiosks can tailor their advertisements to match the attributes of the people standing in front of them.

How accurate are biometrics and biometric technology?

While many say that the use of biometric technology can bring more convenience to people’s everyday lives and even provide society with greater security, critics point out a major shortcoming – its accuracy can be highly uneven.

Facial recognition software, for instance, produces high rates of error. Many times, it wrongly accepts the identity of some people (known as false positives) while rejecting the correct identities of others (also called false negatives), say analysts. Notable examples include the following:

- According to the Electronic Privacy Information Center, Boston’s Logan Airport in 2003 had tested facial recognition systems at security checkpoints using volunteers posing as



terrorists. The airport decided not to use these systems after they had “correctly identified the volunteers 153 times and failed to identify the volunteers 96 times.”

- A couple who had accidentally swapped their passports in February 2011 at Manchester airport in the United Kingdom still passed through the facial recognition scanners which compared their faces to their passport photos, reported the *Daily Mail*.

On the other hand, while many say that the use of fingerprints in identifying people has been much more reliable, critics point out that doing so is still not foolproof. For instance:

- Two South Korean women in January 2010 managed to pass through a multimillion-dollar biometric immigration system in Tokyo International Airport by using fake passports and wearing invisible tape carrying the fingerprints of other people, reported *Homeland Security News*.
- In July 2012, James Makowski, a U.S. citizen, filed the first lawsuit against a fingerprint sharing program called Secure Communities – administered by the FBI and the Department of Homeland Security – after it had wrongly identified him as an illegal immigrant, reported the *Los Angeles Times*. Authorities had placed Makowski in a maximum security prison for two months before realizing their error.

Along with evading facial and fingerprint scans, experts also believe that people will soon be able to trick security systems which use iris scans. During an information security conference called Black Hat in July 2012, security researchers had printed out replica images of digitized irises and then used these images to trick a commercial eye scanning system “at a rate of 50 percent or higher,” reported the Electronic Frontier Foundation.

Does the use of biometrics affect privacy?

Along with concerns over the accuracy of technologies which measure biometric data, other critics say that their use in certain ways could threaten and undermine fundamental rights, including the right to privacy.

What is privacy? No single and agreed-upon definition exists for the word “privacy.” Still, many legal experts generally define it as the “right to be let alone” from the undue interference of government officials, private organizations and businesses, and even fellow citizens. (That definition comes from a dissent written by U.S. Supreme Court Justice Louis Brandeis in a 1928 case called *Olmstead v. United States*.)

According to Jethro K. Lieberman, a professor at New York Law School, and author of *Privacy and the Law*, society would become “self-conscious and guarded” if government agents or private detectives followed everyone’s movements, kept a record of their financial transactions, and regularly monitored cell phone conversations and Internet use. Without privacy, says Lieberman, “people would become afraid to talk openly, to express opinions that might antagonize others.” This could then lead to what he calls a “conformist nation” where the lack of privacy stifles creativity and even legitimate dissent.

Just as people define privacy in many ways, there are different kinds of privacy, though this article will address only two types related to the debate concerning biometrics.

Physical privacy: One type is physical privacy which is to be “left physically alone,” says Lieberman. “It means to be apart from others so that they cannot see or hear what you are doing.” Such privacy also includes “the right to control access to one’s body and personal space,” say legal analysts Herbert Fineberg and Erica Intzekostas. Governments protect physical privacy by passing laws which



prohibit peeping into other people's windows, prevent the police from barging into people's homes without sufficient justification, or which criminalize stalking. These laws also prohibit the electronic surveillance of private conversations without a court order, and also the gathering of blood samples and DNA swabs without a legal justification.

In the area of biometrics, some groups worry that governments could violate people's physical privacy by locating them and tracking their physical movements through, for instance, high resolution cameras installed in public locations which capture facial or retinal images and then match such information with already collected images in a database. Critics such as those at the Electronic Frontier Foundation point out that the FBI – during a 2010 presentation on biometrics – had stated that its Next Generation Identification system will be “able to track people as they move from one location to another.”

But does such biometric technology actually exist? The *Washington Post* reported in 2007 that researchers at the West Virginia University Center for Identification Technology Research were working on technology which will capture “images of people's irises at distances of up to 15 feet, and of faces from as far away as 200 yards,” which is around the length of two football fields. *BBC News* said that “face recognition is being used by some authorities to scan crowds to identify suspects whose faces have been entered into a database.”

Such a technological development could also lead to a loss of anonymity which could then affect other rights, including those protecting free speech, say observers. When Argentina announced in 2012 that it was creating a new centralized biometric ID service containing people's fingerprint and facial images, a critic told the *Miami Herald* that such a development could discourage political protests – a form of speech – by making it easier for authorities to identify and retaliate against demonstrators.

Information privacy: Another type of privacy is information privacy which is “the freedom to control access to information about oneself” – such as that dealing with the intimate details of our lives, including our criminal background, financial situation, health status, and political and religious affiliations – and keeping it private, according to biometric experts Peter Gregory and Michael Simon. “When intimate facts are revealed,” says Jethro Lieberman of New York Law School, “our privacy is invaded as surely as if someone barged into our homes to discover those facts.”

Legal analysts note that many nations have passed various laws which protect information privacy. These laws may, for example, prohibit government agencies and private organizations from sharing certain information which they had gathered from people during the course of their operations. They may also prohibit them from gathering the information deceptively or from using the information in ways which differ from the original purpose for collecting it.

While nations have been addressing how best to protect information privacy for many centuries, doing so has become more difficult in the face of rapid technological advances (such as those concerning biometrics) over the last decade. “New machines, new processes, new techniques make it much easier to enter a room, eavesdrop, spy, collect, and transmit data about people,” says Lieberman of New York Law School. “It is easier than ever to collect, store, and transmit extremely personal data about almost anyone.”

The use of biometrics and biometric technologies could threaten people's information privacy in many different ways, say observers.

Function creep: Under a phenomenon which many analysts describe as “function creep,” a government agency or private business may use the data it had collected for one function and then slowly expand their use – in a creeping effect – to other purposes without disclosing its action to the people from whom it had collected personal information.

Analysts say that function creep had existed long before the creation of biometric systems. For example, they point out that various government agencies and private businesses routinely ask people for their Social Security numbers (or SSNs) to verify their identities. According to the Social Security Administration (or SSA), the federal government had created Social Security numbers “for the sole purpose of tracking the earnings histories of U.S. workers, for use in determining Social Security benefit entitlement, and computing benefit levels.” Nearly every legal resident of the United States has such a number. But now, “the SSN's very universality has led to its adoption throughout government and the private sector as a chief means of identifying and gathering information about an individual,” said the SSA.

Along with SSNs, governments and businesses could use other personal data (including biometric information) for purposes which go beyond the original reason for their collection.

Experts point out, for instance, that biometric data such as iris and retinal scans contain sensitive health information which people may not want to disclose to others. According to ophthalmologists, clots in blood vessels on the retina can indicate a risk of stroke and other conditions. Also, they say that additional blood vessels may grow in cavities near the retina in people with diabetes. “There's no question the eye has always been the window to the body,” said Emily Chew of the National Eye Institute during an interview with the *Wall Street Journal*. While some businesses may use such data to target consumers with new services, others believe that health insurance companies may be able to use them against the interests of their customers.

Access and security: Observers worry aloud whether governments and private businesses can effectively secure and protect biometric information from access and use by unauthorized personnel, criminals, and those engaged in identity theft. According to the Electronic Frontier Foundation: “A Social Security number can always be cancelled and reissued if it's compromised, but it's impossible for someone to get a new eyeball if an attacker succeeds in seizing control of his or her digital biometric information.” The U.S. Government Accountability Office adds: “Loss of such information may lead to identity theft or other fraudulent use of the information, resulting in substantial harm, embarrassment, and inconvenience to individuals.”

Such scenarios in the case of biometric data are not farfetched. In 2009, the *Daily Mail*, a British news daily, announced that it had hired a computer expert to test the security of the now defunct national identity card which contained a person's biometric data on a computer chip. Using a cellphone and laptop computer, the expert (within a few minutes) managed to copy the data on the test ID card, create a new card, and then change the data on it.

Because of these concerns over physical and information privacy, many nations have scaled back their plans to use biometric technology. For instance:

- While EU regulations require member states to issue passports which contain people’s facial and fingerprint images, the United Kingdom (an EU member) has been issuing biometric passports since 2006 which contain only digitized facial images. In May 2010, amid a public outcry over privacy concerns, the UK government ended plans to add fingerprints to biometric passports which were supposed to start in 2012.
- In March 2012, France’s Constitutional Council – that nation’s highest body of judicial review – struck down a law calling for the creation of a national biometric ID card (which would contain fingerprints, facial images, and information such as a person’s height and eye color) to prevent identity fraud. The Council said that the range of data to be collected by the government “cannot be considered as proportional to the meant purpose.”

Responding to critics of biometrics and the use of biometric technologies

Supporters of the use of biometric data and technology believe that while these various concerns over the use of biometrics are valid, some may be overblown.

First, in response to concerns that governments and private companies will use biometrics to track people, many observers point out that many entities – such as banks; credit card companies;

Along with concerns over the accuracy of technologies which capture and process biometric data, critics say that such data used in certain ways could threaten and undermine certain fundamental rights, including the right to privacy.

bridge, subway, and tunnel authorities; online businesses; and even our workplaces – are already doing so without even using biometrics. Also, close to one billion people are willingly (and in many cases, openly) placing vast amounts of personal information on the Internet – including their photos, dates of birth, exact physical locations, recent purchases, and dating status – through sites such as Facebook, Foursquare, and Twitter which allow others to track them. So supporters ask why critics are singling out the use of biometric data for greater scrutiny.

Second, supporters agree that while some people have evaded biometric systems at security checkpoints, they believe that further advances in technology (combined with human personnel who double-check people’s identities) will make biometric technology more reliable in the future. They also point out that no one has reported instances of large-scale security breaches where hundreds or thousands of people have regularly evaded biometric security checkpoints or instances where computer hackers have stolen vast amounts of biometric data.

Third, in response to fears that governments and businesses will engage in function creep or that thieves will use biometric data to carry out identity fraud, some analysts say that these concerns apply “literally to any system that creates a unique identifier for an individual, and is not a problem specific to biometrics.” In order to address function creep and identity theft, observers say that governments and businesses must pass and adhere to laws and standards protecting the privacy of biometric data.

How does the United States address biometrics and its effects on privacy?

Even with the assurances given by those who support the use of biometric data and technologies, many people still express worry over their effects on individual privacy. Skeptics say that existing U.S. laws (passed decades ago) do not adequately protect privacy in the face of fast-changing developments in biometric technologies, and argue that legislatures must adopt new laws or amend current ones to ensure privacy.

Biometric data and federal laws: Does the United States have laws which broadly protect all types of privacy? And are there laws which specifically protect the privacy of a wide range of personal data (including people’s biometric data) from abuse and misuse by the government and private entities?

Legal observers say that the U.S. Constitution – the highest law of the land – does not explicitly guarantee a broad “right to privacy” which covers all kinds of privacy such as information and physical privacy. (In fact, the word “privacy” does not appear at all in the Constitution.) Instead, the Constitution prohibits federal, state, and local governments from violating certain aspects of privacy. For example, the “Fourth Amendment search-and-seizure provision protects a right of [physical] privacy by requiring warrants before [the] government may invade one’s internal space.”

says the Congressional Research Service (or CRS), a non-partisan research department for the U.S. Congress.

In the area of information privacy, CRS says that no single federal law comprehensively protects the privacy of all personal information held by different levels of governments across the United States. Instead, it notes that “a patchwork of federal and state laws exists to protect the privacy of certain personal information.”

At the federal level, the most important is the *Privacy Act of 1974* (or 1974 act) which regulates how only federal agencies collect, use, and disseminate personal information collected from people during the course of their respective duties. According to the National Biometric Security Project, the United States enacted this law in response to concerns that government officials and others could affect privacy rights if they misused or abused the growing use of computerized databases which contain people’s personal information such as their names, dates of birth, addresses, and Social Security numbers. For the first time, a statute explicitly stated that federal agencies were “legally responsible for the protection of personal information.”

Under the 1974 act – which does *not* apply to state and local governments or to private companies – a federal agency:

- Must allow a U.S. citizen or permanent resident (upon request) to review, make copies of, and correct his personal information on file at the federal agency, though the law does make certain exceptions.

- May only collect and maintain personal information about an individual “as is relevant and necessary to accomplish a purpose of the agency.” That is to say, the agency may not collect more information than it needs to carry out a certain task.
- May disclose someone’s personal data only if the agency receives his permission or if it discloses the data under certain situations specified in the 1974 act such as when a court requests that data.
- May not share and compare personal data with another agency unless they have a written agreement to do so.
- Must establish appropriate “administrative, technical, and physical safeguards to ensure the security and confidentiality” of its records.

What exact kinds of personal information does the 1974 act protect? To start, the act does not use the term “personal information.” Instead, it uses the term “record,” which is any information about an individual, “including, *but not limited to*, his education, financial transactions, medical history, and criminal or employment history.” But each of these examples, in and of itself, is still not a record. To be considered a record, each example must also contain a person’s name or an identifying number (such as a Social Security number) or identifying symbol, including a person’s finger or voice print or a photograph. (Nowadays, rather than using the term “record,” many analysts use the term “personally identifiable information” – or PII – which the U.S. Government Accountability Office defines as “information that can be used to locate or identify an individual, such as names, aliases, Social Security numbers . . . that is linked or linkable to an individual.”)

Does the 1974 act specifically protect the privacy of biometric data? Analysts note that while the 1974 act does mention biometric data such as fingerprints, it does not explicitly view such data (in and of themselves) as PII (on par with a person’s name or date of

birth) which need to be safeguarded by the government. But at the same time, the 1974 act does not say that a biometric can never be viewed as a PII. (The specific examples of PII were not meant to be exhaustive, says the act itself.)

To avoid this ambiguity from the very start, why didn’t the federal government simply protect biometric data (in and of themselves) as PII in the 1974 act? To place matters in context, the federal government had implemented the 1974 act – nearly four decades ago – during a time when “biometric technology was in its infancy,” and when biometrics could not be readily used to “commit fraud or penetrate security,” said the National Biometric Security Project. But given rapid technological advances in the last decade alone – where scanners can now identify a person by viewing, say, only his face – analysts have been debating whether the 1974 act (along with subsequently passed laws) should now treat a biometric itself as a stand-alone PII which needs privacy protections.

In 2010, the National Biometric Security Project issued a report (“Biometrics & Personally Identifiable Information”) where it describes how the federal government slowly began to view biometric information (gathered from millions of people) as a stand-alone PII which it had to protect from misuse and abuse even though the 1974 act did not explicitly provide that protection. Some developments include the following:

- In May 2007, the Office of Management and Budget (or OMB) – the Executive branch department responsible for the overall management and functioning of every federal agency – issued Memorandum M-07-16 which provides detailed instructions to all federal agencies on implementing safeguards to prevent the breach of PII and also instructions on reporting and responding to breaches of such information. In its first footnote, the memorandum explicitly says that “biometric records” are a



form of PII which, by themselves, can identify a person. (This is in contrast to the 1974 act which does not view biometric information as a stand-alone PII.) Still, many note that the memorandum is neither considered a law nor did it amend the 1974 privacy act.

- The White House began to issue instructions to federal agencies which implicitly said that the federal government now views biometrics as PIIs which, by themselves, can identify people. For instance, in June 2008, the White House issued two directives (called NSPD-59, and HSPD-24, both of which contain the exact same instructions) requiring executive branch agencies to use “mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing” of the biometric information of known and suspected terrorists.

Despite these developments, the 1974 act still does not formally view biometric data as stand-alone PIIs. But legal observers say that, *in practice*, the federal government seems to protect biometric data as stand-alone PIIs.

In recent years, several members of Congress have introduced legislation which would require the 1974 act to classify biometric data as PIIs. For example, in October 2011, Senator Daniel Akaka (D-HI) introduced the *Privacy Act Modernization for the Information Age Act of 2011* (S. 1732). Among other purposes, the bill would have explicitly classified biometric records as stand-alone PIIs on par with a person’s name, Social Security number, and date of birth. But Congress did not enact this bill into law.

Existing U.S. laws do not adequately protect privacy in the face of fast-changing developments in biometric technologies, say critics. The *Privacy Act of 1974*, for instance, still does not formally protect the privacy of biometric data. They argue that legislatures must adopt new laws or amend current ones to ensure privacy.

Those who support the updating of the 1974 act, including groups such as the Center for Democracy & Technology, a Washington, D.C.-based non-profit organization promoting Internet freedom, argues that “the wording of the [1974] Act renders it ill-equipped to meet many of the privacy challenges posed by modern information technology,” among other perceived shortcomings.

If the 1974 act applies only to the federal government, are there federal laws which regulate how private sector entities collect, use, and disclose people’s personal information, including biometric records? Analysts say that no single federal statute comprehensively addresses and protects the privacy of all personal information (including biometric records) held by every entity in the private sector.

Instead, CRS notes that the federal government has passed – “on a sector-by-sector basis” over a period of many years – individual laws regulating how the private sector collects, uses, and discloses personal information. For example, to protect the personal health information of patients held by private entities, the federal government in 1996 enacted the *Health Insurance Portability and Accountability Act* (or HIPAA), which, among other aims, sets certain procedures that health care organizations must use to protect the privacy and security of that information, including

their biometric data. But HIPAA applies only to the healthcare sector.

Still, to this day, no one federal statute sets a single standard on how all private entities – ranging from health care providers to financial institutions to small businesses – must specifically protect people’s biometric data (that is, if they collect and use that data). But over the years, members of Congress have proposed legislation which would place comprehensive restrictions on how private companies gather, use, and disclose such data.

In a recent effort, then-Senator John Kerry (D-MA) and Senator John McCain (R-AZ) in April 2011 introduced the *Commercial Privacy Bill of Rights Act of 2011* (S. 799) which, according to the *Wall Street Journal*, would have created “the nation’s first comprehensive privacy law.” Specifically, the law would have established a single set of rules on how all private sector entities collect, use, disseminate, and protect PIIs, including names, addresses, Social Security numbers, and biometric data such as “fingerprints and retinal scans.” But Congress did not vote to pass this bill.

Biometric data and state laws: Along with the federal government, individual states have passed their own laws protecting personal information (including biometric records), and which would apply both to their own governments and also to the private sector within their respective jurisdictions. But the provisions of these laws and the extent to which (and how) they protect personal information vary greatly from state to state.

According to the National Conference of State Legislatures (or NCSL), 10 states recognize a right to privacy in their state constitutions. (They are Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina and Washington.) But as in the case of the U.S. Constitution, nearly all of these individual state constitutions recognize a right to privacy rooted specifically in the Fourth Amendment where people have a right to protect their private affairs, homes, papers, and other possessions from unreasonable searches and seizures and against unreasonable invasions of privacy unless a court issues a warrant. (For those state constitutions which do not explicitly mention a right to privacy, the NCSL says that individual state courts have issued decisions which do so.)

While several state constitutions recognize a right to privacy, many don’t explicitly say whether they protect the privacy of biometric information. But some actually do. For example:

- Under the *Biometric Information Privacy Act* (740 ILCS 14), passed by Illinois in 2008 and which applies only to the private sector, a party has several duties concerning what it calls “biometric identifiers” (defined as “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry”). For example, a party must establish a schedule for the destruction of

biometric identifiers once it completes the purpose of gathering the data; inform a person before collecting, capturing, or purchasing his biometric information; and may not “sell, lease, trade, or otherwise profit” from a person’s biometric information.

- In 2001, Texas passed a law addressing how the private sector may use biometric identifiers. Under the *Business and Commerce Code* (Section 503.001), a person may capture another person’s biometric identifier (or disclose it) for a commercial purpose only when he first informs that other person and then receives permission to do so. In contrast to the 2008 Illinois statute, the Texas law does not require commercial entities to set policies for the destruction of biometric information, says analyst Robert Weiss.
- In 2010, legislators in the New Hampshire House of Representatives introduced a bill (HB 1409) which would have prohibited any government agency or private entity in the state from issuing an ID card or using an ID system that “requires the collection or retention of an individual’s biometric data,” which it widely defined as fingerprints, palm prints, facial features, behavior characteristics such as handwriting speed, voice data, and retinal scans, among other methods. (But the bill would have made certain exceptions.) Legislators rejected the bill by a 267-39 vote. According to an industry publication, *Security Management* magazine, various companies said that the terms of the law were too broad, and that the law would have “[deprived] businesses of providing their customers with a cutting edge technology that promotes security and privacy rather than eroding it.”

How do international and regional agreements protect the privacy of biometric information?

Decades ago, nations began to adopt treaties and agreements which broadly called on them to respect and protect people’s privacy. But their provisions neither provided specific guidance on how to do so nor did they say which types of privacy to protect. In subsequent years, these nations and various global organizations began to pass other agreements with much more detailed requirements on protecting people’s privacy, including the privacy of their personal data. But even with such developments, these later agreements did not provide clear guidance on whether their privacy protections extended to biometric information.

Even today, no international treaty or regional agreement explicitly protects the privacy of biometric information. But some analysts believe that these existing agreements implicitly protect such data. What are some of these treaties and agreements?

1948 Universal Declaration of Human Rights (or Universal Declaration): Adopted by the UN General Assembly, the Universal Declaration calls on nations to recognize and respect a wide variety of human rights for “all peoples” such as the right to life and liberty, equal protection of the laws, and freedom from slavery, discrimination, and arbitrary arrest, among many others. In the area of privacy, Article 12 says that “no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence . . .” and that “everyone has the right to the protection of the law against such interference or attacks.”

But the Universal Declaration neither defines the term “privacy” nor does it mention other terms such as “personal data” or even “biometrics.” As a general matter, declarations issued by the United Nations (including the Universal Declaration) are mostly

aspirational *statements* on how nations should address a certain issue which is not specifically covered by a formal international treaty or agreement, say legal observers. They also don’t have the force of law. In fact, many legal experts do not view the Universal Declaration as an international treaty.

1966 International Covenant on Civil and Political Rights (or ICCPR): This treaty, also adopted by the UN General Assembly, calls on its more than 160 state parties to recognize and protect a wide range of fundamental civil and political rights, including the right to life, freedom of association, and the right to a fair trial. (Unlike the Universal Declaration, the ICCPR is an enforceable international treaty. But experts note that the Universal Declaration served as the foundation of the ICCPR and many other treaties.) A body called the UN Human Rights Committee (comprised of independent experts) monitors the implementation of the ICCPR by its signatory nations and also issues authoritative interpretations – called “general comments” – of specific treaty provisions which nations should then follow.

Article 17 of the ICCPR specifically addresses the right to privacy. But its text is virtually identical to Article 12 of the Universal Declaration. (That is to say, the ICCPR does not provide any more guidance on protecting privacy than the Universal Declaration.) Also, Article 17 neither defines terms such as privacy nor does it mention others, including personal data or biometrics.

In 1988, the Human Rights Committee issued – in what is called General Comment No. 16 – an interpretation of and guidelines for carrying out Article 17. (The number of an ICCPR article doesn’t always correspond with its general comment, including this particular case.) Along with addressing various other issues, General Comment No. 16 provides broad guidelines on how nations must specifically protect personal information. It calls on nations (in paragraph 10) to do the following:

- Use laws to regulate “the gathering and holding of personal information on computers, data banks, and other devices, whether by public authorities or private individuals or bodies.”
- Take “effective measures” to ensure that unauthorized individuals may not receive, process, and use other people’s personal information.
- Give people the right to: (a) know which public authorities or private entities are storing their information, (b) know what information such entities are storing, (c) know the purpose of storing it, (d) correct their personal information, and (e) call on these entities to delete information which was collected illegally.

One can argue that the term “personal information” would logically include biometrics, and that nations (as a result) would have to apply the protections mentioned in General Comment 16 to biometrics. Still, the general comment does not explicitly mention the term “biometrics.” Also, observers note that governments and companies still did not extensively use biometrics when the Human Rights Committee passed the general comment in 1988.

1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (or the OECD guidelines): During the latter half of the 20th century, more and more industrialized nations began to develop and use technologies which not only quickly collected and processed all sorts of data, but also transmitted them instantly across national borders, say analysts. To protect such data from unauthorized use and disclosure, individual countries began to pass their own data protection laws. (Nations

in continental Europe generally refer to laws which protect the privacy of personal data simply as “data protection laws” while English-speaking nations call them “privacy protection laws,” say experts.)

But, according to experts, the level of protection of these laws varied widely from one nation to the next, and, as a result, hindered many economic sectors (such as banking and finance, among others) from easily and quickly transmitting data to each other and to other nations where they did business. Also, existing agreements during that time (such as the Universal Declaration and the ICCPR) did not provide practical guidance.

To address these shortcomings, the Organisation for Economic Co-operation and Development (or OECD) – a forum where 30 of the world’s most industrialized nations gather to pass various agreements on economic cooperation – adopted in 1980 its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which includes an “Explanatory Memorandum” that gives context and details concerning the guidelines.

As its name suggests, these *voluntary* guidelines established – for the first time on a global basis – many basic principles on protecting the privacy of personal data which every OECD member nation should incorporate into its own laws and policies while still promoting the free flow of information. Personal data is defined as “any information relating to an identified or identifiable individual” (i.e., any information which can be used to identify a certain person), though the guidelines do not give specific examples.

These guidelines soon “emerged as the universal foundation for the formulation of national privacy legislation,” according to the National Biometric Security Project. But experts do not view the OECD guidelines as a legally binding international treaty. (Again, adherence is voluntary.) What are some of the principles in the OECD guidelines which protect personal privacy?

- Under the “Collection Limitation Principle” in paragraph 7, nations should pass laws which limit the collection of personal data. It also calls on data collectors to gather information through “lawful and fair means,” and with the “knowledge and consent of the data subject.” Concerning the latter phrase, while the Explanatory Memorandum (in paragraph 52) explains that nations should not use “hidden data registration devices” or deceptive means when gathering personal data from people, it doesn’t define terms such as “consent.”
- Under the “Data Quality Principle” in paragraph 8, nations should pass laws which require data collectors to gather only information that is “relevant” for specified purposes.
- If a data collector wants to use someone’s data for other purposes (or disclose or make them available to others), it must – under the “Use Limitation Principle” in paragraph 10 – receive permission from that person or must have authority to do so under the law. But paragraph 10 does not say what exactly would constitute “permission.”
- The “Security Safeguards Principle” in paragraph 11 says that nations should pass laws calling on data collectors to protect personal information from unauthorized access or use, loss, destruction, or disclosure by using “reasonable security safeguards.”
- Under the “Individual Participation Principle” in paragraph 13, nations should give individuals the right to obtain copies of their personal information from a data collector within a “reasonable

time” and at a cost that is not “excessive.” (But paragraph 13 does not define these terms.) In addition, if a data collector denies a person’s request for a copy of his personal information, it should explain why. Under paragraph 59 of the Explanatory Memorandum, the right of a person to access his personal data should be “simple to exercise . . . and should not involve any legal process or similar issues.”

- Under the “Accountability Principle” in paragraph 14, nations should pass laws which hold data collectors accountable for complying with these various principles, though it does not say whether other parties hired by a data collector to process information would be held responsible for mishandling or abusing such data. But according to paragraph 62 of the Explanatory Memorandum, “sanctions against [for instance] breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information . . .”
- The guidelines also say, under paragraph 17, that an OECD nation should restrict the transborder flow of personal data between itself and another nation when that other nation does not “substantially observe” the OECD guidelines.

The OECD acknowledges that these various provisions are vague, but note that they are supposed to serve only as guidelines. According to the Explanatory Memorandum, “the detailed implementation [of the OECD guidelines] . . . is left in the first place to Member countries,” and is “bound to vary according to different legal systems and traditions.”

Do the principles and protections in the OECD guidelines apply to people’s biometric information? Do they, for example, call on data collectors to gather only biometric information which is relevant for a specific purpose and to gather such data only with the informed consent of a person? Do the OECD Guidelines also give a person the right to ask data collectors for his biometric information? The answers to these questions are still debatable.

Many say that the OECD guidelines, including its definition of personal data (“any information relating to an identified or identifiable individual”), do not explicitly mention biometrics. (When the OECD had passed the guidelines over three decades ago, many nations did not extensively use biometrics.) But others can argue that the definition of personal data would implicitly include biometrics since people can possibly use such data to identify specific individuals. Others can also say that the drafters of the OECD guidelines had deliberately crafted a broad definition of personal data to take into account the evolving nature of personal data.

As the use of biometric technology began to grow since the passage of the guidelines, the OECD in 2004 issued a report called *Biometric-Based Technologies* (DSTI/ICCP/REG(2003)2/FINAL) where it broadly surveyed the “benefits and limitations of biometric-based technologies.” It also discussed various privacy and security concerns regarding the collection and use of biometric data, including function creep and the use of biometric technologies to carry out surveillance.

To address these specific concerns, the 2004 report makes several recommendations. For example, it calls on nations to “communicate openly and honestly about any planned [biometric] system.” In addition, nations should, “whenever possible, develop opt-in voluntary enrollment systems” for the collection of biometric data.

Furthermore, biometric data should be collected “openly and with the consent of the user.” Moreover, data collectors should not store people’s biometric templates “in a central system.” The 2004 report also recommends several approaches to ensure that nations protect the security and privacy of biometric data. It says, for instance, that nations can pass “generalized or specific criminal sanction” to protect biometric systems.

While the report makes these various recommendations in the area of biometrics, analysts point out that they are voluntary and do not amend the OECD Guidelines themselves. (The report says, for instance, that its recommendations for securing the privacy of biometric data “are provided for discussion purposes in the hope that they will stimulate further development.”) Also, the report does not determine, once and for all, whether nations should view biometrics as a form of “personal data” which they should protect using the broad principles of the OECD guidelines. Still, some argue that because the OECD issued a report which specifically addresses the use of biometrics and its related technologies, that organization implicitly considers biometric data as a form of personal data which should receive certain privacy protections.

1981 Council of Europe: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data: Along with OECD members, nations in Europe began to worry about the privacy effects of technology which automatically processes personal data. While they began to pass their own laws to address this concern, the provisions of these laws varied widely from one jurisdiction to the next.

In an attempt to streamline these various approaches, the Council of Europe (an organization established to “promote democracy and protect human rights” in Europe) adopted in 1981 a regional treaty – called the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* – requiring its 47 member nations (nearly all in Europe) to establish, in their respective legal systems, minimum responsibilities and duties for data collectors who automatically process personal data. In addition, the 1981 Convention calls on members to give certain legal rights to people when their governments (and also the private sector) automatically process their personal data. Many of these responsibilities and rights resemble those found in the OECD Guidelines. For example:

- Under Article 5, when a data collector – such as a government agency or a private company – collects personal data which will undergo automatic data processing, it must collect such information “fairly and lawfully,” and store it for “specified and legitimate purposes.”
- Nations and private entities may automatically process personal data which reveal sensitive information (such as those concerning a person’s racial origin, political opinions, religious and other

beliefs, and health status) but only when they implement certain safeguards, according to Article 6.

- Article 7 calls on nations to implement what it calls “appropriate security measures” to protect personal data stored in automated files from accidental destruction or loss and to prevent unauthorized access and dissemination.
- A data collector must, under Article 8, let a person know whether it is storing his personal data and allow him to see and correct such data “without excessive delay or expense.”
- When a data collector violates these domestic laws or regulations, Article 10 says that a nation must “establish appropriate sanctions and remedies.”
- Under Article 12, a member nation may not invoke the Convention “to justify interference with transborder data flows for reasons which have nothing to do with the protection of privacy (for example, hidden trade barriers),” according to an Explanatory Report which was issued along with the Convention, and gives more guidance to nations as they implement that agreement.

Does the protection of personal data under the Convention also extend to biometric data? Currently, the Convention provides only a broad definition of personal data – “any information relating to an identified or identifiable individual” (which is the same as the one found in the OECD Guidelines) – and does not list any specific examples. The term “biometric data” does not even appear anywhere in the agreement.

Still, as in the case of the OECD Guidelines, one could argue that personal data would implicitly include biometric data. For example, the Explanatory Report says that a nation, under Article 6, may process personal data revealing sensitive information only using certain safeguards, and that its examples of sensitive data are “not meant to be exhaustive.” Therefore, sensitive data could include biometric information since such data can be used to identify others. In addition, the Convention does not specifically prohibit nations from protecting biometric data as part of personal data. Furthermore, because the Convention requires nations to adopt their own laws and regulations to protect personal data, it leaves many terms undefined, thus allowing nations to decide on their own whether to protect biometric data under the Convention.

But others can point out that the Council of Europe had adopted the agreement during a time (the early 1980s) when the use of biometrics was in its infancy, and that its drafters may not have intended to include such data.

1995 European Union Data Protection Directive: Along with the Council of Europe, a separate organization called the European Union (or EU) also addresses the privacy of personal data in Europe.



As its name implies, the EU is an economic and political union of 27 independent and sovereign states (all located in Europe). They are bound together by a series of complex international treaties. To increase the economic competitiveness of the EU (which is the largest trading bloc in the world) and also to prevent future conflicts, these treaties created common institutions to manage certain economic and political areas of mutual concern such as trade, finance, environmental protection, and agricultural policy. (This is in contrast to the much narrower focus of the Council of Europe, which is to promote democracy and human rights.) In turn, these institutions have passed European-wide laws (addressing a wide variety of issues) which every EU member nation must incorporate into its domestic legal system.

To protect personal data, the EU undertook its own attempt separate from the one taken by the Council of Europe. In 1995, it passed a European-wide law – known as Directive 95/46/EC, or simply, the 1995 directive – which established minimum standards on how all member governments and private entities in Europe must process (i.e., how they collect, store, use, disclose, and protect) people’s personal data. Under the directive (which is still in effect today), all EU members must ensure that their own data protection laws meet these minimum standards. At the same time, each EU member nation may adopt stricter standards than the minimum ones set by the 1995 directive. In fact, many did so.

So what minimum standards does the 1995 directive require EU nations to set? Analysts note that many of its provisions overlap with those found in the OECD Guidelines and also in the 1981 Convention, *but include more details*. For instance:

- In the preamble – which explains why the EU decided to adopt the 1995 directive in the first place – Paragraph 26 says that the directive (and its protections) must apply to “any information” which can be used to identify another individual, either directly or indirectly. (But the directive doesn’t apply in cases where people use their own data to carry out personal or household activities.)
- But what exactly is personal data? In the main body of the directive, Article 2 defines that term in the same way as the OECD Guidelines and the 1981 Convention – “any information relating to an identified or identifiable natural person.” But in various commentaries, the EU adds that personal data “can be anything from a name, a photo, an email address, your bank details, your posts on social networking websites, your medical information, or your computer’s IP address.” Under Article 2, personal data also include an “identification number” such as a person’s date of birth and home address, among other examples, say observers.
- Under Article 6, EU nations must incorporate several broad principles into their own domestic data protection laws. For example, every EU member nation must ensure that personal data is processed fairly and lawfully, and is collected for “specified, explicit, and legitimate purposes.” Article 6 also says that when data collectors gather information, they must only collect what is relevant and must not go beyond what is needed to carry out a certain task. (Legal observers call this the principle of proportionality.)
- Under Article 7, governments and private entities may process a person’s personal data only if he “unambiguously” gives consent or unless they need to comply with a legal obligation or carry out

a task in the public interest, among other situations. But Article 7 does not describe what exactly constitutes unambiguous consent. Many companies now simply assume that a person automatically provides his consent unless he explicitly says otherwise, say observers.

- While the aim of the 1995 directive is to protect a broad range of personal data, it gives what the EU says is “extra protection” to sensitive data. Specifically, Article 8 prohibits governments and private entities from processing personal data which reveals a person’s “racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership,” and also data concerning “health or sex life” unless that person gives his consent, among other conditions and safeguards.
- Under Article 10, entities collecting a person’s data must identify themselves and give the purpose for processing that data.
- A person has a right, under Article 12, to request a data collector to send him information on whether it has been gathering his personal data, the kinds of data it has collected, and the reasons for doing so. The data collector must reply to the person making such a request “without excessive delay or expense.” But Article 12 does not say when exactly a data collector must fulfill a person’s request or how much money it should charge when processing it.
- EU member nations may, under Article 13, restrict the scope of these data protection rights to safeguard their national security, public security, and economic and financial interests.
- Under Article 17, data collectors must implement “appropriate technical and organizational measures” to protect personal data from accidental loss or destruction, alteration, and unauthorized disclosure or access. But the 1995 directive does not explicitly say what steps a data controller must take when it discovers a security breach or whether (after discovering a breach) it must contact certain authorities or even the people from whom it had collected data.
- Under Article 25, data collectors may transfer personal data to a third country, but only if that country “ensures an adequate level of protection.” The data collectors themselves determine whether a third country’s protection is adequate by considering, among other criteria, the nature of the data, the purpose of their transfer, and the rules of data protection in the third country.

Do the 1995 directive and its protections apply to biometric information? The definition of “personal data” in Article 2 does not explicitly mention biometrics. Still, do EU governments believe that “personal data” should include a person’s biometric information? According to the National Biometric Security Project, “the issue as to whether and under what circumstances biometric information is considered ‘personal data’ has not been resolved among [EU] member states.” It noted, for example, that individual member states have offered varying definitions of the term “personal data” and have also decided on their own whether to include biometrics. Some member states, including the Czech Republic, Estonia, and Slovenia, explicitly include biometrics as personal data and, accordingly, protect such information, according to the European Commission.

To clarify whether the 1995 directive protects biometric information, an EU expert group in August 2003 adopted a report – called “Working document on biometrics” (12168/02/EN) – saying that when member nations process people’s biometric data,

they must “fully respect the data protection principles provided for in Directive 95/46/EC.” Some of the major points from the 2003 report include the following:

- The definition of “personal data” does include biometric information. In fact, the 2003 report said: “It appears that biometric data can always be considered as ‘information relating to a natural person’ as it concerns data which provides, by its very nature, information about a given person.”
- Because personal data includes biometric information, the only lawful way to collect biometric information in the EU is for governments and private entities to follow the provisions of the 1995 directive.
- So, for example, under Article 6, EU nations may process biometric data for only “specified, explicit, and legitimate purposes,” and, conversely, may not process such data if doing so “would be incompatible with the purpose for which the data was collected.” Also, under the principle of proportionality (also in Article 6), EU governments and private entities may only collect biometric information which is relevant and does not go beyond what is needed to carry out a certain task.
- Under Article 7, governments and private entities may process a person’s biometric data only if he gives consent.
- Under Article 8, data collectors may not process biometric data if doing so reveals information about a person’s racial or ethnic origin, or information about their health or sex life, unless they receive permission from that person. (It noted that “in biometric systems based on face recognition, data revealing racial or ethnic origin may be processed” as long as the data collector implements specified safeguards to protect that data.)
- Under Article 10, the 2003 report said that the EU must require entities collecting biometric data to identify themselves and give the purpose for processing a person’s personal data. It added that “systems that collect biometric data without the knowledge of data subjects” – including distance facial recognition – “must be avoided.”

Although the EU adopted the 2003 report, doing so did not (in and of itself) change the text of the 1995 directive. Also, EU nations are not legally obligated to implement its conclusions. As a result, the level of protection for biometric data continued to vary widely across Europe.

Decades ago, nations began to adopt treaties which called on them to respect and protect people’s privacy. But these agreements did not say whether their privacy protections extended to biometric data. Even today, no international treaty or regional agreement explicitly protects the privacy of biometric information.

2012 European Union Data Protection Regulation: Shortly after the passage of the 1995 directive, people in the EU (and around the world) began to use and rely heavily on breakthrough technological developments such as the Internet – in conjunction with innovative electronic devices – to carry out daily tasks such as banking transactions and retail purchases, and also to communicate and exchange information with other people through e-mail, mapping, social networking, and video services. According to an EU press release: “17 years ago, less than 1% of Europeans used

the Internet.” Now, in the EU alone, 250 million people use the Internet daily.

But along with greater convenience, these technological developments and services have given governments and businesses a much better ability (and also ample opportunities) to capture, collect, use, store, and transfer vast amounts of personal data on a scale and at a depth unimaginable just a few years ago. According to a 2011 poll carried out by Eurobarometer, 70 percent of Europeans are “concerned that their personal data may be misused,” and are also worried that “companies may be passing their data to other companies without their permission.”

Recent media stories revealing how technology and Internet companies collect people’s personal data and how they address security breaches involving such information have caused concern around the world. For example:

- In 2010, the *Wall Street Journal* reported that, when testing 100 iPhones and Android apps, it found that “more than half were transmitting identifying details without the user’s knowledge.”
- In that same year, Google admitted that its Google Maps Street View cars (which have special cameras mounted on their roofs) had mistakenly collected certain data from unprotected Wi-Fi networks as they drove through various cities in Europe, the United States, and elsewhere, according to *The New York Times*.
- In April 2011, Sony issued a public warning that hackers may have gained access to the personal information of 77 million customers on its Playstation Network, but it waited one week to inform its customers about the security breach, reported the *Guardian*, a British newspaper.

Does the 1995 directive (in its current form) adequately address these various concerns? Officials say no and even point out many shortcomings. For example, they note that the 1995 rules were “introduced at a time when many of today’s online services and the challenges they bring for data protection did not yet exist.”

In addition, officials said that allowing each EU member state to implement its own data protection standards under the 1995 directive has “led to an uneven level of protection for personal data, depending on where an individual lives or buys goods and services.” It added: “The result is a fragmented legal environment with legal uncertainty and unequal protection for individuals.” In the case of the Google Maps Street View cars which had collected certain

data through people’s Wi-Fi networks, various data protection authorities responded differently to this development, noted officials. While some called on Google to destroy immediately the data it had collected and also to pay fines, others asked the company to retain the data as evidence but did not impose any fines.

Furthermore, EU companies have long complained about the 1995 directive. To comply with what the EU itself describes as a “patchwork of national rules in 27 Member States,” businesses must spend up to €2.3 billion (or nearly US\$3 billion) a year.

Also, “companies that are active throughout the EU must notify up to 27 different national authorities” every year about their data protection efforts, which can cost them €130 million (or nearly US\$166 million) annually.

To address these various concerns, the EU in January 2012 announced a comprehensive effort to reform its 1995 data protection directive. Specifically, it introduced a proposed “regulation” (called the *Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, or, simply, the 2012 regulation) which, if implemented, would replace the 1995 directive and require every EU member nation to incorporate a single set of stringent rules for data protection into their respective domestic legal systems. In contrast, the 1995 directive allows EU member nations to adopt varying degrees of data protection as long as they comply with its established minimum standard.

The 2012 regulation does not discard all of the provisions in the 1995 directive. Instead, many provisions in the 1995 directive remain in the proposed regulation such as those which call on nations to ensure that personal data is processed fairly, lawfully, and for specific and legitimate purposes. Still, the 2012 regulation proposes what EU officials believe are significant improvements over the 1995 directive. For example:

- With a single set of rules which all EU nations must adopt into their domestic legal systems, every person across Europe will have the same rights in the area of data protection, said officials.
- In contrast to Article 12 of the 1995 directive, Article 12 of the 2012 regulation says that when a person requests a data collector to send him information on whether it has been gathering his personal data, a data controller must reply within a month of the request, and must also process that request “free of charge” unless the extent of the request is “manifestly excessive.”
- Under Article 17 (dubbed the “right to be forgotten”), every EU nation must give a person the right to call on a company to erase his personal data if “the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed,” among other situations. EU officials add that data collectors “must prove that they need to keep the data rather than [your] having to prove that collecting your data is not necessary.”
- A data collector must obtain a person’s explicit consent before processing his personal data. Specifically, Article 7 says that “the [data collector] shall bear the burden of proof for the data

subject’s consent to the processing of their personal data for specified purposes.” In contrast to Article 7 of the 1995 directive, the data collector cannot assume that a person had automatically given his consent simply because he did not provide it explicitly.

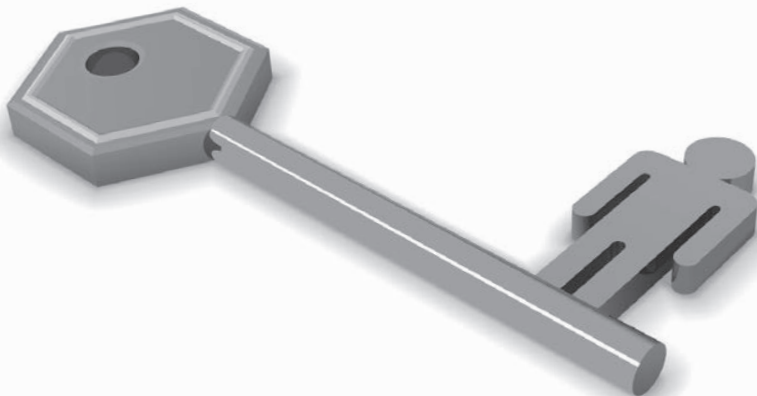
- As in the case of Article 8 of the 1995 directive, Article 9 of the 2012 regulation specifically prohibits the processing of sensitive personal data unless a person gives his consent.
- In contrast to the 1995 directive, when a company discovers a serious data breach, it must (under Article 31 of the 2012 regulation) notify government authorities no later than 24 hours after becoming aware of the breach.
- Article 41 of the regulation says that a data collector may transfer personal data to a third country only if an agency called the European Commission has “decided that the third country . . . ensures an adequate level of protection.” This is in contrast to Article 25 of the 1995 directive which allows a data collector to determine on its own whether to transfer data to a third country.
- A company will no longer have to submit a report explaining how it protects personal data to 27 different national authorities, “a requirement that has led to unnecessary paperwork,” said the EU. Instead, it only has to report to its own national data protection authority since the 2012 regulation will require every EU nation to enforce a single set of data protection rules.

What is the status of the proposed regulation? Officials say that EU member states are currently discussing the regulation in the European Parliament. If the EU adopts the regulation in its final form (tentatively scheduled for 2014), it will come into force in 2016.

Do the 2012 regulation and its protections apply to people’s biometric information? As in the case of the 1995 directive, the 2012 regulation does not explicitly protect biometric data. For example, the definition of “personal data” found in Article 4 of the 2012 regulation does not explicitly include biometric data. In addition, Article 9 (which again prohibits governments and data collectors from processing specific categories of sensitive personal data) does not explicitly list biometric data.

Officials are currently debating whether EU nations should specifically include biometric data in Article 9 of the 2012 regulation. When the EU released its proposed regulation in January 2012, it also issued a document called *Commission Staff Working Paper: Impact Assessment* (SEC(2012) 72) where officials examined the possible effects of the regulation in different areas of EU policymaking. Among many other issues, the document noted that “the increase in biometric data is a common worry among [EU] citizens, and respondents [to a survey] want it to be addressed in the new legal framework.” Including biometric data as part of Article 9, said the document, “would vigorously improve the level of protection for those data, and [that] this option would have a very high positive impact,” noting that the domestic laws in several nations – such as the Czech Republic, Estonia, and Slovenia – consider biometric data as “sensitive data.”

At the same time, the document said that “expanding the categories of sensitive data [in Article 9] to biometric . . . data would also entail substantial costs as it would require data controllers to adapt their procedures and technical system to more stringent rules concerning the processing of such data.” EU officials are still trying to decide whether to include biometric data in Article 9.



In the meantime, analysts point out that Article 33 of the 2012 regulation calls on data collectors to carry out what it calls an “assessment” of how processing certain kinds of personal data (including biometrics, among others) could affect people’s rights. It specifically says that these assessments must include a general description of the processing operation, a summary of the risks of this operation on people’s rights and freedoms, and a description of measures, safeguards, and other mechanisms “to ensure the protection of personal data.”

2004 APEC Privacy Framework: Europe has several of its own agreements to protect the privacy of personal data. Industrialized nations look to the 1980 OECD Guidelines. How do other regions of the world such as East Asia address data protection?

In November 2004, the leaders of the Asia-Pacific Economic Cooperation (or APEC) forum – a regional trade and economic organization of what are called “member economies” located in the Pacific Rim, including China, Japan, Russia, South Korea, and the United States – adopted a voluntary agreement called the *APEC Privacy Framework* which calls on its 21 members to implement a list of common principles within their domestic jurisdictions to protect the privacy of personal information while promoting business and commercial interests.

The voluntary principles of the Privacy Framework – which apply to both the public and private sectors in APEC member economies – largely replicate those found in existing agreements such as the 1980 OECD guidelines and the 1995 EU data protection directive. For example:

- According to Principle II (“Notice”), a data collector should provide people with “clear and easily accessible statements” which say that it is collecting personal information and also give the purpose for collecting such information, among other requirements.
- Principle III (“Collection Limitation”) says that a data collector should limit its collection of personal information to what is relevant for the purpose of collecting it in the first place and that such information should be obtained by lawful and fair means.
- Under Principle VIII (“Access and Correction”), APEC members should allow an individual to obtain his personal information from a data collector within a reasonable time and at a charge which is not excessive.
- When a data collector transfers personal information to another person or organization (either in-country or to another nation), Principle IX says that it should take “reasonable steps” to ensure that the recipients of such information will “protect the information consistently” with the principles of the Privacy Framework.

The Privacy Framework gives APEC member economies a broad range of methods to implement these principles, including “legislative, administrative, industry self-regulatory, or a combination of these methods.” It adds that “in view of the differences in social, cultural, economic, and legal backgrounds of each member economy, there should be flexibility in implementing these Principles.”

Do the Privacy Framework and its protections apply to biometric information? While the Privacy Framework defines “personal information” as “any information about an identified or identifiable individual,” it neither gives specific examples nor does it include the term “biometrics.” (At the same time, it does not explicitly prevent

nations from including biometric data as a form of personal data.) But the Privacy Framework also says that personal data includes information that, “when put together with other information, would identify an individual.” So one can argue that personal information could implicitly include biometric data.


2009 Madrid Resolution: While several agreements protect the privacy of personal data in specific regions of the world and also protect such data mainly in industrialized countries, no single agreement on data protection applies to every nation in the world. But recently, participants at a data protection conference passed a voluntary resolution which they hope will serve as the foundation for the first-ever global agreement on data protection.

In November 2009 in Madrid, Spain, during the 31st International Conference of Data Protection and Privacy Commissioners – a global forum where data protection authorities discuss privacy issues – participants passed a non-binding resolution called the “Joint Proposal on International Standards on the Protection of Personal Data and Privacy” (dubbed the Madrid Resolution) which establishes a minimum set of voluntary principles, rights, and obligations which nations “should strive” to incorporate into their respective legal systems when protecting data privacy but which must also help facilitate the international flow of data “needed in a globalized world.”

The Madrid Resolution – which applies to both the public and private sectors in individual nations (but, again, is voluntary) – largely contains major provisions found in existing international agreements regulating the processing and protection of personal data. For example:

- Article 6 says that a data collector must collect personal information fairly and lawfully.
- When a data collector processes information, it must do so (under Article 7) for “specific, explicit, and legitimate purposes,” and in a way which is relevant and not excessive in relation to these purposes, according to Article 8.
- Once a data collector obtains personal data, it should (under Article 9) delete such information when it no longer needs it to carry out a certain purpose.
- Under Article 13, nations may establish safeguards to protect sensitive data such as those which can reveal a person’s racial or ethnic origin, his religious and political views, or his health status.
- A nation may transfer personal data to another country but only if the country receiving the data has implemented the provisions of the Madrid Resolution, says Article 15.
- Under various articles, a nation must give a person the right to access and obtain his own personal data from a data collector.

Even though the Madrid Resolution is not considered binding international law, supporters hope that its provisions will serve as “the basis for the drawing up of a future universally binding agreement.” But they have not yet made progress towards this effort.

Does the Madrid Resolution protect the privacy of biometric information? As in the case of other existing international agreements, the Madrid Resolution does not explicitly include biometric data in its definition of personal data, which it defines as “any information relating to an identified natural person or a person who may be identified by means reasonably likely to be used.” At the same time, the Resolution does not contain any provision which would stop a nation from protecting the privacy of biometric data. 

Should nations regulate digital photo editing?

The widespread availability of sophisticated software programs (such as Adobe Photoshop) allows virtually anyone with a computer to digitally alter photographs and other images much more easily and frequently compared to decades past when doing so required painstaking work. While both professional and amateur users rely on such programs for minor alterations, others use them to make dramatic changes. For example, aging celebrities in print advertisements can look much younger, images of political rallies seem to contain hundreds of more people, and certain individuals have apparently disappeared from official government photographs.

While some argue that digitally altering photos is a harmless act, others believe that it could have certain harmful effects on society, and that nations should restrict or set minimum standards to regulate that practice. Do nations already have laws which regulate the digital altering of photos? Are they proposing new ones? Are these measures effective in their stated aims? And does international law address this issue?

The politics of altering photos and images

Why do people alter photos and other images? While the majority usually wants to correct blurry images and improve poor lighting, among other imperfections, people also alter photos for political reasons. Doing so, in fact, is not even a modern phenomenon. Historians note that governments have been altering photos and other images for over 100 years. The Soviet Union and Nazi Germany, for instance, had edited their photographs by removing officials who had fallen out of political favor. During the 2012 presidential election in South Korea, critics believe that supporters

of a certain candidate had digitally altered the photo of a campaign rally by adding hundreds of more people. Other examples include:

U.S. Civil War mix-and-match: In 1860, photographers had produced a majestic portrait of then-president Abraham Lincoln by superimposing his head on a preexisting photo of South Carolina politician John C. Calhoun. In another example, photographers had created a well-known Civil War image of Union general Ulysses S. Grant by manipulating the negatives of three different photos. They placed his head on the body of another person on horseback, and then superimposed this montage on the forefront of a field of captured Confederate soldiers, according to research carried out by the Library of Congress.

Beirut smoke or smudge? Adnan Hajji, a freelance photographer working for *Reuters*, had digitally altered a photograph of the aftermath of an Israeli air strike on Beirut, Lebanon, in August 2006 to show darker and larger plumes of smoke. After publishing the photo and realizing that it had been changed, *Reuters* fired Hajji (who blamed the excess dark smoke on smudge marks and fingerprints), and removed all of his photos from its database, reported *BBC News*.

Iran missile launch cut-and-paste: The Iranian state media in July 2008 digitally altered the photograph of a missile test exercise by adding an extra missile (along with its cloud fumes) to cover a grounded missile which had failed to launch. Several newspapers, including *The New York Times* and the *Chicago Tribune*, had featured the altered photograph on their front pages, not knowing that Iran had changed it.

Egypt at the head of the line: The government-controlled Egyptian daily *Al-Abram* digitally altered a photograph of Middle East leaders walking behind U.S. President Barack Obama at the White House in September 2010 by placing then-Egyptian president Hosni Mubarak at the very front of the procession. (Egyptian newspaper editors frequently retouch photos of government officials before publication to make them appear more prominent, said the *Guardian*, a British newspaper.) In defending the decision to alter the photo, the editor-in-chief of *Al-Abram* said: "The expressionist photo is . . . a brief, live, and true expression of the prominent stance of President Mubarak in the Palestinian issue."

Digitally altered images in the world of cosmetics, celebrities, and public health

While governments may alter photos for political reasons, businesses do so to make their products look better. For instance, cosmetic companies routinely alter their advertisements. In a July 2011 Lancôme advertisement for Teint Miracle foundation



DOES SHE
REALLY LOOK
LIKE THIS?

featuring actress Julia Roberts, editors had digitally erased all of her wrinkles and age lines, leaving a flawless complexion. In a December 2011 mascara advertisement, CoverGirl editors had digitally lengthened the eyelashes of country singer Taylor Swift to claim that its product had more volume than competing ones.

Along with the cosmetics industry, magazine editors alter the images of people featured in their publications. For its July 2007 cover of country singer Faith Hill, editors at *Redbook* magazine had digitally erased her age lines and also slenderized her arms and back. For *SELF* magazine's September 2009 cover, editors had digitally shrunk the waist and torso of singer Kelly Clarkson by nearly one half. After editors at *Men's Fitness* magazine had digitally enhanced

not realize that the company had digitally removed split ends and stray strands. Others may believe that they will resemble a model in a print advertisement for exercise equipment without knowing that an advertising agency had digitally inserted muscles onto the model's original image.

Maintaining an unbiased media: Others argue that the media have a duty to publish honest, unbiased, and unaltered information, and that digital editing unfairly imposes a publication's views of various subject matters (or even its political or social agenda) onto its unwitting readers.

Preventing shifts in standards of beauty: Many say that digital editing can negatively shift accepted standards of appearance and

While most people alter photos and other images to correct imperfections, governments have long altered them for political reasons. And businesses routinely do so to make their products (and even the celebrities endorsing them) look better.

the bicep muscles of tennis star Andy Roddick for its May 2007 cover, Roddick said in an interview: "Little did I know I have 22-inch guns and a disappearing birth mark on my right arm . . ."

Even editors for parenting magazines and toddler apparel catalogs are digitally removing blemishes, drool, and fat creases from baby pictures to present more attractive images for their covers and advertisements, reported the *Telegraph*, a British newspaper.

Organizations may also digitally alter images for public health reasons. For example, the New York City Department of Health – in an effort to raise awareness of diabetes and its health risks, including the need for amputation – hired an agency to create an advertisement warning people not to drink supersize sodas. Using an image of an overweight actor, the agency digitally removed his right leg below the knee.

In a health awareness campaign against cigarette use, the U.S. Food and Drug Administration implemented a regulation (which was withdrawn in March 2013) requiring tobacco companies to place explicit images of the effects of tobacco use – such as smoke-ridden lungs, a mouth with decayed and missing teeth, a gaping hole in a smoker's throat, and an ex-smoker lying on an autopsy room table – on all cigarette packaging. According to a decision issued by Judge Richard Leon of the U.S. District Court for the District of Columbia in a case where several cigarette companies had challenged the regulation: "Some, if not all, of these images are digitally altered to evoke emotion and endorse the government's 'obvious anti-smoking agenda.'"

Reasons to regulate the digital alteration of images

As more and more people, companies, and governments digitally alter photographs and other images, critics argue that nations should restrict or set minimum standards to regulate this ubiquitous practice. What reasons do they give?

Stopping deceptive advertising: Digital alteration can be a form of deceptive advertising which not only undermines consumer trust in companies and their products, but also violates consumer protection laws, say some critics. For example, people may believe that their hair will look as shiny and voluminous as the model's hair appearing in a shampoo print advertisement, but do

beauty in a society. According to Michael Schiffer, an attorney at the law firm Frankfurt Kurnit Klein & Selz, PC, advertisements which feature digitally altered models are "selling an unattainable beauty rather than the product [itself]," and that young viewers – who don't yet have the ability to perceive such changes – will accept these images as reality.

Curbing eating disorders: Many analysts believe that a connection exists between the rise of eating disorders and the increasing use of digitally altered models in print and online materials. People with anorexia nervosa (abbreviated as "anorexia" or "ana"), for example, have an extreme fear of gaining weight. According to one eating disorder study, adolescent girls in the United States are more afraid of gaining weight than getting cancer, the threat of nuclear war, or losing their parents.

To stay thin, anorexics reduce their caloric intake from anywhere between zero to 600 calories per day, which can then lead to low blood pressure, kidney failure, chronic depression, a weakened immune system, and heart damage, says the U.S. Department of Health and Human Services (or HHS). The suicide risk of

IS SHE
FOR REAL?



anorexic women, reports the World Health Organization, is 20 times greater than those women who are not anorexic. According to the South Carolina Department of Mental Health, anorexia has the highest death rate of any mental illness. It added that only about 30 to 40 percent of anorectic individuals ever make a full recovery.

While experts classify anorexia as a mental disorder, some with that condition disagree and have used social media outlets on the Internet to help support what they call an “anorectic lifestyle.” These so-called “pro-ana” websites offer extreme dieting tips, advice on how to hide weight loss, and a sense of community to anorectic men and women. “Anorexia is a lifestyle, not a disease,” according to *The Pro Ana Lifestyle* blog.

In contrast to anorexia, people with an eating disorder called bulimia nervosa (abbreviated as “bulimia” or “mia”) consume large quantities of food in one sitting and then purge everything by vomiting. They may also exercise for extensive periods of time to avoid gaining weight, says HHS. Bulimia, which affects both men and women, can lead to chronic depression, heart failure, osteoporosis, substance abuse, tooth decay from the extra acid that remains in the mouth after bouts of vomiting, and even death, reports the Office of Women’s Health at HHS.

What leads to the development of these various eating disorders? Experts have cited periods of stress and traumatic experiences, among other factors. But some studies suggest that the constant viewing of digitally altered images plays a strong role in the development of eating disorders. How? People may feel pressure to resemble the digitally altered slender models featured prominently in print advertisements who look unrealistically beautiful, happy, healthy, and successful.

In a study conducted by Harvard Medical School and Brigham and Women’s Hospital, nearly 70 percent of girls reported that viewing magazine photos had a significant impact on what they considered to be the ideal weight. The study also revealed a “positive linear association” between dieting to shed pounds and reading

fashion magazine articles and advertisements. (That is to say, as a person reads more fashion magazines, it becomes more likely she will go on a diet.)

The London School of Economics and Political Science in November 2011 presented what it called the first-ever economic analysis of eating disorders where it said that viewing digitally altered advertisements did not directly cause eating disorders but likely played a significant factor in their development.

In a 2010 article published in a British tabloid called the *Daily Mail*, a former editor for *Cosmopolitan* magazine, Leah Hardy, wrote that many magazines (including *Healthy*, *SELF*, and *Vogue*, and even her own publication) engage in a common practice called “reverse retouching” where editors digitally insert “luscious curves” and “gleaming skin” to enhance the appearance of models who, in real life, are actually “frighteningly thin.” Doing so, said Hardy, implies that emaciated people are actually healthy when the opposite is true. “[It’s] no wonder women yearn to be super-thin when they never see how ugly thin can be,” she said.

In response to these various developments, the Royal College of Psychiatrists in 2010 said that the media industry must stop using underweight models and also stop airbrushing their advertisements because it potentially “glamorizes” eating disorders such as anorexia and bulimia.

But how prevalent are eating disorders throughout the world? Statistics from various nations and regions of the world include the following:

Africa: Over half of female students expressed dissatisfaction with their bodies, according to a 2002 University of Zululand study. It also said that more women in rural areas in Africa are abusing laxatives and appetite suppressants in an effort to maintain a skinny, sometimes borderline skeletal frame. The study attributed these developments to a desire by women to replicate the thin, Westernized ideal of female beauty, even though African cultures traditionally value full-figured women. Overall, bulimia is more common than anorexia among African women with eating disorders, said researchers.

Asia: Since the turn of the century, India has reported rising cases of anorexia among women, even in neighborhoods where some families do not have enough to eat each day, reported *BBC News*. Some have blamed the growing prevalence of Western apparel advertisements and films which regularly show thin models and actors.

In cities such as Hong Kong, Singapore, Seoul, and Tokyo, *USA Today* reported that more women are being hospitalized for eating disorders. They attempt to lose weight through self-starvation regimens, liquid diets, chemical weight loss treatments at clinics, and by taking diet pills which are banned in other countries. Critics have told publications such as the *Los Angeles Times* that the influx of Western advertising (which depicts slim women as more beautiful and successful) has caused the rise of eating disorders. Bulimia is very common in Japan, especially in cities where 24-hour convenience stores let people engage in binge eating, reported the *Shanghai Star*.

South America: Since the 1990s, the media have reported that many women in South America have “fashion model syndrome” where they undergo plastic surgery and also develop anorexia and bulimia in order to look like the thin yet curvaceous models featured in magazines. A British daily, the *Independent*, noted



that those in the public eye – such as athletes, daytime soap opera stars, politicians, and Miss Universe hopefuls (particularly those from Argentina and Brazil) – regularly undergo plastic surgery and dramatically lose weight and that doing so may encourage the general public to follow their lead. It also reported that the Hospital for Anorexia and Bulimia located in the Argentine capital of Buenos Aires receives an average of 10 new patients every day. Argentina has the highest per capita rate of anorexia in the world, exceeding those found in Europe, Japan, and the United States, according to statistics.

University of California, Los Angeles, exposure to Western media did not lead to substantial differences in the prevalence of eating disorders in a sample of female Iranian students living in Tehran and female Iranian students living in Los Angeles. In fact, the students in Tehran suffered from eating disorders at the same rate as those living in Los Angeles.

Critics also question whether requiring warning labels and disclaimers on digitally altered images will curb the development of eating disorders. Just as warning labels on cigarettes did not lead to the complete cessation of smoking, disclaimers on digitally altered

Why regulate the digital altering of images? The increasing use of digitally altered models in advertisements has led to a rise of eating disorders throughout the world, say supporters of regulation. Opponents say otherwise.

United Kingdom: Approximately 1.6 million people in the UK have eating disorders, says the Priory Hospital Group, the largest independent provider of mental health education and services in that nation. In addition, the UK has the highest rate of eating disorders among all European countries, said a private support group called Anorexia and Bulimia Care. In 2006, Great Ormond Street (a children's hospital in London) saw an increase in the number of young patients admitted for treatment of eating disorders, with some as young as seven. One physician, Dr. Jon Goldin, said in an interview with *BBC News* that cultural expectations and the presence of rail-thin runway models may be a “contributory factor” in the development of eating disorders in these younger patients.

United States: Some groups say that approximately eight million people in the United States have an eating disorder and that most of them (85 percent) are women. But these statistics may not be accurate because many people with eating disorders do not report them or seek treatment, points out the National Association of Anorexia Nervosa and Associated Disorders. According to that group's own estimates, around 24 million adolescents and adults could have an eating disorder, nearly three times the documented rate.

Given these statistics and developments, many eating disorder experts, psychologists, physicians, and even models have argued that nations should pass laws to regulate or restrict the practice of digitally altering images. Some say that governments should require companies to print, for example, warning labels on such images or even prohibit the practice altogether. If nations can require warning labels and disclaimers on cigarettes, foods, and medicines, why not require them on digitally altered ads, they ask. The 2011 study by the London School of Economics concluded that having the government enforce certain policy measures concerning digital editing or even intervene in the fashion and advertising industries could help to promote healthier images for youth and also curb the development of eating disorders in Europe.

Reasons to oppose efforts in regulating the digital alteration of photos

Many people point out that no study has ever conclusively shown that the frequent use of digital editing has directly or indirectly led to an increase in eating disorders. So, they say, nations don't have a strong basis to regulate that practice. According to the results of a study released in 2001 by the Department of Psychology at the

images will not likely lead to any marked decrease in the number of men and women who diet to match the physiques of skinny celebrities and models, they say. (Still, others point out that ever since the United States had required tobacco companies to print warning labels on cigarette packages, the number of smokers has decreased significantly in recent decades.)

Some argue that if the government regulates the practice of digitally altering images, fashion magazines will not suddenly begin to feature plus-sized models in their advertisements. They will continue to hire tall, slim, and toned models. In response, analysts such as Elizabeth Perle, an editor at the *Huffington Post*, say that models who are not slim may then resort to anorectic measures because they know that a certain magazine will only hire slim people.

So how should society address the development of eating disorders? Several child psychologists believe that parents should tell their children to focus on good health and nutrition instead of physical appearances. This approach, they believe, will do more to prevent the development of eating disorders than regulating the practice of digital alteration.

Other critics have broader concerns over efforts to stop the development of eating disorders by regulating the digital alteration of images. For instance, once a government starts to do so, will it then regulate photo alterations for other unrelated purposes? Where would it stop, they ask?

Even though some people may oppose efforts to regulate the digital alteration of photos, many nations have already taken certain measures which, to some extent, address this practice.

United Kingdom: Regulating digital alteration through self-regulation

The United Kingdom does not have a law or an agency whose sole and primary purpose is to regulate the practice of digitally altering photos in advertisements and other images. Instead, the government largely allows the advertising industry to regulate its own activities and practices.

Currently, a self-regulatory body called the Committee of Advertising Practice (or CAP) – whose members include groups which represent advertisers, marketers, and media businesses – had created and now regularly updates a body of published rules for non-broadcast advertisements. Known as the *UK Code of Non-*

broadcast Advertising, Sales Promotion, and Direct Marketing (or the *CAP Code – Edition 12*, for short), these rules are designed to “ensure that advertising does not mislead, harm, or offend,” and they apply to advertisements appearing in magazines, newspapers, the Internet, mail, and even text messages. (Up until 2010, the UK had used *CAP Code – Edition 11*. While the numerical order of the

accurate.” Companies must also present evidence backing the claims which they make for their products, and they may not use “unfamiliar scientific words for common conditions,” among many other rules.

- Other sections set rules on advertisements for weight control products, food supplements, lotteries, alcohol, and tobacco.

While the UK does not have explicit rules or standards which specifically regulate the digital altering of images, it has used existing consumer protection laws and a self-regulatory system to withdraw advertisements featuring altered images of celebrities which can mislead consumers.

rules in Edition 11 and Edition 12 do not correspond to each other, the rules themselves broadly share the same text.)

The rules in the current *CAP Code* set out broad principles which the advertising industry must follow when they create and publicize their advertisements. They include the following:

- The rules under *Section 01* say that marketing communications should be decent, honest, and truthful. Rule 1.3, for instance, says that “marketing communications must be prepared with a sense of responsibility to consumers and to society.”
- *Section 03* sets out general rules to prevent misleading advertising. For example, Rule 3.1 says that “marketing communications must not materially mislead or be likely to do so.” Rule 3.11 says that “marketing communications must not mislead consumers by exaggerating the capability or performance of a product.”
- *Section 04* establishes rules to “ensure that ads do not cause harm or serious or widespread offence.”
- *Section 05* sets rules which advertisers must follow if they direct ads at children or create ads that feature them.

Along with these broad principles, the *CAP Code* sets rules for specific types of advertisements. For instance:

- Advertisers must follow certain rules under *Section 11* when they claim that their products are environmentally friendly.
- *Section 12* sets rules for advertisements which specifically market medicines, medical devices, and beauty products. Under Rule 12.15: “Illustrations of the effect or action of a product should be

To be sure, the UK certainly has existing laws (over 200, in fact) which protect consumers from false advertising and also establish formal rules for marketing communications, say analysts. Where does the *CAP Code* fit into this legal framework? According to one group: “The [*CAP*] Code supplements the law, fills gaps where the law does not reach, and often provides an easier way of resolving disputes than by civil litigation or criminal prosecution.” (The United States has a similar approach which this article describes in a later section.)

While the *CAP* updates the *CAP Code*, who enforces its rules? An independent regulatory body called the Advertising Standards Authority (or ASA) – which describes itself as a “limited company” connected neither to the government nor to the advertising industry – administers the *CAP Code* and verifies that advertisements comply with its rules. How? It reviews approximately 26,000 complaints filed each year by consumers against various advertisements which they believe had violated certain provisions of the *CAP Code*.

When it receives a complaint, a body called the ASA Council – a 13-member committee of industry representatives, management executives, and lay members – carries out an inquiry. It then publishes its decision, which includes a discussion of the issues, responses from the company in the inquiry, and the ASA Council’s assessment of the complaint. The decision may allow a company to continue running its advertisement or call on it to amend certain problems. In some cases, the ASA Council may ban an advertisement from UK publications. In 2011, the ASA opened 22,397 cases, and called on advertisers to change or withdraw 4,591 ads.

While adherence to the *CAP Code* is not legally binding, the ASA says that “the vast majority of advertisers comply with the ASA’s rulings.” Those who don’t could face sanctions. For example, the ASA can ask its other members to withhold advertising space for the non-compliant advertiser or even pre-vet its marketing materials before publication, among other measures.

Recent cases under the *CAP Code*: Does the *CAP Code* have explicit rules which specifically and directly address the digital altering of photos and other images? At this time, it does not. But an advertiser may violate existing rules in the *CAP Code* if it digitally alters a photo in a certain manner. In fact, many people had, in recent years, filed complaints against several cosmetics companies for creating ads which they say had misled them about the claims of their products through the use of digital editing.

An eye cream for Twiggy: In July 2009, Procter & Gamble (or P&G) began a print ad campaign for an eye cream called Oil of Olay Definity eye illuminator which showed a 62-year-old British actress



and former model, Leslie “Twiggy” Lawson, wearing the eye cream, but whose face was completely wrinkle- and blemish-free. “Reduces the look of wrinkles and dark circles for brighter, younger-looking eyes,” claimed the ad.

Through a website campaign, over 700 people filed complaints with the ASA, arguing that the Procter & Gamble ad was misleading because, in their opinion, it implied that “Twiggy’s appearance in the ad was achieved solely through the use of Olay Definity.” Instead, they believed that the company had digitally altered the photo. Others believed that the ad was “socially irresponsible” because the use of post-production techniques such as digital altering could have a “negative impact on people’s perceptions of their own body image.”

In response, P&G reviewed its post-production techniques for the ad, and concluded that “there had been some minor retouching around Twiggy’s eyes which was inconsistent with their own policies.” The company then voluntarily replaced Twiggy’s image with a photo which didn’t have any “post-production work in the eye area.” P&G also responded that its ad was not socially irresponsible. By placing the ad in magazines for older women, it was unlikely to have a negative impact on people’s perception of their own body image, said the company.

In its decision (number 105108) released in December 2009, the ASA concluded that the ad was “likely to mislead” because while it seemed to promise the public that using the eye cream itself would reduce wrinkles and dark circles, it did indeed feature a retouched photo of Twiggy. Therefore, the ad breached what was then *CAP Code* 7.1, which said that “no marketing communication should mislead... by inaccuracy, ambiguity, exaggeration, omission, or otherwise.”

The ASA also concluded that the ad was not socially irresponsible, agreeing with Procter & Gamble that it was unlikely to have a negative impact on the body perception of its viewers because those viewers were of “an older age group.” Therefore, the ad did not breach what was then *CAP Code* 2.2, which said that “all marketing communications should be prepared with a sense of responsibility to consumers and to society.” Because P&G had already withdrawn the post-production ad on its own, the ASA said that “no further action [was] required.”

A foundation for Julia Roberts: In 2011, a member of Parliament, Jo Swinson, filed a complaint with the ASA Council against a print advertisement by L’Oréal (UK) Ltd. (operating as Lancôme) for its Teint Miracle foundation featuring then 42-year-old actress Julia Roberts. Her flawless facial image, according to the ad, was the direct result of applying the foundation to her face. “Aura is natural light emanating from beautiful skin,” it said. “We can reproduce this. 10 years of research, 7 patents pending: Lancôme invents its 1st foundation that recreates the aura of perfect skin.”

But in Swinson’s opinion, the advertisement was misleading because Robert’s photo was “not representative of the results the [product] could achieve.” She also claimed that the “flawless skin in the image was the result of digital manipulation, not the product.” Therefore, the ad violated the *CAP Code*, which prohibits misleading advertising.

In response, Lancôme said that the ASA must consider the fact that its advertisement was trying to sell foundation, “a product which was designed to cover skin flaws and imperfections.” It added that the flawless skin in its advertisement was also due to Roberts’ “naturally

healthy and glowing skin.” Furthermore, the company said that the photographer for the ad had used “a lot of light” which helps to reduce the appearance of skin imperfections. Moreover, after researching and testing Teint Miracle foundation for 10 years, Lancôme claimed that its foundation can “reinforce the skin’s radiance.”

In its July 2011 decision (A11-149640), the ASA concluded that the ad was misleading because it violated *CAP Code* 3.1 (Misleading advertising) and 3.11 (Exaggeration).

While Lancôme provided some details on the enhancements it had added using post-production techniques for the ad, the ASA noted that “we had not been provided with information that allowed us to see what effect those enhancements had on the final image.” In fact, the *Guardian* reported that “the ASA was not allowed to see the pre-production pictures of Roberts due to contractual agreements with the actor.” As a result, the ASA said, “on the basis of the evidence we had received, we could not conclude that the ad image accurately illustrated what effect the product could achieve and that the image had not been exaggerated by digital post-production techniques.” What final action did the ASA take? “The ad must not appear in its current form again,” it ruled.

Anti-wrinkle cream for Rachel Weisz: The member of Parliament, Jo Swinson, who in 2011 had filed the complaint against L’Oreal (UK) Ltd.’s advertisement for Teint Miracle foundation filed another one (in the same year) against that company’s advertisement for RevitaLift Repair 10 (an anti-wrinkle cream) featuring then 41-year-old actress Rachel Weisz with flawless and wrinkle-free skin. Among other claims, the company said that using its facial cream would make a person’s skin look smoother and her complexion more even.

In her complaint, Swinson argued that the advertisement was misleading because she believed that L’Oreal had “digitally manipulated” the original photo of Weisz, and that doing so had exaggerated the effects of the product itself.

In response, L’Oreal said that professional make-up artists had styled Weisz’s face, and that the photographer had used “a lot of light” to make Weisz appear more flattering – all done in the pre-production phase. But it noted that the ASA had previously ruled that “cosmetics ads could present their product in the best possible light.” The company also gave its images taken during the photo shoot to the ASA to show “what level of post-production had taken place” to them.

ALTERED HAIR?



In its February 2012 decision (A11-171059), the ASA concluded that the advertising image was misleading and had exaggerated the claims of the anti-wrinkle cream, thus violating the CAP Code's prohibition (Rules 3.1 and 3.11) against misleading advertising and exaggeration. Specifically, it said that the "image had been altered in a way that substantially changed [Weisz's] complexion to make it appear smoother and more even. The ASA told L'Oreal that "the ad must not appear again in its current form."

Too drop-dead skinny? While the previous ASA decisions called on companies to revoke certain advertisements because they had digitally edited their images in a way which could mislead consumers, the ASA did release a decision where it concluded that an advertisement was socially irresponsible not because a company had used digital alterations, but because it had featured a model who was actually underweight.

In 2011, a member of the public had filed a complaint against an Internet advertisement which featured apparel from Drop Dead Clothing, Ltd. The advertisement, claimed the complaint, was socially irresponsible because the model was "underweight and looked anorexic." It also noted that the model had dark, sunken eyes. In response, the company gave photos of the model to the ASA which it said showed that she was "not emaciated" and was "perfectly healthy." While the model in the advertisement did not have any fat around her ribs, the company said that she had a bust, hips, and healthy skin. It also said that the make-up on the model's face may have given her the appearance of dark, sunken eyes.

In its decision (A11-164206) released in November 2011, the ASA said that the advertisement violated Rule 1.3 on social responsibility because it had used a model who looked underweight. For example, it noted that the model's "hip, rib, and collar bones were highly visible," that the "hollows in her thighs were noticeable," and that the model had "prominent thigh bones." Because the company was marketing its products to young people, using the underweight model was "likely to impress upon that audience that the images were representative of the people who might wear Drop Dead's clothing, and as being something to aspire to." The ASA said that the advertisement "must not appear again in its current form."

What is being done today? In response to the increasing use of digital alteration in commercial advertisements, several members of Parliament in August 2009 said that the ASA should regulate that practice, according to reporting from the *Independent*, a news daily.

Specifically, they called on the ASA to adopt new rules for the CAP Code which would completely ban the digital alteration and enhancements of advertisements aimed specifically at people under the age of 16. For advertisements aimed at adults, the ASA should adopt rules requiring a company to include a disclaimer which reveals the extent to which it had altered its images, they said. But a spokesperson for the ASA told the *Independent* that such rules would be difficult to pass and enforce because "all ads are altered or enhanced, whether it's food that has steam added at a later date to lighting techniques to airbrushing." The ASA never passed these proposed rules. Even today, no law in the UK sets specific standards for the digital alteration of advertisements.

While the ASA did not amend the CAP Code to address the specific use of digital alterations in print advertising, it did publish in April 2011 what it calls a *Help Note* named "Use of production techniques in cosmetic advertising." According to the ASA, a *Help Note* gives "detailed guidance on specific sectors or subjects that

are covered only generally in the Code." While the *Help Note* is "intended to help advertisers, agencies, and media owners interpret the Code," says the ASA, "it is not a substitute for those Codes." It adds that the *Help Note* "neither constitutes new rules nor binds the ASA."

The April 2011 *Help Note* gives general guidance on how companies can avoid misleading the public about the claims of their products when they use pre- and post-production techniques in their advertisements. In the specific area of digital alterations, it said that re-touching "any characteristics directly relevant to the apparent performance of the product being advertised" would likely mislead the public and could violate the CAP Code. For example, the *Help Note* cautions against removing wrinkles around the eyes for an eye cream advertisement or adding shine to hair for a product which claims to produce shiny hair. On the other hand, the *Help Note* said that a company can make "minor adjustments [to its advertisement] to correct for lighting problems," and that it could also remove skin blemishes as long as doing so "does not affect the impression given of the effectiveness of the product."

In a more roundabout way to address eating disorders, the British Fashion Council (a non-profit trade group promoting the British fashion industry) in 2007 accepted several voluntary recommendations from an independent government report examining the health of models. One recommendation said that the fashion industry should not allow girls under the age of 16 to appear in photo shoots and on catwalks during fashion shows. (Why? To prevent them from losing weight to compete with more experienced models.) The Council also said that models may appear in fashion shows only if a medical certificate says that they are not suffering from an eating disorder.

Addressing digital alteration in other nations

Along with the United Kingdom, several nations have made some efforts in recent years to address the digital alteration of images in advertisements, though they have been largely unsuccessful. Others have avoided the issue and, instead, are implementing indirect measures to address eating disorders. They include the following countries described below.

France: While France has consumer protection laws which prohibit advertisements from misleading or deceiving consumers, no law in France directly regulates or sets standards for the digital altering of images.

Echoing criticisms in other nations, many people in France believe that the prevalence of very thin models in print and Internet advertisements along with the practice of digitally altering their appearances have led to eating disorders. According to Valérie Boyer, a member of the French parliament, "being confronted with unrealistic standards of female beauty could lead to . . . eating disorders," reported *Reuters*. Approximately 30,000 to 40,000 people in France suffer from anorexia, said the French Ministry of Social Affairs and Health.

In response, Boyer in 2009 proposed a law which would have required all digitally altered advertisements to include a disclaimer saying: "Photograph retouched to modify the physical appearance of a person." In a statement to the media, Boyer said that requiring such a disclaimer was not "just a question of public health, but also a way of protecting the consumer. The government would have punished violators with a fine of €37,500 (or approximately US\$50,000) or

up to 50 percent of the advertisement's cost of production, reported *Reuters*. While the proposed law had garnered the support of 50 other politicians, the French parliament did not adopt it.

Has France taken other measures to address what it says is a growing problem with eating disorders? In April 2008, the nation's health ministry signed a charter (i.e., an agreement) with fashion houses and advertising agencies which call on them to follow a series of *voluntary* guidelines to promote "healthy body images" and to combat anorexia, according to various media reports. Parties to the agreement (officially called the *Charter on voluntary engagement over the body image and against anorexia*) should, for instance, promote "a diversity of body representations" and avoid using "images of people, in particular youth, that could contribute to promoting a model of extreme thinness." Because the provisions of the charter are voluntary, some analysts have questioned its

In March 2012, Israel became the first country in the world to pass legislation requiring an advertisement to include a notice if it shows a model who had been digitally altered to look thinner. The law also prohibits underweight models from appearing in advertisements.

effectiveness. They also note that the agreement does not explicitly address the digital alteration of images.

In 2009, France proposed a law which would prohibit people from creating or promoting websites or publications which encourage eating disorders such as anorexia and bulimia. According to an excerpt from the law reported by the *Associated Press*, those found guilty of "inciting others to deprive themselves of food" to an "excessive" degree could face punishment of up to two years in jail and fines up to €30,000. France's parliament did not yet pass the law. Opponents of the bill say that the bill raises serious issues concerning freedom of speech and is also a misguided attempt to micromanage people's lives. They also believe that the law would be difficult to enforce, especially if a particular website was created outside of France.

In an indirect approach to address eating disorders, France, during the 1980s, adopted guidelines which require medical exams for models under the age of 16 to make sure they are not suffering from an eating disorder, reported the *Associated Press*.

Norway: In November 2011, in an effort to curb eating disorders, the then-Minister of Children and Equality, Audun Lysbakken, proposed a law which would require a warning label on advertisements showing digitally altered images of thin models, reported the *Washington Post*. One suggestion states: "This advertisement has been altered and presents an inaccurate image of how this model really looks."

Arguing that digitally altered images of thin models promoted "unobtainable ideal bodies," Lysbakken said in a press conference reported by *The Local*, an English daily in Norway, that his law would "reduce the pressure" felt by young people to become as slim as the altered models shown in advertisements. But many had doubts about whether the warning will curb eating disorders. Said one critic: "We have also introduced rules against hidden advertisements by putting text into ads that say this is an ad. I don't know if this has had an effect on the impression the ad gives." As of 2013, Norway has not enacted the law.

Australia: In 2011, the government implemented a single, national consumer protection law (called the *Australian Consumer Law*) which prohibit businesses from making false or misleading claims when selling their products or services, among other restrictions. But that nation currently does not have any legislation which directly regulates or sets standards for the practice of digitally altering images.

Instead, the government introduced in 2009 a *Voluntary Industry Code of Conduct on Body Image* which calls on the advertising, fashion, and media industries to follow several voluntary principles to promote healthy body images.

For example, when using technology to digitally alter images of people, these industries (under the code) should "refrain from enhancing images in a way that changes a person's body shape . . . by lengthening a person's legs, tightening their waist, or changing his or her body shape." It also encourages them to refrain from

"removing moles, freckles, and other permanent distinguishing marks." Furthermore, the code says that these industries should "disclose images that have been retouched."

The code also encourages them to show "a wide range of body shapes, sizes, and ethnicities" in their advertisements, use models who are "a healthy weight and shape," stock clothing in a "wide variety of sizes," and use people 16 and older "to work or model in adult catwalk shows."

Polls in Australia showed that over half of young people expressed concerns that the advertising, fashion, and media industries were promoting unattainable body images – where women have thin yet healthy bodies and where men are perfectly chiseled – and that they felt social pressure to aspire to these so-called ideals. But as more young people fail to reach these ideals, they may become dissatisfied with their figures, and then engage in "dangerous eating behaviors [such as binge-eating, purging, and skipping meals] in an effort to achieve the 'thin-ideal' presented in media," said Amanda Dearden of Isis, a non-profit based in Brisbane, Australia, which helps people with eating disorders.

Are various industries in Australia following the code? While no one has carried out a comprehensive study, Isis said that one study had tracked 10 magazines and found that three had followed all of the principles in the code. In an interview with the *West Australian*, a news daily, a women's advocate described the code as "meaningless," adding that it is "voluntary, has no teeth, there are no penalties and there appears to be no meaningful progress at all, aside from the occasional token gestures like a special edition of a magazine using larger girls."

Spain: Spain does not currently have any law or regulation which explicitly regulates and sets standards for digitally altering images in the media. Instead, it has implemented several voluntary measures to promote healthy-looking bodies.

For example, after protests from medical and women's advocacy groups, the Association of Fashion Designers of Spain reached

a voluntary agreement with the Madrid regional government in September 2006 where the association would prohibit models from appearing in the Madrid Fashion Week if their body mass indices fell below a certain level. (According to the Centers for Disease Control and Prevention, experts use a numerical indicator called a body mass index (known as BMI) – which is calculated by using a person’s weight and height – to determine whether an individual has possible weight problems. Adults with a BMI between 18.5 and 24.9 have a healthy weight. Those with a BMI over 25.0 are overweight. Adults with a BMI under 18.5 are considered underweight.)

CNN described the agreement as “the world’s first ban on overly thin models at a top-level fashion show.” When the association first used the BMI agreement, around 30 percent of models could not participate in Madrid Fashion Week, according to media reports. An official with the Madrid regional government said to *CNN* that the fashion industry had a responsibility to present healthy models because “fashion is a mirror, and many teenagers imitate what they see on the catwalk.”

But opponents said that the agreement could be unfairly discriminatory. “I think it’s outrageous,” said Cathy Gould of the Elite Modeling Agency to *CNN*. “I understand they want to set this tone of healthy, beautiful women, but what about discrimination against the model and what about the freedom of the designer?” In response, the Association in Defense of Attention for Anorexia and Bulimia said that if the fashion industry does not follow the voluntary agreement, then “the next step is to seek legislation” in banning too-thin models from fashion shows in Spain.

In a separate development to address eating disorders, the Ministry of Health, Social Services and Equality announced in 2007 that it had reached a voluntary agreement where major retailers (such as Zara and Mango) would slowly replace unrealistically thin storefront mannequins with those which can wear clothing starting at a size 10. According to the Health Ministry’s director of consumer affairs: “There is a lot of pressure, not just from the fashion world, but society in general, for women to seek models of beauty that are unreal and even unhealthy.”

Along with replacing thin mannequins with larger ones, the health ministry announced that fashion retailers must standardize women’s clothing sizes. That is to say, a size 10 dress made by different manufacturers will be roughly the same size. (According to *BBC News*, “clothes . . . on sale in Spain often vary in size from shop to shop, despite carrying the same size label.”) In order to create realistic sizes for the general population of women, Spain’s National Consumer Institute will take the measurements of 8,000 Spanish females (from the ages of 12 to 70) and give this data to fashion retailers.

Italy: Italy does not have any legislation which directly regulates the digital alteration of images. But the Italian ministries of Health and Sports launched a national anti-eating disorder campaign in 2008 which calls on magazines, the broadcast media, and Internet sites to follow voluntary guidelines in discouraging “ultra-thin beauty ideals,” reported the *Associated Press*. According to the Ministry of Health, two to three million people in Italy have an eating disorder, and men make up approximately 10 percent of that figure. The Association of Pediatric Medicine reported that, in Italy, nearly “65 percent of girls between 10 and 16 want to be thinner than they are.”

In December 2006, representatives from various ministries and the fashion industry publicly signed voluntary guidelines (called the *National Manifesto of Self-Regulation by Italian Fashion Against*

Anorexia) which say that fashion houses should use models who are 16 and older during catwalks and shows. Fashion houses should also ask models to present medical certificates from doctors indicating that they are in good health using various criteria, including their BMI.

But the manifesto does not address the digital alteration of fashion images. It also “does not spell out any sanctions and carries no legal weight,” noted the *Washington Post*, though it reported one industry source saying that “fashion houses who broke the rules would be made to suffer, including by being knocked out of important time slots or dates at fashion events.” These technical punishments, said one expert, “are very important in fashion.”

Brazil: As in the case of many other nations, Brazil does not have a law which directly regulates the digital altering of images, though it does have laws which prohibit false advertising. But after several people in 2006 died from complications arising from eating disorders (including a model whose BMI was approximately 13.4 at the time of her death, according to the *Washington Post*), a member of the National Congress of Brazil, Wladimir Costa, proposed a bill requiring a warning label on digitally altered images to prevent eating disorders. The label would state: “Attention: image retouched to alter the physical appearance of the person portrayed.” According to a 2010 survey, 64 percent of Brazilians wanted to be thinner, including many people who were medically healthy.

While Costa told the *Irish Times* in a 2010 interview that the bill would not prohibit people from digitally altering images, doing so can (in some cases) violate existing false advertising laws. Many magazine advertisements in Brazil “include models as if they have beautiful, sculptural bodies, when, in reality, it is a great lie,” he said, adding, “These are ads with celebrities promoting anti-aging creams, and advertising agencies use Photoshop to remove these celebrities’ own wrinkles from ads. This is criminally false advertising.”

Critics of the bill say that society should not single out the advertising industry for causing eating disorders. “To put this responsibility on advertising and hope that advertising alone can combat these problems is wrong,” said Eduardo Fonseca Martins of the Brazilian Association of Advertising Agencies to the *Irish Times*. Another critic, editor Edson Aran of the Brazilian edition of *Playboy* magazine, said that the proposed law was “too stupid to even bother commenting on.” The National Congress did not adopt the proposed law.

Israel: Several nations (as described in the examples above) have implemented voluntary measures to encourage the advertising and fashion industries to use healthy models in their advertisements. Others have proposed (but did not implement) laws which would require disclaimers on advertisements featuring digitally altered models.

In contrast to these countries, Israel in March 2012 became the first country in the world to pass legislation – the *Law for Restricting Weight in the Modeling Industry* (5772-2012) – requiring an advertisement to include a notice if it shows a model who had been digitally altered to look thinner, according to an analysis carried out by the Global Legal Monitor of the Library of Congress. Although the law does not indicate the exact words which must appear on a disclaimer, the disclaimer must take up at least seven percent of the advertisement’s total space. The law’s provisions apply to advertisements produced in Israel, but not to those appearing in foreign magazines sold in that nation, reported the *Jewish Press*.

The law also prohibits an advertisement from featuring models who do not take a medical exam (at least three months before a photo shoot) where a doctor can confirm that they are not underweight under current BMI standards. (In other words, underweight models can no longer appear in advertisements.) Along with the disclaimer requirement, the mandatory medical exam for models is the first of its kind in the world, say observers.

Supporters of the law said that they wanted to minimize the effects of advertisements showing extremely thin models and also help to curb the growth of eating disorders in Israel. According to a study of 28 nations released in 2000 by Yossi Harel and Michal Molcho of the Bar-Ilan University in Israel, poor body image is more common in Israel than in other Western countries,” said the *Jewish Press*. The study also said that “more than 70 percent of Israeli girls want to change their body (ranking fourth among the 28 countries).” Legislators had proposed the bill after visiting an eating disorder clinic where they saw anorectic patients, including teenagers, adults, and even the elderly, said the media.

Critics have told the *Telegraph*, a British daily, that the law will not be effective because Israel itself only has around 300 professional models, and only a few of them work in other nations. They also point out that Israelis will continue to have unfettered access to fashion advertisements in foreign publications which, again, don’t have to comply with the Israeli law. Others, including Israeli model Adi Neuman, argue that the Israeli law should focus more on a person’s health instead of weight because some models have naturally low BMIs even with healthy eating habits and normal caloric intake. One writer in a health and fitness magazine called *Fruityvore* said that the new law will “make people feel good about themselves but amounts to putting a band-aid on a cut that requires stitches.”

United States: Existing laws, self-regulation, and growing concern over digital alteration

Like other nations, the United States does not have laws or standards whose sole purpose is to regulate the digital alteration of advertisements. Rather, it has a legal and also a self-regulatory system which both indirectly prohibit the digital alteration of images in a way which could deceive consumers. Analysts also debate whether the U.S. Constitution would allow a government to place strict restrictions on digital alterations.

Laws at the federal and state levels: No federal law explicitly regulates the digital alteration of commercial images or sets specific standards for that practice. But existing ones such as the *Federal Trade Commission Act* (or FTCA) – a law overseeing competition and business practices in the United States – could allow the federal government to indirectly regulate the extent to which businesses digitally alter images used in advertisements.

For example, Section 5 of the FTCA prohibits “unfair or deceptive acts or practices” in commerce. According to the Federal Trade Commission (or FTC), the agency which oversees and enforces the FTCA, an act or practice is deceptive when a consumer (acting reasonably under the surrounding circumstances) relies primarily on the deceptive act when making a decision whether to purchase a product or service, and which then leads to consumer harm. Section 12 of the FTCA prohibits the “dissemination of any false advertisement that is likely to induce the purchase of food, drugs, devices, services, or cosmetics.” In combination, these two sections “[establish] the authority for false advertising enforcement

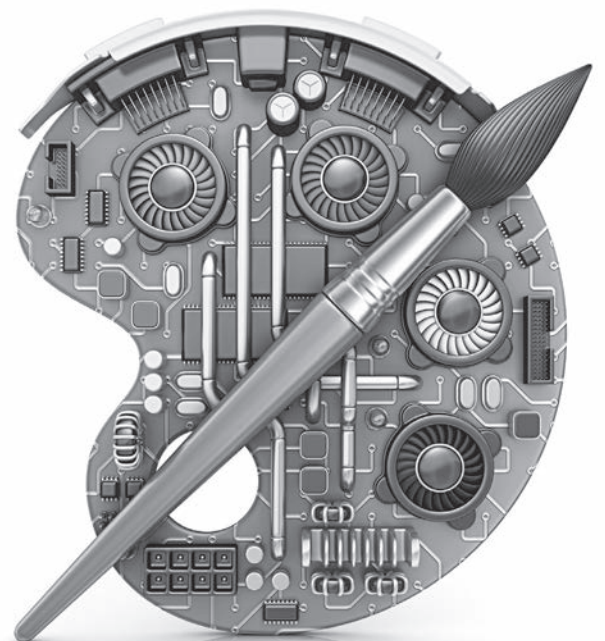
in the FTC,” according to an informational memo prepared by law firm Kilpatrick Townsend & Stockton LLP.

The staff of *The International Review* carried out a search query in the FTC’s online collection of cases and decisions, and it did not find any in which the FTC had accused a business of violating Sections 5 or 12 of the FTCA by digitally altering an image in an advertisement which then led to consumer harm. But such cases are possible. A company could potentially violate Section 5 if it had, for example, digitally altered the image of a model’s abdominal muscles to make them much more well-defined in an advertisement for exercise equipment but then publicly claimed that the model had developed them by solely using its device. Such an alteration could constitute a deceptive practice (under Section 5) and also a false advertisement (under Section 12) if consumers had relied primarily on the digitally altered image when deciding whether to buy the device in the first place and then (as a consequence) suffered some harm.

In another scenario, the FTC said – during a recent interview with Medical Justice, a private group which works to deter what it describes as frivolous medical malpractice lawsuits – that “digital alteration of before-and-after [cosmetic surgery] photographs would be a violation of [Section 5 of] the FTC Act.”

Has the U.S. Congress taken any action to address the digital altering of images found in commercial advertisements? In March 2010, Rep. Tammy Baldwin (D-WI) introduced a proposed law called the *Healthy Media for Youth Act* (H.R. 4925) which called on the Secretary for Health and Human Services to conduct and support research on how the current depiction of girls and women in the media has affected the “psychological, sexual, physical, and interpersonal development of youth.” The proposed bill noted that “sixty percent of teenage girls compare their bodies to fashion models, and almost 90 percent of girls say the media places a lot of pressure on teenage girls to be thin.”

No provision in the proposed bill directly called on the government to regulate the digital alteration of images appearing in advertisements. But it did call for the creation of a “National Task Force on Girls and Women in the Media” to develop “voluntary



steps and goals for promoting healthy and positive depictions of girls and women in the media for the development of all youth.” (The bill did not describe these voluntary steps.) It also said that the government may fund programs which supported “public or private partnerships that encourage businesses, advertisers, the entertainment industry, and other media content providers to promote media content that encourages healthy body images,” but didn’t provide more details.

After H.R. 4925 failed to advance in the legislative process, Rep. Baldwin reintroduced the bill as H.R. 2513 in 2011. But Congress again failed to take up the proposed law. (The U.S. Senate also did not advance its version of the bill in 2011.) No member of Congress had reintroduced the bill in 2012 or 2013.

In a more direct approach to address what many people believe are the harmful health effects of digital alteration, an online magazine called *Off Our Chests* (headquartered in Los Angeles) partnered with the New York-based National Eating Disorders Association (or NEDA) to begin a campaign in January 2012 which called on the U.S. Congress to pass a *Media and Public Health Act*. This proposed federal law – which did not have any Congressional sponsors or even a text – would have required a label “on all ads and editorial content in which the human form [had] been materially altered through computer manipulation or other means.” While these organizations had begun an online petition seeking 10,000 signatures to present to Congress in support of the proposed law, they fell short of their goal, and closed their petition drive in early 2013 with 2,647 signatures.

Along with efforts at the federal level, every state has laws – analysts refer to them as “little FTC acts” – which prohibit deceptive business practices and also the dissemination of false advertising. No state currently has an existing law which explicitly regulates or sets standards for the digital alteration of images appearing in advertisement.

Like other nations, the United States does not have laws or standards whose sole purpose is to regulate the digital alteration of advertisements. Rather, it has a legal and also a self-regulatory system which both indirectly prohibit the digital alteration of images in ways that could deceive consumers.

But in February 2012, Arizona became what some analysts said was the first state to propose a bill regulating digitally altered images. Specifically, Rep. Katie Hobbs of the Arizona House of Representatives introduced House Bill 2793 which stated that “an advertiser shall not use postproduction techniques to alter or enhance printed media advertisements that are distributed or displayed in this state.” (It defined that technique as “the application of image editing techniques to photographs to create an illusion or deception, in contrast to mere enhancement or correction.”) If an advertiser did use postproduction techniques, it would have had to include a disclaimer which states: “Postproduction techniques were made to alter the appearance in this advertisement. When using this product, similar results may not be achieved.” Advertisers which used postproduction techniques but did not include a disclaimer on their ads would have been “[subjected] to enforcement through private action and prosecution by the Attorney General.” The Arizona legislature did not pass the law, and Rep. Hobbs did not reintroduce it in 2013.

Rep. Hobbs, the primary sponsor of the proposed law, told the *Republic*, a news daily in Arizona, that she and her supporters had introduced it – even though it has little chance of passage – because “we need to bring attention to these body-image issues, especially with young girls. Girls need to know that they don’t have to look perfect.” But opponents, including Louie Moses, the creative director of the Moses Anshell advertising agency, told the *Republic*: “I don’t like legislation that tells us what to do and what not to do in marketing. I know what’s right.”

Measures undertaken by private organizations: Along with federal and state initiatives in addressing the digital alteration images in the media, several private organizations have set voluntary standards or have taken a public stance concerning this practice.

National Advertising Division: The advertising industry in the United States adheres to its own self-regulatory system. An independent body called the National Advertising Review Council (or NARC) oversees this self-regulatory system using a voluntary *Code of Advertising* (or Code) which sets basic advertising principles and standards for “advertisers, advertising agencies, and advertising media.” For instance, one principle says that “advertisements which are untrue, misleading, deceptive, fraudulent, . . . shall not be used.” Under another one, “advertisers should be prepared to substantiate any claims or offers,” and that, upon request, “present such substantiation promptly.”

The Code presently does not have any standards which specifically address the digital alteration of images in an advertisement. But a section concerning “Layout and Illustrations” says that the “composition and layout of advertisements should be such as to minimize the possibility of misunderstanding by the reader.”

Within the NARC, a body called the National Advertising Division (or NAD) serves as the “investigative arm charged with monitoring and evaluating truth and accuracy in national

advertising directed towards consumers age 12 and over.” The NAD also reviews complaints filed by individual consumers, consumer groups, and even by businesses themselves against certain advertisements which they believe violate the Code. According to the Better Business Bureau, businesses themselves have filed the most complaints against advertisements made by other businesses. They may, alternatively, file a complaint with the FTC. (Analysts say that the NAD is similar to the Advertising Standards Authority in the United Kingdom, a self-regulatory body overseeing the advertising industry in that nation as described earlier in this article.)

According to an overview of the complaint process written by law firm Arent Fox LLP, when an individual or business files a complaint against a particular advertisement, the challenger and the advertiser submit their arguments and evidence to an NAD proceeding, though the NAD does not have the legal authority “to demand the attendance and testimony of witnesses, answers to interrogatories, and the production of documents.” After reviewing the submissions,

the NAD issues what it calls a “final case decision” where it allows the challenged advertisement to continue, calls for certain changes, or requires its removal from public viewing. Arent Fox points out that “the decisions of the NAD are not legally binding on the parties, but instead are considered recommendations.” In cases where an advertiser refuses to participate in an NAD proceeding or says that it will not comply with a final case decision, the NAD may “refer the matter to the appropriate federal or state enforcement agency.”

Has the NAD ever addressed cases where someone complained that advertisers had used digital alteration in way which violated the Code? In December 2011, the NAD said that it had resolved (for the first time) a case involving a digitally altered advertisement. According to the NAD, consumer goods manufacturer Procter & Gamble (or P&G) had created an advertisement for NatureLuxe Mousse Mascara (featuring country singer Taylor Swift) which said that its product had “2X more volume” and was “20% lighter” compared to other mascaras, among other claims. At the same time, the advertisement included a disclaimer noting that the singer’s eyelashes were “enhanced in post production” (i.e., the company had digitally altered the image in some unspecified manner). Analysts said that the company had used digital technology to make them look darker and more voluminous.

The P&G advertisement implied that consumers using only its NatureLuxe Mousse Mascara would have eyelashes resembling those of Taylor Swift even without the use of postproduction techniques, argued the NAD. “The [advertisement’s] photograph stands as a product demonstration,” said Linda Bean, a spokesperson for the NAD in an interview with *The New York Times*. “Your eyelashes will look like this if you use this product.”

When the NAD contacted P&G, calling on it to substantiate the advertisement’s claims, the company said that it “permanently discontinued all of the challenged claims and the photograph in its advertisement.” Afterwards, the NAD said that “it is well established that product demonstrations in advertisements must be truthful and accurate and cannot be enhanced.” An NAD director, Andrea Levine, told a publication called the *Business Insider*: “You can’t use a photograph to demonstrate how a cosmetic will look after it is applied to a woman’s face and then – in the mice type – have a disclosure that says ‘okay, not really.’”

Council of Fashion Designers of America: In 2007, the Council of Fashion Designers of America (or CFDA) – a non-profit trade association of American fashion designers whose goal is to promote fashion design and maintain a code of ethics and practices for the industry, among other objectives – developed its six-point Health Initiative Guidelines. These voluntary guidelines do not (directly or indirectly) address the digital alteration of photos. Instead, they address what the CFDA calls the “overwhelming concern about whether some models are unhealthily thin, and whether or not to impose restrictions in such cases.”

For example, the guidelines call on designers to “educate the industry to identify the early warning signs in an individual at risk of developing an eating disorder.” They also encourage models who may have an eating disorder to “seek professional help for an eating disorder.” Furthermore, these guidelines call on fashion designers not to hire models under the age of 16 for runway shows, and also not hire models under the age of 18 to “work past midnight at fittings or shoots.” Moreover, under the guidelines, designers should “supply healthy meals, snacks, and water backstage and at shoots.” In contrast to practices in other nations such as Israel, Italy,

and Spain, the CFDA guidelines do not establish minimum BMIs for models. Rather, they “recommend that models receive regular medical care to ensure their well-being.”

These guidelines are not legally binding. According to the CFDA, its health initiative is “about awareness, education, and safety, not policing.”

Girl Scouts of the USA: In 2010, the Girl Scouts of the USA – the organization representing 3.2 million Girl Scouts – published what it calls “depiction suggestions” to promote healthier and positive messages about girls and women. For instance, these guidelines (which are not legally binding) say that the media should “feature and value girls and women with varying body types,” and also “portray realistic, unaltered images of females with natural, physical imperfections,” among many other suggestions. But it does not provide any further details.

American Medical Association (or AMA): Calling itself the “nation’s largest physician group,” the AMA, during its annual meeting in June 2011, called on advertising associations to work with the public and private sectors to “develop guidelines for advertisements, especially those appearing in teen-oriented publications, that would discourage the altering of photographs in a manner that could promote unrealistic expectations of appropriate body image.”

In justifying its stance, the AMA noted in a press release that “a large body of literature links exposure to media-propagated images of unrealistic body image to eating disorders and other child and adolescent health problems.” One member on the AMA Board of Trustees, Dr. Barbara McAneney, told the media that “we must stop exposing impressionable children and teenagers to advertisements portraying models with body types only attainable with the help of photo editing software.”

Observers note that the AMA itself has not developed any of its own guidelines for the digital alteration of advertisements, and that any guidelines would be voluntary and not legally binding.

Can the government restrict the use of digital alteration? In the ongoing debate on whether society or a government should set standards for or even restrict the digital altering of images, analysts ask whether doing so would be legal under the First Amendment of the U.S. Constitution.

The First Amendment restricts the government from regulating speech and other forms of expression, among other provisions. It simply states: “Congress shall make no law . . . abridging the freedom of speech . . .” Although there are many different kinds of speech, the courts have generally divided that term into two broad categories – political and commercial speech.

Despite its wording, the term political speech encompasses more than just speech concerning actual politics. It may include ideas, arguments, opinions, other expressions of thought, and even speech which a person communicates through certain acts – known generally as expressive conduct – such as creating artwork or wearing certain kinds of clothing such as a black armband during a protest. Under the realm of political speech, several U.S. Supreme Court decisions have given all sides of a public debate some room (or “breathing space”) to make factual errors during the course of debate. At the same time, it has placed limits on political speech such as those which prohibit libel and obscenity.

While the courts have given political speech robust protection from undue restrictions, the same cannot be said about commercial speech which the Supreme Court defines as speech which does “no more than propose a commercial transaction.” Some examples

include advertisements, product labels, sales pitches, packaging, and other “profit-motivated communications” promoting a particular product or service.

Although the Supreme Court has ruled that commercial speech deserves protection under the First Amendment, it didn’t confer the same kind of protection afforded to political speech where individuals are given some leeway to make factual errors. In fact, the Supreme Court said that the government may ban commercial speech which is false, deceptive, or misleading, and it may also require certain products to carry disclaimers and warnings such as those found on tobacco products.

Still, just because a government says that its regulation of commercial speech (in a particular case) is legal under the Constitution does not automatically make it so. In a 1980 decision called *Central Hudson Gas & Electric Corp. v. Public Service Comm’n of New York*, the high court created a test to help lower courts determine whether a certain law which restricts commercial speech is legal under the Constitution. As mentioned earlier, the government may pass a law or regulation which prohibits commercial speech which is false, deceptive, or misleading. If the government wants to prohibit a certain instance of commercial speech which is not misleading, it must have “a substantial interest in regulating the speech; the regulation directly advances the government’s interest; and the regulation is not more extensive than is necessary to serve that interest.”

So would a law restricting a business from digitally altering an image in an advertisement violate its First Amendment right to freedom of speech? The answer would depend on the extent to which a law restricts the use of digital alteration, among other factors. As mentioned previously, the government can prohibit an individual or business from creating an advertisement (an example of commercial speech) which deceives or misleads consumers. So if a business, for instance, digitally alters an image of a product in its advertisement for the sole purpose of deceiving or misleading consumers to buy it, then a government can prohibit such an ad without violating that business’ First Amendment right to commercial speech.

On the other hand, if a government passed a law which broadly prohibits a company from digitally altering its advertisement – for a lawful product which is not misleading – for any reason whatsoever (such as artistic ones or simply making adjustments which do not affect whether a person will buy a product), then that blanket restriction may violate a company’s right to commercial speech under the First Amendment by imposing a restriction which doesn’t seem to advance, for instance, any substantial government interest.

But some observers say that a government could forbid companies from making models look thinner in their advertisements if doing so achieves a substantial governmental interest such as protecting the public from developing eating disorders. In response, critics say that it would be very difficult to prove that a law restricting companies from making models look thinner (through digital means) would actually lower the incidence of eating disorders. (So the law would not directly advance the government’s interest to address, in this case, eating disorders as set out in *Central Hudson Gas*.) Even experts say that the development of eating disorders is a complex phenomenon involving a wide variety of factors and that putting much (if not all) of the blame on digitally altered advertisements would not be fair or even accurate.

Do any treaties or global organizations address the digital altering of images?

At this time, no treaty or international body explicitly regulates or sets standards for the digital alteration of images. But the provisions in one existing treaty – the *International Covenant on Economic, Social and Cultural Rights* (or ICESCR) – could possibly set the foundation for such an undertaking, though doing so faces high hurdles.

Adopted by the UN General Assembly in 1966, this treaty calls on its 160 signatory nations to ensure basic economic, social, and cultural rights of individuals within their respective jurisdictions. These rights, among others, include the right to work, free primary education, favorable and safe work conditions, an adequate standard of living, limitation on work hours, and social security. Which provisions in the ICESCR can a nation use to justify its attempt to regulate or set standards specifically for the digital altering of images?

Article 11(2): This article calls on nations to recognize “the fundamental right of everyone to be free from hunger.” One can argue that companies and advertisers who digitally alter their models on commercial advertisements (to make them look much thinner or to make sickly models look much healthier) are causing the development of eating disorders, which leads to hunger. To prevent hunger, a government can, for example, prohibit companies from digitally altering images on their advertisements. It could also require companies to place disclaimers on the advertisements so that viewers will know that the images in the advertisements do not reflect the actual appearance of the model.

But others can respond by saying that a government would first have to show that exposure to digitally altered images causes hunger (through the development of eating disorders) before it can strictly regulate digital alterations. While experts say that viewing such images plays a role in the development of an eating disorder, no one has yet proved that such images are one of the primary causes of that disease. So a government may not have a strong basis under Article 11(2) to regulate or set standards for the digital alteration of images in advertisements.

In addition, others could argue that Article 11 (viewed in its entirety) applies only to situations where a nation’s system in the “production, conservation and distribution of food” leads to an actual shortage of food (which then causes hunger) and that it doesn’t apply to cases where people are deliberately limiting their food intake for, say, fashion reasons.

Article 12(1): This article says that nations must recognize “the right of everyone to the enjoyment of the highest attainable standard of physical and mental health.” To fully achieve this right, a government may – under Article 12(2)(c) – carry out steps necessary for the “the prevention, treatment and control of epidemic, endemic, occupational and other diseases.”

Using Article 12, governments can argue that the digital alteration of images directly causes the development of eating disorders (a disease) which, in turn, prevents people from enjoying the highest attainable standard of physical or mental health. To prevent, treat, and control such a disease, a government could more strictly regulate the digital alteration of images, among other measures. Still, as in the case of using Article 11(2), a government would have to show that exposing people to digitally altered images is one of the main causes in the development of eating disorders, which no one has done yet. 🌐

How do nations and international law address bribery?

Nations all over the world face clear and obvious problems which threaten their security, including economic crises, natural calamities, terrorism, and war, among many others. Some are not as apparent, but can still lead to societal instability and also undermine the rule of law. One such problem is corruption, which occurs when those entrusted with authority use their power for personal gain at the expense of society as a whole.

While the media, in recent years, have increased their reporting of various forms of corruption, they have focused their attention on instances of bribery. What exactly is bribery and how pervasive is this practice? How do various nations around the world deal with bribery? Does international law address this problem, and does it do so effectively? What more can be done to curb bribery?

Corruption and bribery: A “slow-growing cancer on society”

Various forms of corruption have existed worldwide since times of antiquity. For instance, in cases of nepotism, a person of authority gives jobs and other favors specifically to family members, friends, and supporters. An individual may use extortion – where he threatens to use force or other forms of coercion – to get something from another person. Embezzlement occurs when a person illegally takes money or property belonging to others from a fund which he is entrusted to oversee.

Lanny Breuer, the former Assistant Attorney General for the Criminal Division at the U.S. Department of Justice, once described corruption as a “slow-growing cancer on society.” Corruption allows unqualified contractors to perform shoddy and substandard work when constructing a bridge. It could also prevent the most qualified people from filling important positions such as those concerning financial management. Corrupt officials may sell fake passports to unauthorized people, including criminals and terrorists, allowing them to enter nations which have barred their entry. When corruption occurs, “roads are not built, schools lie in ruins, and basic public services go unprovided,” said Breuer in a 2010 speech at the United Nations.

Many believe that corruption is confined mostly to poorer nations, and that these countries must improve their economic development simply to address that problem. But according to a 2004 report from the World Bank, nations such as Botswana, Chile, Costa Rica, and Slovenia have “curtailed corruption to levels comparable with those of many wealthy industrialized countries.” Still, observers say that corruption, while affecting all nations, is still a significant problem in poorer countries. The *2012 Corruption Perceptions Index* – issued by anti-corruption group Transparency International – ranks Afghanistan, North Korea, and Somalia as having the most perceived corrupt public sectors in the world. Denmark, Finland, and New Zealand are ranked as having the least corrupt ones. The United States tied with Japan for 24th place out of 176 nations in the index.

One of the most common forms of corruption is bribery which experts broadly define as the act of giving a gift of value (not necessarily money) to influence or change the behavior and actions of another person. “It is a business transaction albeit an illegal

or unethical one,” says Carl Pancini, a professor of law at Florida Gulf Coast University, and gives “an unfair advantage upon those paying the bribe.” The World Bank estimates that \$1 trillion in bribes exchange hands every year around the world.

In many countries, bribery is so “pervasive in daily life that a whole terminology of euphemisms has evolved,” according to Jeremy Bransten of Radio Free Europe. “If you’re stopped by a police officer in Tajikistan and he tells you his ‘hand is tingling’ or if the phone repairman comes by the house and asks for a ‘cup of tea’ – chances are you’re being solicited for a bribe,” he reported. Examples of bribery from around the world include:

- **China:** In order to keep within their budget, builders paid \$15,700 in bribes to corrupt officials in 1999 to overlook the faulty welding of the newly-built Rainbow Bridge over the Qijang River, according to the *Baltimore Sun*. When the bridge later collapsed due to the faulty welding, 40 people plunged nearly 500 feet to their deaths. In another incident, the former head of the State Food and Drug Administration accepted over \$800,000 in bribes to approve counterfeit medicines such as fake cough syrups containing antifreeze. According to a report compiled by California Polytechnic State University, the cough syrup killed 339 children in Bangladesh, 85 children in Haiti, and 100 children in Panama in 2007.
- **Greece:** A 2010 Transparency International survey revealed that 13.5 percent of households paid an average of €1,355 (or over US\$1,700) in bribes that year. Ordinary citizens hand out cash-filled envelopes to obtain driver’s licenses, get a doctor’s appointment, and reduce their tax bills, said the survey.
- **Indonesia:** Bribery has allowed poachers to smuggle over 200,000 endangered orangutans out of the country. The Orang Utan Republik Foundation says the animals are “sold to crews of foreign-owned ships, and, through a system of corruption,



bribes, and collusion, clear customs easily.” It estimates that for every orangutan that survives the journey out of the country, six to eight are lost.

- **Russia:** In 2011, customs officials posted videos on YouTube rapping about their lavish lifestyles filled with designer clothes, fine wines, and expensive cars which they had acquired by taking bribes. According to British daily *The Telegraph*, customs officials in Russia possess one of the most coveted public sector jobs, most of which can be purchased from the government at the right price. The going rate for a traffic cop’s job, for instance, is roughly \$50,000 while a junior aide to a district prosecutor is around \$10,000. Those who purchase these positions quickly recoup their money by asking for (or demanding) bribes from the public.

As some of these examples show, bribery has real life consequences, said Transparency International. Those involved in corruption may even cover up crimes and damage the environment through illegal activity. And when bribery becomes more endemic in a society, citizens may lose confidence in their governments. To address bribery and its effects, many nations started to pass laws to combat this corrupt practice.

United States: The Foreign Corrupt Practices Act

According to analysts, the United States has one of the strongest legal frameworks which prohibit and criminalize many forms of corruption, ranging from bid-rigging to extortion. Many laws – such as the *General Federal Bribery Statute* found in 18 U.S.C. § 201, among others – prohibit people and companies from bribing domestic public officials and also prohibit these officials themselves from demanding or accepting bribes.

In the 1970s, the Securities and Exchange Commission (or SEC) – which oversees the regulation of the securities industry in the United States – investigated over 400 U.S. companies, including major defense contractors, energy companies, and large retailers, which admitted to paying over \$300 million in bribes, according to the U.S. Department of Justice. They paid these bribes specifically to *foreign* government officials to obtain business in other nations.

In 1977, Congress enacted (and the President signed into law) the *Foreign Corrupt Practices Act* (or FCPA) to put an end to this specific type of bribery. In summarizing the law, the Justice

Department said that “the FCPA makes it unlawful to bribe foreign government officials to obtain or retain business.” Prior to the enactment of the FCPA, no government had made it a crime to bribe a foreign official, said various groups such as the U.S. Chamber of Commerce, a private business lobby. Many had even allowed companies to deduct the payment of bribes from their taxes as a business expense.

Two overarching provisions make up the FCPA: an anti-bribery provision and an accounting provision. The anti-bribery provision prohibits the payment of money or anything of value to a foreign official in order to obtain or retain business. The accounting provision requires corporations to insure that they are not hiding the payment of bribes. How? They must keep financial records which accurately reflect their transactions and payments, and also maintain internal accounting controls which reasonably assure that these transactions are carried out with proper authorization from management.

Both the Justice Department and the SEC enforce the provisions of the FCPA. The Justice Department conducts both civil and criminal investigations of alleged FCPA violations. On the other hand, the SEC handles only civil investigations of alleged FCPA violations carried out by companies (both foreign and domestic) which have registered their securities in the United States. It is common for both agencies to be involved in the same case, said Michael Koehler, an assistant professor at Southern Illinois University School of Law, who is an expert on the FCPA and is also the creator of a blog called *FCPAProfessor.com*.

Proving an FCPA violation: To show that a company or person had violated the FCPA, the government must prove that:

- The FCPA statute applies to specific entities which had bribed or planned to bribe a foreign official. Under the statute, these entities include: (a) U.S. citizens, (b) foreign nationals and residents in the United States, (c) a corporation (both domestic and foreign) which has issued securities registered in the United States, and (d) any association, business trust, corporation, or partnerships, among other entities, which has the United States as its principle place of business.
- The entity had paid money or “anything of value,” a term which the FCPA statute does not specifically define, though the government has interpreted this term broadly. For example, in past convictions of FCPA violations, “anything of value” has included charitable contributions, promises of employment, directed business, cars, and unreasonable travel expenses. But the FCPA does not apply to: (a) what are called “facilitating payments” made to foreign officials for routine government action such as processing fees for visas and other paperwork, (b) payments which are lawful in the official’s country, or (c) payments for a “reasonable and bona fide expenditure” such as reasonable meal expenses as long as they are not made for corrupt purposes.
- The entity had made a bribe with the *intent* of causing the recipient to “misuse his official position to direct business wrongfully to the payer or any other person.” Even when a bribe fails to induce a recipient to misuse his official position, the Justice Department says that “the offer or promise of a corrupt payment can [still] constitute a violation of the [FCPA] statute.”
- The recipient of the bribe was a “foreign official, a foreign political party or party official, or a candidate for foreign political office.” The FCPA statute defines “foreign official” as “any



officer or employee of a foreign government or any department, agency, or instrumentality thereof, or of a public international organization.” But it does not provide more specific examples of these terms.

- The entity had made a bribe to a foreign official with the specific objective of “obtaining or retaining” business. This includes not only bribing a foreign official to obtain or retain business with a government itself, but also bribing foreign officials to retain or obtain business with private sector companies, says the Justice Department.

Situations where the government can hold entities responsible for violating the FCPA: The U.S. government can hold these specific entities responsible for violating the FCPA in many broad situations. For example, it can do so when they carry out an act of bribery either within or even entirely outside of the United States. In addition, a company may be held liable if employees and agents located outside of the United States carry out acts of bribery.

Furthermore, the U.S. government can hold a U.S. parent corporation responsible when its foreign subsidiary bribes a foreign official in cases where the parent company “authorized, directed, or controlled” that action. Moreover, it can hold an entity responsible if it bribed a foreign official through intermediaries (also called third parties) “while knowing that all or a portion of the payment will go directly or indirectly to a foreign official.”

Punishment and avoiding punishment for FCPA violations: While the FCPA punishes the bribe makers, it does not punish the foreign officials who take the bribes, say experts. For individuals who violate the FCPA, a court can (for each violation) impose civil penalties of up to \$10,000, criminal fines of up to \$250,000, and imprisonment for up to five years. For companies, a court may impose civil fines of up to \$10,000 per violation and criminal fines of up to \$2 million per violation. The government deposits these various fines directly into the U.S. Treasury, says the Justice Department.

Along with fines and imprisonment, the federal government may prohibit convicted individuals and firms from bidding on lucrative government contracts. As in the case of individuals and private companies, even governments need to buy goods and services to run its operations. In 2010, the U.S. government bought nearly \$538 billion in goods and services from private contractors, according to Jessica Tillipman of George Washington University Law School.

Violators of the FCPA may also face various other penalties and negative consequences. For instance, the federal government could deny them export licenses or suspend them from the securities industry. Parties could even face private lawsuits filed by an individual (such as a shareholder of a company) who had suffered damages because of an FCPA violation. While the FCPA statute does not contain any provisions which allow a private person to file a lawsuit against an entity for simply violating that statute itself, the Justice Department said that an FCPA prosecution could reveal violations of other statutes and that a person could then file a lawsuit because he believes that he had suffered damages because of those violations.

While the penalties for violating the FCPA can be substantial, legal experts point out that the government rarely prosecutes the majority of accused offenders. Instead, nearly all enter into what are called non-prosecution or deferred prosecution agreements with the government. Under these agreements, the government says that it will not prosecute or may even dismiss charges against companies and individuals accused of violating the FCPA if they

voluntarily disclose violations, agree to pay a fine, cooperate with government investigators, and put into place internal controls to prevent future violations, said Peter Henning, a professor at Wayne State University Law School.

According to the *Wall Street Journal*, parties accused of violating the FCPA often choose to enter into these agreements due to the financial costs associated with negative publicity and internal investigations and also the uncertainty surrounding a jury’s verdict. Companies such as Avon Products, Inc., Weatherford International Ltd., and Wal-Mart Stores, Inc. – all of which are currently under investigation for alleged violations of the FCPA – have collectively paid \$456 million to law firms and investigators to carry out internal reviews even though the government has not formally charged them with any FCPA violations. Another company paid nearly \$100 million to a law firm just to carry out a document review during a bribery investigation.

To avoid an FCPA violation in the first place, individuals and companies may obtain an opinion from the Justice Department – through what is called the Foreign Corrupt Practices Act Opinion Procedure – on whether an actual (and not hypothetical) transaction conforms to the FCPA, though they have rarely done so. From 1980 to 2012, government statistics show that the Justice Department had issued 58 opinions.

FCPA statistics and notable cases: Since the creation of the FCPA, the government has investigated more than 200 cases of alleged FCPA violations involving around 80 countries, according to the Mintz Group, which bills itself as “an international investigative services firm” helping clients comply with the FCPA.

Has the Justice Department collected more fines from and imposed more penalties on domestic or foreign companies? As of December 2012, foreign companies comprised nine out of the 10 largest FCPA cases (in terms of collected penalties and settlements) since the enactment of that statute, according to Richard Cassin, a lawyer and editor-in-chief of the *FCPA Blog*, which describes itself as the “world’s biggest anti-corruption compliance portal” on the Internet. Why do foreign companies comprise most of the largest FCPA cases? According to the general counsel of Siemens AG (which is the number one company on the top 10 list): “U.S. companies have been living with this law a lot longer than [say] European companies.”

While foreign companies make up the vast majority of the top 10 FCPA settlements and penalties, the *FCPA Blog* notes that of the 81 companies which the Justice Department is currently investigating for possible FCPA violations, the vast majority is American, including 3M, Avon Products, Inc., Bristol-Myers Squibb, Goldman Sachs Group Inc., Halliburton Company, Hewlett Packard, Kraft Foods, Inc., Morgan Stanley, Qualcomm Incorporated, and Smith & Wesson Holding Corporation.

While recent statistics seem to show a government making robust use of the FCPA, observers say that this wasn’t always the case. They point out that it had rarely enforced the FCPA during the first three decades of its existence. “It has always had teeth,” said Rachel Brewster, a professor at Harvard Law School. “The United States government just was never interested in biting.”

So what accounts for this change? Some believe that the government has ramped up its investigations and prosecutions because doing so brings in revenues to the United States during a time of continuing economic uncertainty. In 2009, the federal

government collected \$657 million in criminal fines and civil penalties, according to statistics from law firm Arnold & Porter LLP. In 2010, it collected around \$1.8 billion in total penalties while 2011 brought in close to \$700 million. In contrast, the government collected around \$11 million in fines in 2004.

Still, the Justice Department officials told *The New York Times* that “it is in the United States’ interest to prosecute corporate bribery wherever it takes place” because U.S. companies have “long complained that they are at a disadvantage when competing for overseas business against bribe-paying foreign competitors.”

While there have been many FCPA cases, some of the more significant and interesting cases have included the following:

Siemens AG: According to a 2008 U.S. government press release, Siemens (the German-based electronics and engineering giant) had committed bribery “unprecedented in scale and geographic reach,” paying at least \$805 million in bribes to foreign officials from at least 2001 through 2007 to obtain work contracts around the world. While no American had given or demanded bribes in this case, and while none of the bribes exchanged hands in the United States, the company’s stock does trade on the New York Stock Exchange, and at least \$25 million in bribes had passed through American institutions, reported *The New York Times*. As a result, the federal government said that it had jurisdiction to prosecute the company.

The company pled guilty to several counts of conspiring to violate the anti-bribery, internal controls, and record-keeping provisions of the FCPA and paid a record-breaking \$800 million in fines to the United States and another \$800 million to German authorities. It also agreed to appoint an independent compliance monitor for four years to prevent bribery in the future. Others point out that several senior executives had left the company but are still being prosecuted by the Justice Department and the SEC on civil and criminal bribery charges.

African Sting Cases: Beginning on a Miami beachfront hotel and ending at a gun show in Las Vegas, the FBI undertook the first-ever undercover sting operation – dubbed the “African Sting Cases” – in which it arrested and charged 22 U.S. executives in January 2010 for violating and conspiring to violate several provisions of the FCPA. Posing as a fake foreign official from Gabon who needed to equip his nation’s presidential guard, an undercover FBI agent offered a \$15 million contract to the executives (who run small companies which provide equipment to the military and also to law enforcement agencies) to supply him with what *The New York Times* termed a “Warlord Starter Kit,” which included “grenade launchers, rifles, handguns, ammunition or bulletproof vests” – all in exchange for a 20 percent bribe. “This is the first time we’ve used the technique of an undercover operation in a case involving foreign corporate bribery,” said then-Assistant Attorney General Breuer of the Justice Department.

But various analysts note that no jury had convicted any of the defendants during trials in 2011 and 2012. A jury foreman – writing in *FCPAProfessor.com* – said that his “jury with near unanimity found nearly all of the prosecution witnesses to be evasive and combative.” He also believed that several jurors “were troubled by the nature of the FBI sting operation,” saying that they were unwilling to convict the defendants since they “had not sought out the deal” in the first place.

Lindsey Manufacturing: In September 2010, the Justice Department charged two executives of California-based Lindsey

Manufacturing Co., which makes electrical systems, with violating the FCPA by paying nearly \$6 million in bribes (from 2002 to 2009) to high-level employees of a state-owned Mexican utility company in exchange for business contracts worth \$19 million. The government alleged that Lindsey had given substantial commissions to a third-party intermediary company in Mexico, but knew that the commissions would “be used to pay bribes to Mexican officials” at the utility. The third party had used some of the bribes to purchase a yacht and a Ferrari sports car for an official, said the indictment.

The defendants decided to fight the charges, and the case – *United States v. Lindsey* – became the first-ever criminal prosecution where a jury had to decide whether a company violated the FCPA. Up to this point, all corporate defendants in FCPA cases had reached settlements with the government or pled guilty to certain charges.

In May 2011, a jury in the U.S. District Court for the Central District of California convicted the defendants of conspiring to violate the FCPA and also for actually violating several provisions. But the judge in December 2011 threw out all of the convictions, citing “flagrant misconduct” by the prosecution, including lying to a grand jury and presenting false information in affidavits to obtain search warrants. (But the court did not exonerate the defendants of the bribery charges.) In May 2012, the government withdrew its appeal of the district court’s decision to throw out the convictions.

Wal-Mart: An April 2012 investigative report in *The New York Times* alleged that Wal-Mart’s largest subsidiary – Wal-Mart de Mexico – had, for years, “orchestrated a campaign of bribery to win market dominance” throughout Mexico, a nation which one in five Wal-Marts now calls home. Top executives, including the chief of Wal-Mart de Mexico, had apparently approved and then concealed the distribution of over \$24 million in cash-filled envelopes to Mexican officials. According to a former executive and lawyer working for Wal-Mart de Mexico, the bribes had helped to change zoning regulations, silenced the reporting of environmental violations, and pushed for the rapid processing of permits.

The former executive and lawyer for Wal-Mart de Mexico had first contacted the company’s headquarters in Bentonville, Arkansas, about the bribery scheme in September 2005. “The former executive gave names, dates, and bribe amounts,” according to the *New York Times* article. Investigators from Wal-Mart then went to Mexico where they “unearthed evidence of widespread bribery.” But the company decided not to report their findings to U.S. or Mexican authorities. It disregarded the advice from the investigators to expand the investigation (calling such a move “overly aggressive”), and then ordered a shutdown.

In December 2011, when Wal-Mart discovered that *The New York Times* was writing about the company and the alleged bribes, it contacted the Justice Department, the Securities and Exchange Commission, and also Mexican officials, saying that it had begun an internal investigation. The *Wall Street Journal* said that Wal-Mart had “portrayed itself as taking aggressive steps to address the scandal, saying it has created a new position, global compliance officer, to ensure it [was] not violating” the FCPA. The Justice Department started a criminal probe but has not issued any indictments. Various legal observers say that any investigation could take two to four years. In November 2012, Wal-Mart said that the company was expanding its bribery investigation to subsidiaries in Brazil, China, and India.

Criticisms of and proposed changes to the FCPA: Since its passage in 1977, many businesses have criticized the FCPA and have proposed several changes.

First, they point out that, in many countries, bribery is imbedded in everyday life and that the United States (because it bans the bribery of foreign officials) regularly loses business to them. An October 2010 report issued by the Institute for Legal Reform (a group which calls for the reform for the FCPA and was founded by the U.S. Chamber of Commerce) cites a government statistic

In 1977, the United States prohibited the bribery of foreign officials by enacting the *Foreign Corrupt Practices Act*. Previously, no government had made it a crime to bribe a foreign official. Many nations had even allowed companies to deduct the payment of bribes from their taxes as a business expense.

which says that the FCPA's anti-bribery provisions cause an annual loss of \$1 billion in lost export trade for the United States.

But Secretary of State Hillary Clinton, in a speech given to anti-corruption group Transparency International, said that the current administration is "unequivocally opposed to weakening" the FCPA. "We don't need to lower our standards," she said. Instead, "we need to work with other countries to raise theirs." To be sure, even the U.S. Chamber of Commerce said that "the solution to [bribery] is not to do away with the FCPA and permit American companies to engage in bribery alongside their foreign competitors."

Second, many question whether the FCPA actually deters bribery, noting that its current penalties range from \$10,000 to \$2 million per violation. Companies could view fines as "a cost of doing business," according to Professor Drury Stevenson of South Texas College of Law. These fines offer "little deterrence value in the corporate setting," he said, adding (in his opinion) that the risk of losing business by not paying a bribe outweighs "the cost of getting caught" for doing so.

But others strongly disagree, noting again that the costs to a large company in carrying out an anti-bribery investigation alone could cost hundreds of millions of dollars. Smaller businesses, they say, don't have such resources.

Third, critics point out that the FCPA does not allow individuals and companies to defend themselves against bribery charges by arguing that a rogue employee had evaded reasonable anti-bribery measures already in place. "A company can . . . currently be held liable for FCPA violations committed by its employees or subsidiaries even if a company has a first-rate FCPA compliance program," said the Institute for Legal Reform in a 2010 report called "Restoring Balance: Proposed Amendments to the Foreign Corrupt Practices Act." Instead, the Justice Department or SEC will take a company's compliance program into account only before deciding whether to enter into a non-prosecution agreement with the company, said the 2010 report. Or a court may consider it when sentencing a company.

Critics also note that when a company buys or merges with another business, the government can hold the buyer liable for FCPA violations carried out by the acquired business even if such violations had occurred before the acquisition. "You buy a company, you buy their problems," stated Rita Glavin, a former head of the

Justice Department's Criminal Division. The *Wall Street Journal* noted that "successor liability in the FCPA context, known by the shorthand of 'buying an FCPA violation,' was the subject of six enforcement actions in 2011." The Institute for Legal Reform's 2010 report added that "even when an acquiring company has conducted exhaustive due diligence and immediately self-reported the suspected violations of the target company, it is still currently legally susceptible to criminal prosecution and severe penalties."

So, according to critics, how should the government address this

perceived shortcoming? "At a minimum, a corporation (irrespective of whether or not it conducts reasonable due diligence prior to and/or immediately after an acquisition or merger) should not be held criminally liable for such historical violations," said the Institute for Legal Reform.

In response to such criticisms, experts including Matthew Feeley, an attorney with a practice focusing on FCPA violations, say that successor liability is "rooted in state common law and was developed to prevent business entities from avoiding liability by transferring ownership or modifying organizational structure." He also said that a company can take several steps to avoid successor liability. For example, if the acquiring company carries out strong due diligence and undertakes efforts to make the acquired business FCPA-compliant, "U.S. authorities may decline an enforcement action" even if the acquired business was at one time in violation of the FCPA.

Fourth, critics complain that the FCPA statute neither provides more precise definitions of various terms nor does it give more specific guidance on when the government will carry out an investigation and prosecution of an alleged FCPA violation. (Up until November 2012, companies had to rely on a government publication informally known as the "Lay Person's Guide" on the FCPA which explained the various aspects of the FCPA but did so in only six pages and without providing many examples on when exactly the government would enforce the statute. Legal experts also say that because FCPA cases are rarely adjudicated, courts have not extensively examined the government's interpretation of that statute's provisions or issued many decisions concerning it.)

Which terms and definitions are allegedly in dispute? One point of dispute, said Jamie Guerrero, a lawyer specializing in anti-corruption at Foley & Lardner LLP, "is the question of whether the individual being allegedly bribed is a 'foreign official.'" The statute, in part, defines a foreign official as "any officer or employee of a foreign government or any department, agency, or instrumentality thereof . . ."

Former U.S. Assistant Attorney General Breuer said that while some examples of foreign officials are "obvious" such as ministers and customs officials, others are not. For instance, if a foreign government partially or fully owns a facility such as a drug factory, would the FCPA view that facility as an "instrumentality" of the

government? And would the FCPA view the health professionals who work in that state-owned facility as “foreign officials,” including the “doctors, pharmacists, lab technicians,” asked Breuer?

According to the Institute for Legal Reform, “the [Justice Department] and SEC have provided no specific guidance on what sorts of entities they believe would qualify as ‘instrumentalities’ under the FCPA.” Guerrero of Foley & Lardner contends that this “lack of clarity” concerning this term and others can trip up even the most honest companies.

In response to criticism that the definitions of the FCPA are “shrouded in mystery,” Richard Cassin of the *FCPA Blog*, says “don’t believe it,” and adds that “there’s no evidence in the record that judges or juries have any trouble understanding the FCPA.” Juries understand the definitions, writes Cassin, which is why “there hasn’t been an acquittal in an FCPA trial since 1991.” (In the earlier discussed case of *United States v. Lindsey*, the judge had thrown out the defendants’ convictions due to prosecutorial misconduct. But neither the judge nor the jury had exonerated the defendants of the bribery charges.)

Still, others point out that, for the first time, an appeals court in the United States is currently reviewing a case (*United States v. Esquenazi*) where the defendants are challenging how prosecutors had defined the terms “foreign officials” and “instrumentality” in their convictions for violating the FCPA.

In August 2011, a jury in the U.S. District Court for the Southern District of Florida convicted two executives of Miami-based Terra Telecommunications Corp. on seven counts of violating the FCPA by paying close to \$900,000 to employees of state-owned Haiti Teleco – the only entity in Haiti that provides landline service – in exchange for “preferred telecommunications rates” and also for “the continuance of Terra’s telecommunications connection with Haiti,” said a Justice Department press release. (Terra had signed several contracts with Haiti Teleco so that Terra’s customers can place calls to Haiti.) It said that the former executives had used shell companies to pay the bribes and then recorded the transactions as “consulting services” which they had never intended to carry out.

The court sentenced one executive to 15 years in prison, making it the longest sentence ever given to a defendant for violating the FCPA. It sentenced the other defendant to seven years in prison.

In their brief to the U.S. Court of Appeals for the Eleventh Circuit, the defendants challenged their convictions, arguing that Haiti Telecom was not an “instrumentality” of the Haitian government within the meaning of the FCPA. In their interpretation, just because the government controls Haiti Telecom does not automatically make that entity its “instrumentality.” Instead, that term “should be construed to encompass only foreign entities performing government functions similar to department of agencies.” Because, in their opinion, Haiti Teleco does not carry out actual government functions, it is not an instrumentality. Therefore, its employees are not “foreign officials” under the FCPA. Another brief added that the term “foreign official” applies only to “traditional” government officials, reported a publication called the *International Trade Reporter*.

In response, the federal government argued in court in August 2012 that Haiti Telecom was a government instrumentality, noting that Haiti owns 97 percent of the shares of the company and would have received any profits made by it, said the *International*

Trade Reporter. The government also said that “Teleco’s status as a government instrumentality is also reflected in Haitian law that subjected Teleco officials to the prohibitions against official corruption.”

The case continues to this day, and because this is the first time an appeals court is examining the definition of terms such as “foreign official” and “instrumentality,” legal observers say that any developments will be “very, very, very closely watched” by the government and the business community.

More detailed guidance on the FCPA: In November 2012, the Justice Department and the SEC released a 120-page joint publication called “A Resource Guide to the U.S. Foreign Corrupt Practices Act” which (in a single document) provides companies of all sizes with more detailed and practical guidance on how the federal government interprets and enforces the FCPA “through hypotheticals, examples of enforcement actions, . . . and summaries of applicable case law and [Justice Department] opinion releases.” (In contrast, its predecessor publication – the 6-page “Lay Person’s Guide” on the FCPA – provided fewer details.) Some believe that with growing complaints from both U.S. and foreign companies on the government’s increased use of the FCPA, the government decided to provide them with more guidance.

The 2012 guide points out that it does not amend the existing FCPA statute. (“The enforcement agencies can’t amend the law,” said Richard Cassin of the *FCPA Blog*. “Only Congress and the President can do that.”) In fact, the Justice Department says that the guide is “non-binding, informal, and summary in nature, and the information . . . does not constitute rules or regulations.”

In the area of giving gifts and paying for travel, entertainment, and other things of value, the 2012 guide says that “the FCPA does not prohibit gift-giving,” and also acknowledges that “a small gift . . . is often an appropriate way for business people to display respect for each other.” At the same time, it says that “the FCPA prohibits the payments of bribes, including those disguised as gifts.” In several examples, the guide says that paying reasonable expenses for a foreign official such as his cab fare and meals, and giving nominal promotional materials, are unlikely to influence a foreign official but that the government would view extravagant gift-giving (including luxury items) and also “widespread gifts of smaller items” with more suspicion.

In determining whether or not an entity is an “instrumentality” of a foreign government, the guide provides a non-exhaustive list of factors which courts have considered in the past. (Despite calls from the business community, the guide does not provide a more narrow and comprehensive definition of that term.) These factors include the extent to which a government owns and whether it appoints key officers and directors to an entity.

In determining whether it should hold a company liable for alleged bribes carried out by an acquired company, the guide says that the government will examine the facts and the “applicable state, federal, and foreign law.” It then provides examples of cases where the government decided to take or not take action against companies in cases of wrongdoing by the acquired companies.

In deciding whether a company had committed an FCPA violation and whether the government should take action against it, the 2012 guide says that the government will examine whether a company has what it calls the “hallmarks” of an effective FCPA compliance program, including a “clearly articulated policy against

corruption” and oversight of compliance standards by specific individuals, among many other criteria. The guide adds that while the Justice Department and the SEC “understand that no compliance program can ever prevent all criminal activity by a corporation’s employees,” and that “they do not hold companies to a standard of perfection,” these agencies still expect companies to implement effective anti-bribery measures.

According to an interview with the *International Trade Reporter*, William Devaney, a partner in the law firm Venable LLP, said of the guide: “I think the bottom line is there’s nothing really new here, but the mere pulling it all together in one place is useful.” Added attorney Richard Cassin: “Now we have the government’s view, in its own words . . . it’s nice to know exactly how the [the Department of Justice] and the SEC view [the FCPA].”

Other anti-bribery laws from around the world

Along with the United States, many other countries have their own laws which are supposed to deter and punish bribery. But the effectiveness of these laws and the degree to which a government enforces them varies widely. Some examples include the following:

The United Kingdom: Coming into force in July 2011, some legal analysts have described the *UK Bribery Act 2010* (a criminal statute) as the toughest in the world today. The UK Ministry of Justice also released what it calls a guidance report which explains the provisions of the act in more detail.

Section 1 makes it a crime to offer or give bribes to those working in domestic government and also in the private sector. Specifically, a person commits a crime if he intends to “offer, promise, or give a financial or other advantage” (in other words, a bribe) as a way to induce another person to carry out his duties improperly. (That is to say, in exchange for receiving the bribe, a person will perform his duties in bad faith and in violation of any trust given to him.) But these duties must involve an activity related to a government service or an activity connected with a business. Section 1 even applies to duties performed outside of the UK such as those performed by a British embassy official in another country or an employee of a British subsidiary in another nation.

Under Section 2, a person working in the public and private sectors may not solicit or accept bribes. Specifically, such a person commits a crime if he “requests, agrees to receive, or accepts a financial or other advantage” in direct exchange for carrying out his duties improperly. As in the previous section, these duties must involve a public activity or an activity connected with a business. Section 2 also applies to duties performed outside of the UK.

In contrast to Sections 1 and 2 of the *UK Bribery Act*, the *Foreign Corrupt Practices Act* (or FCPA) in the United States applies only to situations where people give bribes specifically to foreign government officials. Also, the FCPA does not have any provisions which punish foreign officials who solicit or accept bribes. (Still, as mentioned in the previous section concerning the FCPA, the United States does have federal laws which not only prohibit its residents from bribing domestic officials, but also prohibit these officials from demanding or accepting bribes.)

Section 6 of the *UK Bribery Act* makes it a crime for a person to bribe a foreign public official but only if doing so satisfies three conditions. First, he must *intentionally* offer, promise, or give any financial or other advantage as a way to influence how a foreign public official carries out his duties. Second, that person must give

the bribe to a foreign public official specifically to obtain or retain business or to get “an advantage in the conduct of business.” Third, the domestic laws of the foreign public official’s home country must prohibit him “to be influenced” by the bribe. Foreign public officials include, among others, individuals who hold a “legislative, administrative, or judicial position of any kind, whether appointed or elected,” and also individuals who work for international public organizations such as the United Nations and World Bank.

Unlike the FCPA, the text of the *UK Bribery Act* does not seem to allow people to provide reasonable hospitality expenses (such as those for meals and travel) to foreign public officials. It also does not allow facilitation payments for the processing of applications and other documents. “The Bribery Act does not . . . provide any exemption for such [facilitation] payments,” says the 2011 guidance report from the Ministry of Justice. As a result, media reports have described the *UK Bribery Act* as the “toughest in the world.”

But in the guidance report, the Ministry of Justice says that while some people certainly use hospitality and facilitation payments to bribe foreign public officials, it also acknowledges that “bona fide hospitality and promotional, or other business expenditure . . . is recognised as an established and important part of doing business.” The report continues: “The Government does not intend for the Act to prohibit reasonable and proportionate hospitality and promotional or other similar business expenditure intended for these purposes” as long as those who pay for such expenses don’t intend to use them as a way to influence a foreign public official for business reasons. If a company pays for hospitality, promotional, and facilitation expenses, will it automatically trigger a prosecution? According to the guidance report, “prosecutors will consider very carefully what is in the public interest before deciding whether to prosecute.”

Under Section 7, the government could prosecute a commercial organization (such as a private company) if it fails to prevent bribery. Specifically, officials may file charges against what they call a “relevant commercial organization” if a person associated with that entity bribes another person with the specific intent to “obtain or



retain business,” or to “obtain or retain an advantage in the conduct of business.” An “associated person” can include an organization’s employees, agents, subsidiaries, contractors, suppliers, and also incorporated and unincorporated bodies, according to the 2011 guidance report.

Section 7 applies to corporate bodies or partnerships formed in the United Kingdom and which carries out business “there or elsewhere” around the world. It also applies to corporate bodies and partnerships formed in any other part of the world and which carry

Many other countries have their own laws which are supposed to deter and punish bribery. For example, some have described the *UK Bribery Act 2010* as the toughest in the world. It does not even seem to allow people to provide reasonable food and travel expenses to foreign public officials.

out their business (or parts of it) in the United Kingdom. Section 7 allows an organization to defend itself against accusations of bribery by arguing that “despite a particular case of bribery, it nevertheless had adequate procedures in place to prevent persons associated with it from bribing,” says the guidance report. (The FCPA does not allow a similar defense.)

While the FCPA does not have a provision similar to Section 7 of the *UK Bribery Act*, various analysts point out that the U.S. government can (under the FCPA) hold a company responsible for bribes made by its employees and various other agents. Also, officials say that a company may not (under the FCPA) consciously disregard or deliberately ignore the fact that an intermediary may take a payment from the company and then use it to bribe others.

What are the penalties for violating the *UK Bribery Act*? A court can mete out a sentence of up to 10 years in prison for an individual. Also, the act does not set any limits on how much a court may fine violators, says the UK government.

So does the UK have the toughest anti-bribery laws in the world? On its face, the *UK Bribery Act* may seem stricter than those in the United States. But according to an analysis carried out by the law firm Willkie Farr & Gallagher, LLP, in April 2011: “All in all, the anti-bribery legal regimes in the United States and the United Kingdom are more similar than different and are likely to be enforced in a very similar manner.”

In October 2011, prosecutors convicted its first person, 22-year old Munir Patel, under the *UK Bribery Act*. According to *BBC News*, Patel, a court clerk in London, violated Section 2 of the act when he “took £500 [in bribes from a driver] to avoid putting details of a traffic summons on a court database.” Prosecutors believe that he “earned at least £20,000 by helping 53 [traffic] offenders.” Patel pled guilty to one count of bribery (receiving a sentence of three years) and also to a separate offense for “misconduct in a public office” (resulting in a six-year sentence to be served concurrently with the first sentence).

Transparency International’s 2012 *Corruption Perceptions Index* ranks the UK’s perceived level of public sector corruption as 17th out of 176 nations.

Brazil: According to the Business Anti-Corruption Portal (which is funded by several European governments and supports small businesses around the world in their fight against corruption),

the *Penal Code* of Brazil – the largest nation and economy in South America – criminalizes various forms of corruption such as embezzlement of public funds and misconduct in public office, among other acts. In the specific area of bribery, it prohibits people from offering bribes to domestic officials and also prohibits these officials from soliciting or accepting them.

The *Penal Code* also prohibits people from bribing foreign officials during an international business transaction, according to a 2010 report issued by London-based law firm Linklaters.

Specifically, it prohibits “the direct/indirect offering, promising, or giving of any unlawful advantage to a foreign public employee in order to constrain him/her to do, omit, or delay any official act related to an international business transaction.” People who offer or give bribes can face fines and up to eight years in prison. Foreign officials who request and accept bribes can face fines and up to five years in prison.

Even with these laws in place, media reports indicate that corruption and bribery are significant problems in Brazil which its relatively new (and first woman) president, Dilma Rousseff, is trying to address in an ongoing campaign dubbed “sweeping out corruption.” During its first six months, her administration had dismissed six ministers suspected of corruption. Transparency International’s 2012 *Corruption Perceptions Index* ranks Brazil’s perceived level of public sector corruption as 69th out of 176 nations.

India: In 1988, the Indian government implemented the *Prevention of Corruption Act* which criminalizes extortion, abuse of office, money laundering, and other corrupt acts. In the specific area of bribery, the act prohibits people and middlemen from offering or giving what it calls “gratification” to domestic public officials and also prohibits these officials from requesting or accepting them. Those who offer and accept bribes can face a jail sentence of up to five years and a fine which is three times the amount of monetary gain resulting from the bribe. The Indian government is currently working on legislation to criminalize private sector bribery and the bribery of foreign officials, according to the Business Anti-Corruption Portal.

Even with such measures in place, corruption is growing “over 100 percent annually” in India, said economist Bibek Debroy at the New Delhi-based Centre for Policy Research. Transparency International’s 2012 *Corruption Perceptions Index* ranks India’s perceived level of public sector corruption as 94th out of 176 nations.

In response to growing concerns about bribery and the perceived inability of the government to address it effectively, people are paying zero-rupee notes (a fake currency) to domestic officials who request or demand bribes for free government services, reported the *World Bank Blog*.

Indonesia: The international community says that Indonesia – the largest economy in Southeast Asia – is making rapid progress in addressing corruption. For example, *Law No. 20/2001* (known

as the *Anti-Corruption Law*) prohibits people from bribing civil servants, among many other acts of corruption. Specifically, it prohibits people from “[giving] or [promising] something to a civil servant or state apparatus with the aim of persuading him/her to do something or not to do anything because of his/her position in violation of his/her obligation.” It also prohibits civil servants from requesting or accepting bribes. Violators of the law may face fines and a jail sentence ranging from one to five years.

In December 2003, the government created the Corruption Eradication Commission (or KPK) to enforce Indonesia’s anti-corruption laws. Since 2009, the KPK has been prosecuting government bribery with a 100 percent success rate, claimed the Business Anti-Corruption Portal. It also said that the government was working on a new draft of the *Anti-Corruption Law* which would allow it to prosecute not only foreigners accused of bribing Indonesian officials but also people involved in corruption in the private sector.

But even with these efforts, Transparency International noted in June 2012 that “one-third of the nation’s regents, one-fifth of its governors, and one-half of the members of the House of Representatives’ budget commission” have served jail time “for having committed felonies related to corruption spanning the entire spectrum of crimes starting with the embezzlement of public funds and extortion to taking bribes from crony businessmen lobbying for special favors.” Transparency International’s 2012 *Corruption Perceptions Index* ranks Indonesia’s perceived level of public sector corruption as 118th out of 176 nations.

Russia: Russia currently has in place a broad legal framework to fight various aspects of corruption. For example, in 2008, the government passed what it calls *Anti-Corruption Legislation* which criminalized the giving and receiving of bribes, abuse of office, and commercial bribery, reported Russian newspaper *RIA Novosti*. Penalties for bribery include fines of up to 100 times the amount of the bribe. Since May 2011, Russia has criminalized the bribery of foreign officials.

Despite these laws, the Interior Ministry estimated that the payment of bribes had tripled in 2011, averaging \$7,866 for each payoff. Experts such as Elena Panvilvoa of Transparency International said that, in Russia, “corruption isn’t only a threat to the system – it is the system.” Transparency International’s 2012 *Corruption Perceptions Index* ranks Russia’s perceived level of public sector corruption as 133rd out of 176 nations. Groups such as the Business Anti-Corruption Portal claim that the value of corrupt acts in Russia represents around 50 percent of its GDP. When asked how Russia can eradicate corruption, the then-prime minister Vladimir Putin replied: “Probably [execution by] hanging, but this is not our method.”

International treaties and agreements against bribery

Currently, a patchwork of different treaties addresses bribery. How? Nearly all of them call on nations to pass domestic laws which prohibit people and domestic public officials from giving and accepting bribes, respectively. Many also call on nations to pass domestic laws which prohibit people from bribing foreign officials. Several of these treaties even prohibit bribery in the private sector. But not all of their provisions are mandatory, and the circumstances under which they apply differ from one treaty to the next. Examples of these treaties include the following:

1996 Inter-American Convention against Corruption (or IACC): Adopted by the Organization of American States (or OAS), a regional organization of 35 nations in the Western Hemisphere, the IACC was the first international treaty addressing corruption. With the exception of Cuba, all members of the OAS, including the United States, have ratified the IACC, and its provisions apply only to them.

Despite its broad title, the IACC does not address a broad range of corrupt acts. Rather, it focuses on a few and sets common standards which signatories must adopt when addressing them. For example, under Article VII, a signatory nation must adopt domestic laws or other measures which make it a crime for people to offer a bribe (i.e., “any article of monetary value, or other benefit, such as a gift, favor, promise, or advantage”) either directly or indirectly to *domestic* government officials or to people who perform public functions. A nation must also make it a crime for a *domestic* government official to solicit or accept a bribe. These laws must also prohibit people from participating in bribery as a “coprincipal, instigator, accomplice, or accessory after the fact.”

Article VIII calls on nations to prohibit people from bribing *foreign* government officials but only when carrying out any “economic or commercial transaction.”

Along with bribery, the IACC calls on nations (in Article IX) to prohibit illicit enrichment where a government official cannot reasonably explain a significant increase in his assets “in relation to his lawful earnings during the performance of his functions.”

Other provisions are voluntary. Article III, for instance, calls on nations to consider establishing standards of conduct for government officials, creating a system to register the “incomes, assets, and liabilities” of government officials which would be open to public view, denying favorable tax treatment to people and companies which carry out corrupt acts, and requiring companies to keep accurate books and records, among other measures. (When the OAS adopted the IACC in 1996, analysts at the Open Society Foundation described provisions such as Article III as innovative.)

Article VI allows signatory nations to penalize acts of corruption not listed in the IACC if two or more of them reach a “mutual agreement” to do so.

In 2002, OAS member states created an intergovernmental body called the Mechanism for Follow-Up on the Implementation of the Inter-American Convention against Corruption (known as MESICIC) which helps OAS nations implement the IACC and also monitors their compliance with that agreement. Composed of experts from all OAS states, MESICIC “neither sanctions, grades, nor classifies states; rather it facilitates cooperation between them,” according to the OAS. After evaluating a nation’s efforts to implement its IACC obligations, the MESICIC issues a report with recommendations on how that nation can address any shortcomings.

How effective is the IACC? While the IACC sets a common standard on how nations in the Western Hemisphere must address bribery and other acts of corruption, observers note that corruption is still a problem in this region. While all OAS nations have anti-bribery laws, their levels of enforcement still vary considerably. Transparency International’s 2012 *Corruption Perceptions Index* ranks Venezuela’s perceived level of public sector corruption as 165th out of 176 nations. But the index does show some bright spots such as Chile and Uruguay which both rank in 20th place (directly below the United States).

1997 OECD Anti-Bribery Convention: While many treaties prohibit people from bribing a whole range of actors, others have a more narrow focus. For instance, the Organisation for Economic Co-operation and Development (or OECD) – an intergovernmental organization of 34 industrialized nations aim is to increase cooperation on a wide variety of economic issues – adopted in 1997 the *Anti-Bribery Convention on Combating Bribery of Foreign Public Officials in International Business Transactions* (or simply the OECD Convention). It also issued a 6-page “commentary” which provides more details and guidance for each provision. (This commentary is the equivalent of the 120-page resource guide for the *Foreign Corrupt Practices Act*, or FCPA, in the United States). As in the case of the FCPA resource guide, experts do not view the OECD commentary as binding law.

The OECD says that its anti-bribery convention was the first international treaty which had set common standards on how nations must specifically prohibit the bribery of *foreign public officials*. (The convention does not apply in cases where people bribe their own domestic officials or in cases where people bribe those working in the private sector.) The economic activity of the 34 industrialized nations which abide by the convention makes up 70 percent of world exports and 90 percent of foreign direct investment, according to the International Monetary Fund.

Under Article 1, an OECD nation must make it a crime for people to intentionally offer, promise, or give a bribe or another advantage to a foreign public official in order to obtain or retain business when carrying out an international transaction. Article 1 defines “foreign public official” as a person who holds a legislative, administrative, or judicial office of a foreign country; a person who carries out a public function for a public agency; and any official or agent of a public international organization.

As in the case of the FCPA, the provisions of the OECD Convention do not apply to “facilitating payments” such as when a foreign official charges a fee to issue a license or permit, according to the commentary. They also do not apply in cases where a foreign nation allows a certain advantage by law.

While Article 1 prohibits people from promising or giving bribes to foreign public officials, it does not prohibit foreign officials from asking or demanding them. But in 2009, the OECD adopted many voluntary recommendations on how its member nations should implement their obligations under the anti-bribery convention. Under one recommendation, nations should (but are not required to) implement Article 1 in a way which “does not provide a defence or exception where the foreign public official solicits a bribe.”

Article 1 also says that an OECD nation must make it a crime for a person to offer a bribe to a foreign public official through an intermediary, to persuade another person to assist in giving a bribe, and to authorize a bribe. Under the 2009 voluntary recommendations, the OECD said that intermediaries should include subordinates whom a manager asks to carry out a bribe. They also said that a manager should be held responsible for failing to prevent subordinates from giving bribes in cases where he had failed to supervise them or had failed to implement adequate internal controls.

How must a nation punish those who give or promise a bribe to a foreign public official? Under Article 3, a nation must use “effective, proportionate, and dissuasive criminal penalties” which are comparable to those in cases where a person bribes a domestic

public official. (In addition, a nation must ensure that it can seize and confiscate the bribe and the proceeds of bribery.) But Article 3 does not provide any specific examples of criminal penalties which a nation must impose. On the other hand, the 2009 recommendations say that a nation should be able to suspend violators from competing for public contracts, among other measures.

The OECD Convention also calls on nations to pass accounting measures to prevent and detect the bribery of foreign public officials. For example, Article 8 says that nations must prohibit people from creating off-the-book accounts, recording non-existent expenditures, and using false documents, among other actions, to hide cases of bribery of foreign public officials.

While the OECD Convention itself does not give more specific examples of how nations can prevent and detect the bribery of foreign public officials, its 2009 voluntary recommendations do. For instance, they say that private sector companies should adopt a “clearly articulated and visible corporate policy prohibiting foreign bribery” which has the “strong, explicit, and visible support and commitment from senior management.” In addition, companies should adopt a compliance program which addresses issues such as the giving of gifts, hospitality, entertainment, political contributions, and charitable donations. They further recommend that nations should ensure the independence of external auditors. Moreover, they call on governments to stop companies from deducting the cost of bribes from their taxes.

A body called the Working Group on Bribery (composed of all OECD member states) meets four times a year to oversee the implementation and enforcement of the convention. According to the OECD, monitors determine the effectiveness of each country’s anti-bribery measures in a three-phased process where they: (1) determine the adequacy of a country’s legislation in implementing the convention, (2) assess whether the nation in question is applying the legislation effectively, and (3) evaluate the country’s enforcement of the convention.

So how effective is the OECD convention? Transparency International’s *2011 Progress Report: Enforcement of the OECD Anti-Bribery Convention* praised it as “a key instrument for combating global corruption because the parties are involved in two-thirds of international trade and three-quarters of international investment.”

However, the 2011 report also criticized its effectiveness. Under criteria used by Transparency International, a nation is “actively enforcing” the OECD convention if it has at least 10 major cases (including criminal prosecutions, civil actions, and judicial investigations) of which “three must have been initiated in the last three years, and at least three concluded with substantial sanctions.” In 2011, only seven OECD nations – Denmark, Germany, Italy, Norway, Switzerland, the United Kingdom and the United States – had actively enforced the convention. Nine nations moderately enforced the convention, meaning that they had at least one major case and one active investigation.

The progress report listed the remaining 21 nations as having “little or no enforcement,” meaning that they had only minor cases and investigations. These nations included Australia, Brazil, Canada, Israel, Mexico, and South Africa. “It is particularly disturbing,” said the report, “that there are still twenty-one countries with little or no enforcement a decade after the [OECD] Convention entered into force.”

Transparency International said that “the principal cause of lagging enforcement is lack of political commitment by government leaders.” (The OECD Convention does not have an enforcement mechanism which compels members to implement their obligations.) It also noted that because the world economy was still weak, “business organizations have increasingly criticized anti-bribery enforcement as a competitive obstacle.” To strengthen enforcement measures, Transparency International recommended that OECD nations launch an “action programme” where nations

does not make any exceptions for “advantages permitted by law” or even for “gifts of very low values or socially acceptable gifts.”

To address bribery in the private sector, the Criminal Law Convention calls on a nation, when necessary, to adopt domestic laws and other measures making it a crime for people (including legal persons such as companies) to promise, offer, or give directly or indirectly any undue advantage – during a business activity only – to any person who works in any capacity for a private sector entity in exchange for breaching his duties. It also says that a nation

Currently, a patchwork of different treaties addresses bribery. Nearly all of them call on nations to pass domestic laws which prohibit people and domestic/foreign public officials from giving and accepting bribes, respectively. Several of these treaties even prohibit bribery in the private sector. But not all of their provisions are mandatory, and the circumstances under which they apply differ from one treaty to the next.

“prepare plans for strengthening enforcement and a timetable for such action.”

1999 Council of Europe Criminal Law Convention on Corruption: Passed by a regional organization called the Council of Europe, the Criminal Law Convention calls on its 48 signatory nations – located mostly in Europe, but which also includes the United States and Mexico – to create common standards in addressing corruption specifically by using criminal law. (Along with adopting this convention, the Council of Europe also issued a non-binding “Explanatory Report” which describes each provision with more background and details.) While the convention’s use of the term “corruption” in its title seems broad in scope, its provisions focus almost exclusively on bribery.

To address bribery in the public sector, the Criminal Law Convention says that a nation must, when necessary, adopt domestic laws and other measures criminalizing what it calls “active bribery” which occurs when any person intentionally promises, offers, or gives (either directly or indirectly) any undue advantage to certain actors in exchange for how they carry out their duties. These actors include a nation’s public officials, a member of any domestic or foreign public assembly such as a legislature or agency, a foreign government official, an official of any public international organization, and any officials of any international court. (In contrast to its OECD counterpart, the Criminal Law Convention prohibits the bribery of a foreign government official whether or not it occurs in the context of an international business transaction.)

The Criminal Law Convention also calls on a nation to make it a crime for all of these actors to engage in what is called “passive bribery” which occurs when they themselves solicit or receive a bribe. (The OECD Convention, on the other hand, does not address passive bribery, though it recommends that a nation prohibit such an act.)

The Explanatory Report describes an “undue advantage” as either an economic or even a non-material advantage which “the recipient is not lawfully entitled to accept or receive,” and includes, for instance, “money, holidays, loans, food and drink, a case handled within a swifter time, better career prospects, etc.” The report also

must make it a crime for any person who works in any capacity for a private sector entity to solicit or receive an undue advantage during the course of a business activity in exchange for breaching his duties.

The Explanatory Report says that nations must interpret the term “business activity” in a broad sense to include “any kind of commercial activity, in particular, trading in goods and delivering services, including services to the public.”

Along with bribery, the Criminal Law Convention calls on nations to pass domestic laws making it a crime to carry out other acts associated with bribery such as money laundering (where the briber tries to conceal the origins of proceeds derived from corrupt acts) and accounting irregularities where a company creates invoices and documents with false information.

To deter bribery and other corrupt acts, the Criminal Law Convention calls on nations to implement “effective, proportionate, and dissuasive sanctions and measures, including . . . penalties involving deprivation of liberty,” though it doesn’t provide more details or guidance. In the case of legal persons such as corporations, it recommends the same sanctions, including monetary ones.

A body called the Group of States against Corruption (which is composed of two representatives from all member states) monitors the implementation of the Criminal Law Convention by assessing whether parties to the agreement are complying with its provisions and also by issuing recommendations on how they can better carry out their obligations.

According to Transparency International, 77 percent of nations in Western Europe scored above 50 (out of 100 points) in its 2012 *Corruption Perceptions Index*. (Scores closer to 100 mean that a country’s public sector is seen as “very clean.”) Of the 20 nations with the highest rankings, 11 are located in Western Europe. Denmark and Finland tied for first place.

1999 Council of Europe Civil Law Convention on Corruption: When a person suffers damages because of an act of corruption, does he have any recourse? Can he seek compensation from the people who had carried out that act? Soon after adopting its Criminal Law Convention, the Council of Europe adopted another agreement in 1999 which uses civil law to address these questions.

Specifically, the *Civil Law Convention on Corruption* calls on its 43 signatory nations – all of which are located in Europe – to pass domestic laws which give people the right to file civil suits to recover “full compensation” for damages which resulted from an act of corruption. The Council of Europe said that the adoption of this convention marked “the first attempt to define common international rules in the field of civil law and corruption.” It also issued a separate and non-binding “Explanatory Note” which describes the provisions of this agreement with more context and detail.

The Civil Law Convention does not address a wide range of corrupt acts as its title suggests. Instead, it defines corruption as bribery, which is the “requesting, offering, giving or accepting, directly or indirectly, a bribe or any other undue advantage or prospect thereof, which distorts the proper performance of any duty or behaviour required of the recipient of the bribe.”

Under Article 3 of the Civil Law Convention, a nation must allow a person who suffered damage as a result of corruption to seek full compensation to cover “material damage, loss of profits, and non-pecuniary loss.” (The agreement does not say whether a corrupt act had to occur during a specific context such as during an international business transaction.) The Explanatory Note says that “damages must not be limited to any standard payment, but must be determined according to the loss sustained in the particular case.” A person who files a civil claim may receive both financial and non-financial compensation.

Who exactly can a plaintiff hold responsible for damages which he had suffered due to an act of corruption? According to the convention’s provisions and the Explanatory Note, a nation must allow a plaintiff to hold responsible not only those people in both the public and private sectors who had carried out and aided in such acts, but even those who failed to take action in preventing it, given their responsibilities and duties.

In order to receive compensation, a person must meet certain conditions set by Article 4. For example, a plaintiff must prove that he suffered actual damage. In addition, he must show that the defendant had committed or authorized bribery or had failed to take reasonable steps to prevent bribery. Furthermore, the plaintiff must show that the act of bribery had directly led to the damage he had suffered.

Are there cases in which a plaintiff will not receive full compensation? Under Article 5, a nation may reduce or even refuse compensation “if the plaintiff [had] by his or her own fault contributed to the damage [caused by the bribe] or to its aggravation.”

Does a person have unlimited time to file a civil suit to seek damages resulting from an act of corruption? Under Article 7, a nation must set a time limit. Once a person becomes aware (or should reasonably have been aware) that an act of corruption or damage had occurred, a nation must give that person at least three years from that time to file a civil action.

As in the case of the Council of Europe’s Criminal Law Convention on Corruption, the Group of States against Corruption monitors the implementation of the Civil Law Convention.

2003 African Union Convention on Preventing and Combating Corruption (or AU Convention): Adopted by a 53-member regional organization called the African Union, the AU Convention sets common standards which signatory nations must incorporate into their domestic laws when addressing

corruption (largely defined as bribery). Article 4, for example, says that nations must adopt domestic laws and other measures which prohibit bribery.

To address bribery in the public sector, Article 4 says that people may not offer (directly or indirectly) “any goods of monetary value, or other benefit, such as a gift, favor, promise, or advantage” to a public official which will affect the way he carries out his duties. In addition, a public official may not solicit or accept (either directly or indirectly) any goods of monetary value or other benefits which will affect how he performs his public duties. Unlike other treaties which address bribery, the AU Convention does not explicitly say whether the anti-bribery provisions of Article 4 apply to foreign public officials or whether they apply in the context of international business transactions.

To address bribery in the private sector, Article 4 says that people may not offer or give “any undue advantage” to any person who works in “any capacity” for a private sector entity. Conversely, any person working for a private sector entity may not offer a bribe to any other person working for a private sector entity which will lead to a breach of the other person’s duties. (For instance, Article 11 specifically says that a nation must adopt laws which prevent companies from paying bribes to win a contract from another company.) Article 4 also says that nations must prohibit people from offering or giving “any undue advantage” to any person in the public or private sector through an intermediary.

Along with bribery, the AU Convention calls on nations (in Article 6) to adopt laws which make it a crime for people to conceal or disguise the fact that they had gained certain property through corrupt activities. Article 7 says that nations should voluntarily require certain or all public officials “to declare their assets at the time of assumption of office, during, and after their term of office.” Under Article 8, nations must adopt laws which prohibit illicit enrichment which occurs when a public official cannot reasonably explain a significant increase in his personal assets relative to his income.

The AU Convention allows member states to prohibit other forms of corruption not listed in the treaty by reaching a “mutual agreement” with other African Union nations. And as in the case of other anti-corruption treaties, the AU Convention says that nations must adopt various other measures to combat corruption such as those which establish “independent national anti-corruption authorities or agencies” and also those which create internal accounting and auditing systems for collecting public income, custom duties, and tax receipts.

Under Article 22, a body called the Advisory Board on Corruption within the African Union – comprised of 11 independent anti-corruption experts – carries out several functions in support of the AU Convention. For example, it must encourage African Union members to adopt that agreement and carry out its provisions. The advisory board must also collect and document information concerning corruption in Africa, advise governments on how to address corruption, and submit progress reports on how every signatory nation is complying with the AU Convention.

Even with the AU Convention in place, corruption is endemic in Africa. According to Transparency International, 90 percent of nations in Sub-Saharan Africa scored below 50 (out of 100 points) in its 2012 *Corruption Perceptions Index*. (Scores closer to zero mean that a country’s public sector is seen as highly corrupt.) Of the 20 nations with the lowest rankings, eight are located in

Africa. The nations with the highest rankings are Botswana (30th), Rwanda (50th), and Namibia (58th).

2003 United Nations Convention Against Corruption: Up to the very end of the 20th century, major treaties which address bribery applied only to certain nations such as those in specific regions of the world or only to industrialized countries.

But in 2003, the UN General Assembly adopted the *UN Convention Against Corruption* (or UNCAC) which requires its 140 signatory nations to prevent and combat corruption – in particular, bribery, embezzlement, illicit enrichment, the laundering of criminal proceeds, and trading in influence – in both the public and private sectors by implementing specific measures in their domestic legal systems. More than any other treaty, experts say that the UNCAC – in a single agreement – addresses a wide range of corrupt acts. Also, “it is the only [anti-corruption] Convention that is truly global,” says Transparency International, noting that agreement’s 140 signatory nations compared to, say, the 34 nations belonging to the OECD anti-bribery convention.

To address corruption in the public sector, the UNCAC says that nations must create independent bodies which prevent corruption; adopt a transparent civil service system where the government hires and promotes people based on “merit, equity, and aptitude”; ensure an independent judiciary; and apply codes of conduct which set forth standards on the proper performance of public officials.

To address corruption in the private sector, it calls on nations to pass laws which prohibit the establishment of off-the-book accounts, the recording of non-existent expenditures, and the use of false documents, among many other measures.

The UNCAC also has “asset recovery” provisions which require countries to “establish procedures to freeze, seize, and confiscate proceeds of corrupt acts and permit those injured by corrupt acts to initiate an action for damages.” The U4 Anti-Corruption Resource Centre, a Norway-based private research group, says that this provision is “the main selling point of the Convention, and the reason why so many developing countries have ratified it.” Recovering stolen assets, say UN officials, is a “particularly important issue for many developing countries where high-level corruption has plundered the national wealth.”

How does the UNCAC specifically address bribery? For bribery aimed at the public sector, Article 15 calls on signatory nations to adopt domestic laws and other measures which make it a crime for a person to intentionally promise, offer, or give an “undue

advantage” to a *national public official*, either directly or indirectly. (The UNCAC does not define the term “undue advantage.”) It also calls on nations to make it a crime for a national public official to solicit or accept – directly or indirectly – an “undue advantage.” (In contrast, the OECD Convention applies only to the bribery of foreign public officials.)

Article 16 calls on signatory nations to adopt laws and other measures which make it a crime for a person to intentionally promise, offer, or give an undue advantage (either directly or indirectly) to a *foreign public official* or an official of a public international organization, but only in cases where he tries to obtain or retain business during an international transaction. (The OECD also has this provision.) But Article 16 does not require a nation to criminalize instances where a foreign public official (or those who work for a public international organization) solicits or accepts an undue advantage. (The OECD Convention, on the other hand, recommends that nations not make exceptions for foreign officials who solicit or accept bribes.)

When it comes to the bribery aimed at the private sector, the UNCAC diverges significantly from the OECD Convention. Article 21 of the UNCAC says that nations should (but are not required to) adopt domestic laws making it a crime for a person to promise, offer, or give an undue advantage (either directly or indirectly) to any person who works “in any capacity” for a private sector entity which would result in a breach of that person’s duties. It also says that nations should (but, again, are not required to) make it a crime for any person who works for a private sector entity “in any capacity” to solicit or accept an undue advantage which would result in a breach of his duties. (The OECD Convention does not have any comparable provisions concerning the bribery of people in the private sector.) To enforce these standards in the private sector, the UNCAC says nations must provide “effective, proportionate, and dissuasive civil, administrative, or criminal penalties,” though it doesn’t provide any specific examples.

Has the UNCAC helped to reduce instances of bribery around the world? Many analysts don’t believe so. While the UNCAC does tell nations how to address specific acts of corruption, many have neither the political will nor the financial resources to implement and carry out their obligations. (Some observers say that the convention seems “as quixotic as a decree outlawing greed, lust and the other deadly sins.”) The UNCAC also doesn’t have an enforcement mechanism which compels nations to carry out their obligations under the agreement.



Others say that the UNCAC lacked a strong monitoring system when the UN General Assembly had first adopted that agreement. After much criticism, the UNCAC's signatory nations in 2009 implemented a voluntary monitoring system where a nation fills out a self-assessment checklist which is then evaluated by a team of experts from other nations, according to the Business Anti-Corruption Portal.

How effective is the UNCAC? Transparency International's 2012 *Corruption Perceptions Index* said that 70 percent of 176 countries scored less than 50 points out of 100. (Again, scores closer to zero mean that a country's public sector is perceived as highly corrupt.) It also said 43 was the average score worldwide.

Anti-bribery efforts led by international organizations

Even though nations have created a domestic and global legal framework to address bribery, analysts point out that people throughout the world still carry out this act of corruption. In fact, in

Even though nations have created domestic and global legal frameworks to address bribery, people throughout the world still carry out this act of corruption. In fact, in many countries, bribery seems to be getting worse, say analysts.

many countries, bribery seems to be getting worse. But in recent years, several global organizations have called on their member states to do more in curbing bribery and other corrupt acts. They include:

Anti-Corruption Action Plan for Asia and the Pacific: Currently, the Asia and the Pacific region of the world does not have its own regional treaty addressing corruption. Instead, the Asian Development Bank (or ADB) and the OECD introduced a voluntary anti-corruption plan known as the *Anti-Corruption Action Plan for Asia and the Pacific*, or simply the ADB/OECD initiative in November 2001. Thirty nations, as of January 2013, have endorsed the action plan, according to the OECD. They range from powerhouses such as Australia, China, Japan, and Singapore to developing countries, including Cambodia, the Fiji Islands, and Sri Lanka.

Under the ADB/OECD initiative, nations should implement what it calls "three pillars of action" to address corruption. The first pillar calls on them to instill integrity, accountability, and transparency in public service by giving government workers enough compensation which will "sustain appropriate livelihood"; promoting transparent hiring and promotion; adopting procedures which will promote fair competition in public procurement; and abolishing ambiguous or excessive regulations which burden business, among other measures.

The second pillar calls on nations to address bribery using a wide range of measures. For example, it says that nations should adopt legislation which prohibits bribery and punishes such acts with "dissuasive sanctions." In addition, nations should ensure that their respective private sectors adopt "adequate internal company controls"; eliminate indirect support of bribery by allowing its tax deductibility; and penalize companies for falsifying books, records, and financial statements in order to hide evidence of bribery.

The third pillar says that nations should encourage public discussion of corruption by initiating public awareness campaigns,

giving a right to the public to access certain government reporting requirements, and developing relationships with civil society groups, including chambers of commerce, labor unions, and the media, among many other recommendations.

According to Transparency International's 2012 *Corruption Perceptions Index*, 68 percent of nations in the Asia Pacific region scored less than 50 points out of 100. (Scores closer to zero mean that a country's public sector is perceived as highly corrupt.) New Zealand earned a first place ranking while Afghanistan and North Korea tied for last place.

G20 Anti-Corruption Action Plan: In November 2010, a forum of nations called the Group of 20 (or G20, which consists of 20 economically influential nations) adopted an *Anti-Corruption Action Plan* where each member agreed to "lead by example" to fight corruption. The action plan neither creates any new treaties nor does it deal exclusively with bribery. Instead, it says that the G20 nations will continue to "recognize the importance of building

upon and complementing [the] existing global mechanism" in fighting a broad range of corrupt acts.

For example, the action plan calls on G20 nations to "ratify or accede, and fully implement the [*United Nations Convention against Corruption*, or UNCAC] . . . as soon as possible," and also to "invite non-G20 states to ratify or accede [to] the UNCAC." In the specific area of bribery, the action plan calls on G20 nations to "adopt and enforce laws and other measures against international bribery such as the criminalization of bribery of foreign public officials" by working more closely with the OECD in implementing that organization's anti-bribery convention.

Other broad measures in the action plan include calling on G20 nations to prevent corrupt officials from "accessing the global financial system and from laundering their proceeds of corruption," to take more measures in extraditing corrupt officials, and to provide other nations with mutual legal assistance in gathering evidence and recovering assets derived from corrupt activities.

Integrity Initial Public Offering Initiative: In April 2012, the United Nations Office on Drugs and Crime unveiled a plan called the *Integrity Initial Public Offering Initiative* which calls on the private sector (such as companies and investors) to make voluntary financial contributions – one suggestion is pledging \$2 million over five years – in helping developing nations fight corruption. This plan is not related to the traditional use of the term "initial public offering" which is the process under which a privately-owned company decides to become a public one by issuing stocks to the general public.

According to a UNODC press release, a developing country can use these funds to improve anti-corruption legislation and regulations, strengthen anti-corruption programs, and provide training to government workers.

World Bank: The World Bank has been increasing its efforts to combat corruption, and its efforts have especially had an impact

in the developing world, say some observers. The main goal of the World Bank is to reduce poverty and increase living standards in the poorest nations by providing them with financing – in the form of loans and technical assistance – for specific development projects. (In 2011, the World Bank said that it gave out \$43 billion in grants and no-interest loans.) These governments may, in turn, use such financing to hire companies and individuals to help carry out these development projects.

When giving out such financing, the World Bank has what it calls a “fiduciary duty” to “make arrangements to ensure that the proceeds of any loan are used only for the purposes for which the loan was granted.” To protect this duty, the World Bank in 2001 created an independent office called the Integrity Vice Presidency (or INT) which is “responsible for investigating allegations of fraud and corruption in Bank-financed projects.”

The INT says that it may start a corruption investigation only when it suspects that a government, company, or individual had engaged in one of “five sanctionable practices” – which include fraudulent, collusive, coercive, and obstructive acts – in Bank-financed or supported projects. Bribery is also considered a sanctionable practice, and is defined by the World Bank as “the offering, giving, receiving or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party.”

Before starting an active investigation for possible misconduct in Bank-financed or supported projects, the INT says that it can use a tool called the Voluntary Disclosure Program (or VDP) where a suspected person or company promises not to commit wrongdoing in the future, carries out (at its own expense) and then discloses the results of an internal investigation on any possible misconduct in the past concerning Bank-financed or supported projects, and implements a compliance program overseen by a monitor approved by the World Bank. Under the VDP, the INT keeps confidential the identities of these people and companies.


If a person or company under investigation refuses to participate in the VDP program, the INT will carry out a formal investigation using what the World Bank calls “a highly specialized team of investigators and trained forensic accountants.” It will then issue a Final Investigation Report. If that report substantiates the accusation of misconduct, the INT can recommend that a wrongdoer face sanctions, including debarment under which a person or company may no longer bid on World Bank-financed projects.

A sanctioned company can suffer “tens of millions of dollars in lost revenues,” according to a paper issued by the Global Anti-Corruption Task Force of the American Bar Association. It noted a recent example where Macmillan Publishers Ltd., a British publishing firm, had won \$35 million in World Bank contracts in the last decade, but had been later debarred by the World Bank from bidding on its contracts for six years because the company had paid bribes in Sudan. The authors of the paper added that “debarment usually affects parent and affiliate companies, compounding the losses exponentially.”

Since the INT’s formation in 2001, its Sanctions Board has debarred 541 firms, individuals, and non-governmental organizations “for engaging in wrongdoing.” This number includes 83 firms debarred in 2011. Stephen Zimmermann, the World

Bank’s Director of Operations, said that the World Bank’s “power of the purse” serves as a powerful deterrent to corruption.

Companies and individuals that have been debarred by the World Bank will also not be able to bid on contracts from other multilateral banks. Why? Under a 2010 instrument called the *Agreement for Mutual Enforcement of Debarment Decisions*, five multilateral banks – the African Development Bank Group, the Asian Development Bank, the European Bank for Reconstruction and Development, the Inter-American Bank Group, and the World Bank – have agreed to “enforce debarment decisions made by another Participating Institution.” Once a bank finalizes a debarment decision, it must “promptly notify” the other parties of the decision and provide them with the name of the offender, describe the misconduct which it had carried out, and list the penalty it had received. The other banks must then “enforce such decision as soon as practicable” by preventing the violator from bidding on their own contracts. Said World Bank President Robert Zoellick: “Cheat from one of us, and you will be punished by all.”

While the World Bank cannot pursue criminal charges against those parties which carry out misconduct (since that organization does not have such authority), it may refer its findings to domestic prosecutors for further investigation. 

THE INTERNATIONAL REVIEW

Fall/Winter 2012 | Volume 15, Issue 1
International law in plain English™

Center for International Law | New York Law School
185 West Broadway, New York, NY 10013-2921
Tel: 212.431.2865 | Fax: 212.966.6393
www.nyls.edu/CIL | E-mail: Michael.Rhee@nyls.edu

Director: Professor Lloyd Bonfield

Managing Editor: Michael Rhee

International Fellows: Melissa Eng '14, Joanna Lehmann '14, Sandip Pandya

The International Review is the only academic newsletter published by an ABA-accredited law school that reports on a wide range of contemporary international and comparative law issues. For a free subscription to *The International Review*, please send your name and mailing address to Michael.Rhee@nyls.edu or call 212.431.2865.



Find us on Facebook at
www.facebook.com/CenterforInternationalLaw



Stay connected with us on LinkedIn at
www.linkedin.com/pub/international-law-at-new-york-law-school/33/aab/220

Find past issues of *The International Review* at www.nyls.edu/IR.

NEW YORK LAW SCHOOL

Center for International Law
185 West Broadway
New York, NY 10013-2921

