# LEGAL FRAMEWORKS FOR COMBATING CYBERCRIME

## Drafting Procedural Laws: Empowering Law Enforcement with the Legal Tools Needed to Investigate and Deter Cybercrime[1]

Drafting laws that govern the ability of law enforcement to obtain electronic evidence is critical to any country's effort to fight crime, promote economic development, and assure the privacy of its citizens. Because of the many subtle issues that arise in this context, however, drafting such laws is not easy. The following discussion attempts to highlight some of these complex issues. Any country wishing to enact such procedural laws must carefully consider how to implement them within its existing legal and regulatory framework.

## I. Definitions

The following definitions apply to the discussion that follows:

- *traffic data* means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service;

- *content* means any information concerning the substance, purport, or meaning of a communication;

- *interception* means the acquisition of the content of a communication; it does not necessarily imply that the communication is prevented from reaching its destination.

## II. Considering Privacy and Law Enforcement Authorities

A country planning to enact laws governing law enforcement access to electronic evidence must consider the importance of privacy. Privacy is critical to the functioning of a democratic society and a healthy economy. For example, it promotes the freedom of individual thought and expression, as well as the right to free association, upon which a democratic society relies. In addition, competitive markets and economic development also rely on privacy. Businesses cannot

---

[1] This paper and the accompanying slides were presented at a workshop titled, "Legal Frameworks for Combating Cybercrime," in August 17-18, 2002, in connection with the 26th meeting of the APEC TEL. It was prepared by Richard W. Downing, Senior Counsel, Computer Crime and Intellectual Property Section, Department of Justice, United States of America.

compete successfully without the ability to discuss and make decisions in private. Moreover, privacy is critical to government's deliberative process as well. Having every decision made in the public spotlight cripples the ability of government officials to carefully consider problems and develop appropriate solutions through discussion and debate.

These basic notions of privacy fully apply to communications and actions in the electronic environment. Individuals, businesses, and governments are increasingly using electronic means to communicate. More and more, sensitive personal information, proprietary corporate information, and confidential government documents are stored in electronic form. Thus, if a society is to develop appropriate protections on privacy, it cannot ignore the need to protect privacy in the online world as well.

While providing appropriate protections for privacy is important, laws must also supply law enforcement with the tools that it needs to protect public safety. Computers and the Internet have provided terrorists and criminals with a valuable tool both to communicate and to actually commit crime. In order to deter and punish the wide range of crimes facilitated by the Internet, law enforcement investigators must have the ability to investigate them and punish the criminals. For example, if terrorists are using the Internet to communicate and coordinate attacks, law enforcement investigators must have the ability to collect those communications in order to stop the violence. Similarly, attacks on the computer networks themselves, such as the "I Love You" virus, have caused billions of U.S. dollars worth of damage world wide. In order to investigate and punish those who cause such grave harms, law enforcement must have the ability to gather electronic evidence. Indeed, in order to investigate invasions of privacy – such as when a hacker breaks into a financial institution in order to steal financial data and credit card numbers – law enforcement investigators need the authority to gain access to electronic records and communications.

*Considering Privacy and Law Enforcement Authority.* As can be seen in this last example, protecting privacy and law enforcement authority are not diametrically opposed; in other words, a reduction in one does not cause a commensurate increase in the other. In fact, three main groups in a society have the potential to invade the privacy of individuals. First, industry has the ability to invade the privacy of computer users. By tracking computer use and compiling huge databases of private information, for example, businesses can infringe on individual privacy. Such activities are generally regulated by civil laws and regulatory practices and are beyond the scope of this paper.

Second, the government can intrude on individual privacy. When exerting their authority to investigate crime, terrorism, and foreign espionage, governments collect information about citizens, organizations, and businesses. These laws serve a critical function in society by enhancing justice, the economy, and national security. Even though governments enact such laws for the public good, corrupt or over-zealous officials can abuse these authorities to the detriment of individual privacy.

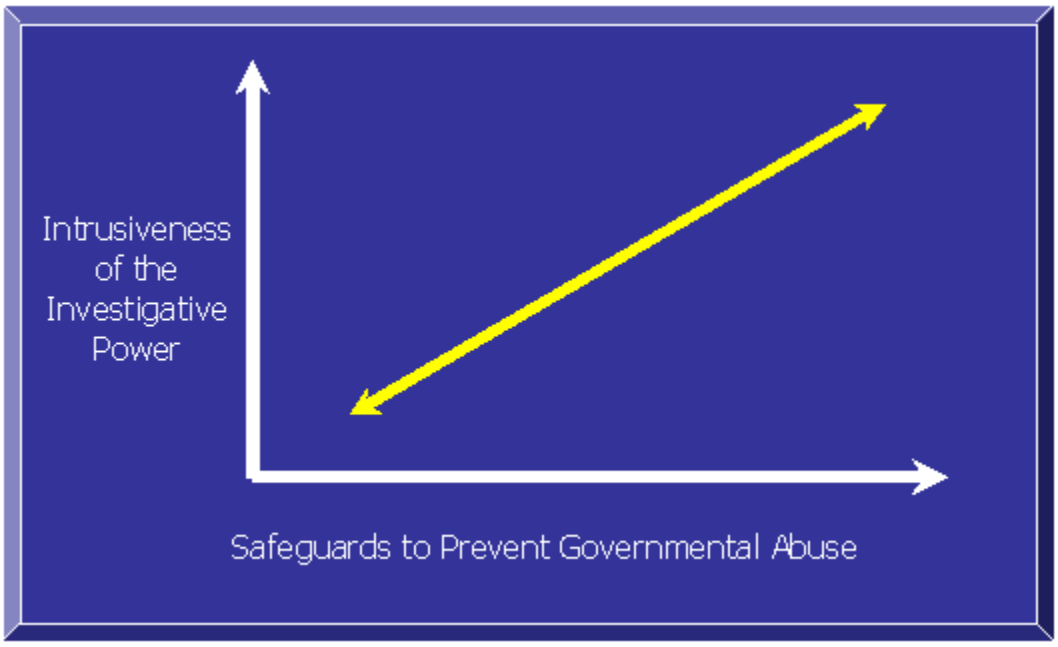
Third, criminals invade individual privacy. By stealing government or corporate secrets, by obtaining financial information from a financial institution, or by accessing the private files stored on an individual's home computer, criminals cause grave privacy violations. Obviously, in order

to deter such crimes, law enforcement must have the procedural tools to investigate them. Thus, limiting government investigative authorities in an effort to reduce *government's* ability to invade individual privacy will invariably increase *criminals'* ability to invade privacy.

No easy answers exist about how to balance these competing concerns. Each political body must make choices about this question, taking into consideration the scope of the country's crime and terrorism problem, existing legal structures, and the historical methods used by the country to protect human rights. Moreover, since the Internet has established connections between countries to an extent never seen before, this decision must also take into account the need to assist other countries in their fight against crime, terrorism, and privacy invasions.

## III. One Model for Thinking About Procedural Laws

In considering how to weigh various concerns in the drafting of procedural authorities for law enforcement, law makers should consider the following rule of thumb: the more intrusive into individual privacy a particular authority is, the greater the need for safeguards to assure that it is not abused. This model can be summarized in the following way:




The laws of many countries incorporate this basic notion. Thus, for example, the legal protections associated with the authority to obtain the content of a communication generally exceed those associated with the authority to obtain non-content or "traffic" data related to that same communication. Similarly, legal systems often provide greater limitations on the authority to

intercept a message passing over a computer network than on the authority to access the content of a file that an individual has chosen to store somewhere on a computer network. Law makers should consider how intrusive a particular authority is in the context of their countries' privacy expectations. Following this basic decision, they can choose from a long list of possible restrictions on the use of this authority.

The restrictions that countries have placed on the use of government investigative authorities include:

- Laws can require that investigators only use the authority during the investigation of one of a class of crimes or a list of particular offenses. For example, some countries' laws restrict the use of the authority for reading the content of messages to only the most serious crimes or crimes whose penalties could result in a particular term of imprisonment.

- With respect to searches that apply to stored data, such as the search and seizure of a computer from a home or business, laws can place limitations on the place to be searched. For example, investigators may have to declare what item they are searching for and can then only search in places in which that item could be hidden.

- With respect to the collection of information that will be carried out for a period of time, such as orders for the interception of communications that last for a period of weeks or months, laws can limit the activity to a specific number of weeks or months.

- Laws can require investigators to develop predicate facts before they are entitled to exercise the authority. For example, certain laws require investigators to possess "reasonable grounds" to believe that the computer has been used to commit a crime, or that electronic evidence of a crime will be found on a particular computer storage device.

- Laws can require that an independent fact finder, such as a judge, review such predicate facts before the investigators can exercise authority. Thus, countries commonly require a warrant or court order prior to the search of a home or office, or before investigators can intercept private communications.

- Laws can require that investigators only use the authority as a "last resort," i.e., that other investigative alternatives have failed or are too dangerous to try.

- Laws can establish penalties against law enforcement officials who fail to comply with the rules. Such penalties could include, for example, administrative discipline, prohibitions on the use of evidence obtained in violation of the rules, and civil and criminal liability.

- Laws can prohibit the disclosure of evidence gained through the use of such an authority where such disclosure occurs for any reason other than the official purpose. For example, laws can sanction officials administratively or even criminally if they leak evidence to the press or use it for financial advantage.

- Laws can require the approval of a senior or politically-accountable government official before investigators can use the authority. This requirement can provide a level of "quality control," restrict the number of times that an authority will be used, and reduce the danger of errors or overreaching by over-zealous investigators.

- Finally, laws can require that investigators make notifications to various parties, creating greater oversight of the use of that authority. For example, laws could require investigators to notify (1) an independent authority such as a court or (2) the individual whose information or communications was obtained. Moreover, such a notification could be required at a set point in time, or the law could allow the government to delay notification during the course of an investigation where the investigators can show that notifying the individual whose information they obtained would harm the investigation.

Law makers can decide to enact these potential restrictions on the use of investigative authorities in any of a myriad of combinations depending on the authority and the particular cultural and legal history of the country. The remainder of this paper discusses the various authorities for obtaining electronic evidence, as well as the ways in which certain countries have chosen to restrict their use.

## III. Interception of the Content of Communications on Computer Networks While They Are Occurring

Technically trained experts, in conjunction with telecommunications carriers, can intercept communications on computer networks while they are occurring using computer software, hardware, or a combination of both. For example, investigators can intercept e-mails sent from one terrorist to another, or they could intercept the commands sent by a hacker to a victim computer in order to steal corporate information. This kind of interception is similar in many ways to the interception of telephone calls. Both obtain the content of communications while the communication is being transmitted. Moreover, like traditional telephone interceptions, electronic interceptions generally require the assistance of the telecommunications provider that is carrying the communication. Indeed, at times, the provider can complete the interception on behalf of law enforcement. Because of these similarities, many countries use laws to intercept electronic communications that are the same or very similar to older laws that govern the interception of telephone calls.

*Law Enforcement Needs and Privacy Considerations.* Law enforcement needs this form of authority for the same reasons that it needs the authority to intercept telephone conversations; terrorists and criminals are increasingly using electronic communications to plan and execute conspiracies and other serious crimes. In addition, many crimes are now committed solely using computer networks such as the Internet. For example, every day, pedophiles distribute thousands or perhaps millions of images of child pornography using the Internet. Similarly, domestic and international criminals use the Internet every day to commit fraud by sending communications that dupe unsuspecting individuals into parting with their money. This kind of fraud costs victims millions of US Dollars every year and is increasing. These criminals rely on the apparent anonymity provided by the Internet. Only by equipping law enforcement investigators with the appropriate authorities can these criminals be deterred and punished. Article 21 of the Council of Europe Cybercrime Convention requires parties signing the convention to have laws that allow the interception of communications.

While this authority is critical to law enforcement efforts to fight terrorism and crime on computer networks, law makers should carefully consider the reasons for placing restrictions on its use. Interception of communications is generally regarded as an intrusive investigative technique. Unrestricted interception can constitute a grave privacy violation as it allows access to the most private communications, inhibiting the freedoms of speech and association. Moreover, fear of overly intrusive government interception of communications can stifle competitive markets, economic development, and the confidence in an country's legal system that underlies foreign investment. Thus, law makers should exercise caution to craft laws that take into account the intrusive nature of full-content, real-time interception.

*Examples of Restrictions on Interception Authorities.* Various countries have chosen different approaches to restricting the interception of electronic communications. Two fairly restrictive legal regimes are those of Australia and the United States. Australian law, for example, has the following provisions: (1) investigators must obtain a warrant from an independent judge by showing that the information gained will assist in the investigation of a serious crime (generally those with a maximum sentence of seven years imprisonment or greater); (2) the judge must balance a number of factors, including the value of the information, the gravity of the conduct, the privacy invasion, and whether other investigative techniques would not be just as effective; (3) certain disclosure restrictions apply to any information gained during the interception; (4) any evidence intercepted in violation of the law cannot be admitted into a court proceeding; (5) investigators must store the evidence for review by inspectors and destroy it once the official purpose, such as a criminal prosecution, has been accomplished; and (6) the interception can occur for only 90 days, but the court may renew the order for further 90 day periods.

The United States has a similarly restrictive set of rules. Not only must investigators meet the requirements found in Australian law, but (1) orders last for only 30 days (although they can be extended); (2) they must be approved by a high-level government official; (3) investigators must minimize the amount of non-criminal information intercepted; and (4) all individuals whose communications are intercepted must be notified at the conclusion of the investigation. While these

rules permit investigators to make relatively few interceptions based upon a court order, as described next many exceptions to these rules permit the interception of communications in particular situations.

*Exceptions Where Interception Is Less Intrusive.* Even where their laws would generally require a warrant for the interception of the content of communications, various countries, including the United States, have created exceptions to this rule. These exceptions generally apply where the privacy interests in the communication are reduced or where some other overriding need justifies the interception. Law makers might consider whether the full legal restrictions should apply in the following circumstances:

- The communications system is intended to be accessible to the public. In such cases, the need for law enforcement access to such information outweighs any possible privacy interest because *no* privacy is promised by the system. In the context of computer networks, this principle might apply to "chat rooms" or "chat channels" that are open to the public.

  United States Code: It is lawful to intercept an electronic communication "made through an electronic communication system that is configured so that [it] is readily available to the general public." 18 U.S.C. § 2511(2)(g).

- One of the parties to the communication has consented to the recording of the communication. In the computer context, such consent might be obtained at the time the user logs onto the service (through a so-called "logon banner").

  United States Code: Interception is lawful "where [a] person is a party to the communication or where one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(c), (d).

- The interception is done by the provider of the computing service in the course of providing that service or to assure that the service is not being misused. Without this kind of exception, owners of computer systems encounter substantial difficulties in securing their systems and in assuring that unauthorized users have not intruded upon them.

  United States Code: It is not unlawful for a provider of electronic communication service to intercept communications "while engaged in any activity which is a necessary incident to the rendition of ... service or to the protection of the rights or property of the provider of that service..." 18 U.S.C. § 2511(2)(a)(i).

- The interception is done by law enforcement in order to monitor the activities of unauthorized users (i.e., trespassers on the computer system). Plainly, those people who are using a computer system without authority cannot reasonably expect their

communications to remain private. 18 U.S.C. § 2511(2)(i).

Law makers should also consider those situations when information intercepted by private persons can be turned over to law enforcement. For example, the United States has enacted a law that allows information lawfully intercepted by a private person – for example under one of the exceptions to the prohibition on interception listed above – to be disclosed to law enforcement. At the same time, U.S. law does not allow illegally intercepted material to be disclosed to anyone, nor used in any court proceeding.

Finally, law makers should consider whether it should be permissible for law enforcement to ask private parties to intercept communications. For example, could investigators tracking a computer hacker who has attempted to steal government information notify a telecommunications carrier and ask them to intercept the hacker's communications? Law makers should use caution in approving such a practice, as it might effectively circumvent all restrictions on law enforcement's authority to intercept communications. U.S. law does not allow such circumventions.

## IV. Collection of Traffic Data While the Communication Is Occurring

Another important law enforcement authority allows the collection of non-content, "traffic" information. Like the interception of the content of electronic communications, this collection occurs while the communications are occurring. As in the collection of content, investigators use software, hardware, or a combination of the two to collect the information. Indeed, often the very same software program can collect either content or non-content information depending on how investigators configure it. The difference between this form of monitoring and full-content monitoring lies in the information obtained. Instead of the obtaining the content of an e-mail message, this authority would only allow collection of the source and destination of an e-mail, as well as the date and time it was sent. Similarly, instead of obtaining the actual commands that a hacker sends to a victim computer and the content of the files that he or she steals, use of this authority would obtain only the source and destination IP address and such information as the date, time, and size of the downloaded file.

*Law Enforcement Needs and Privacy Considerations.* The authority to obtain traffic information has proven to be an important procedural tool for law enforcement investigations. First, in almost every case, investigators attempt to identify the individuals responsible for some criminal conduct, such as a conspiracy to commit a crime or terrorist act. By collecting traffic data in real-time, investigators can often trace the source of the communications to help identify those responsible. In addition, as it involves far less intrusion on individual privacy, laws generally place fewer restrictions on its use than on full-content monitoring. Because investigators can use it more easily, and often at an earlier stage of an investigation, it serves a valuable function. Moreover, this authority has proven important in cases involving transborder crimes. For example, a computer user in country A can route his communications through servers in country B in order to commit a crime in country C. This authority can allow law enforcement officers in all three countries to assist in tracing the true origin of the criminal activity. Article 20 of the Council of Europe Cybercrime

Convention requires parties signing the convention to have laws that allow the collection of traffic data while the communication is occurring.

Even though traffic monitoring raises fewer privacy concerns than full-content monitoring, law makers should nevertheless consider what restrictions are appropriate on its use. With whom an individual communicates may reveal particularly private facts. For example, this authority could uncover the fact that a person is communicating with a psychiatrist or a particular political party.

*Examples of Laws.* Thus, various countries have enacted laws that impose some restrictions on the real-time collection of non-content information. The United Kingdom, for example, requires that such authority be exercised only where (1) the collected information will be "necessary" for the investigation of crime, protection of public safety, or a similar goal; (2) a high-level government official has approved it; (3) the collection is "proportionate to what is sought to be achieved"; and (4) the collection is limited to a period of 30 days. The United States has similar rules, requiring that (1) the collected information is "relevant" to an ongoing criminal investigation; (2) a judicial officer has approved it based upon the certification of a government attorney; and (3) the collection is limited to 60 days (although it can be extended). In addition, criminal, civil, and disciplinary penalties apply for unlawful collection. These statutory schemes provide some safeguards against official misuse, but they are not so restrictive that they prevent law enforcement investigators from using the authority in all sorts of investigations and at various stages of a given investigation.

Finally, law makers should consider when privacy interests are less significant, justifying an exception to any monitoring restrictions imposed by law. Such situations might include where one of the parties to the communication consents to the collection of the information, as well as when the provider of communications service collects the information for billing or security reasons.

## V. Law Enforcement Access to Content Stored on a Network

Modern computer networks commonly allow for the storage of often large amounts of data in locations distant from the computer of any given user. Law enforcement needs the authority to obtain such data or to compel the network provider to disclose that information during a criminal investigation. Such data may, for example, consist of e-mail in the possession of an Internet service provider that has been sent to one of its customers. Similarly, many networks allow for the storage of a user's files in a central high-capacity server.

The laws governing access to such information may be similar to those governing the search or seizure of information from a person's house, but they need not be identical. Indeed, because of several considerations, such laws may have fewer restrictions than those governing the search of physical spaces. First, the individual or institution that stores and can access the data is often a neutral third party, such as a legitimate corporation or service provider. In these circumstances, the coerciveness of traditional legal processes – such as the authority to forcibly enter private property without permission, for example – are inapplicable. Moreover, when individuals choose to store their data with a third party, rather than in their homes or on their persons, this choice may lessen

their expectation of privacy in that information.

*Law Enforcement Needs and Privacy Considerations*. Having the authority to access information stored on a computer network is critical to the investigation of cybercrimes. For example, very often, such information constitutes the "crime scene" from which investigators find clues about what was stolen, how it was accomplished, and who the perpetrator might be. Just as law enforcement needs the power to obtain evidence, or to compel individuals and companies to provide evidence, in more traditional investigations, so they must have the parallel power when the information is in electronic form. Without this authority, law enforcement would be severely hampered in a wide variety of investigations. Article 18 of the Council of Europe Cybercrime Convention requires parties signing the convention to have laws that grant law enforcement access to the content of information stored on computer networks.

Even if individuals may not have as significant a privacy interest in data stored remotely, they may nevertheless retain a substantial expectation of privacy in that information. Businesses, governments, and individuals, store more and more of their most sensitive data in electronic form on remote servers. Thus, law makers should consider reasonable restrictions on law enforcement authority to access such information, bearing in mind that investigators' access to such information also enhances privacy when used to investigate or prosecute criminals who invade privacy by stealing that very same information.

*Example of Laws.* The United States Code grants the greatest level of protection to e-mail that is stored incident to transmission; that is, e-mail stored by the provider that is en route to its destination and about which the receiver may have no knowledge. For this category of stored information, the law requires a search warrant issued by a neutral magistrate and supported by "probable cause" – the same type of legal process used to search an individual's home. In addition, the law provides for administrative sanctions against investigators who abuse this authority (such as demotion or other employee discipline), civil suits against the government for any violation in the procedure, and disclosure restrictions on any information gained by this authority.

Law makers should also consider, however, whether all categories of stored content deserve the same kinds of protections. For example, perhaps information that a user chooses to store at the remote location on the network. The United States code makes exactly this kind of distinctions. For example, when a user accesses e-mail but later chooses to store it at the remote location (by placing it in a "saved mail" folder, for example), investigators may obtain it with the less demanding form of legal process.

Finally, law makers should consider the circumstances under which providers can voluntarily turn information over to law enforcement authorities. On the one hand, unrestricted disclosures by providers might overly infringe on personal privacy, especially where law enforcement officials can exert unofficial pressure on service providers. On the other hand, under certain circumstances, allowing providers to make voluntary disclosures makes sense. For example, information relating to a threat to public health or safety should justify voluntary disclosure, as should information turned

over to law enforcement in order to report an attack on the provider's network.

## VI. Law Enforcement Access to Non-Content Information Stored on a Network

Computer networks generally create many records that show who is using the network, to whom they are sending communications, from whom they are receiving communications, and what actions they have taken with respect to computer programs and information stored on the network. Although these records are often critical to solving a crime or act of terrorism facilitated by the network, access to these records generally raises fewer privacy concerns than access to the actual content of the related communications. For example, in order to determine who sent an e-mail to a known terrorist organization, investigators must relay on stored traffic information if they did not – as is often the case – intercept the e-mail or its associated traffic information while the communication is occurring. Similarly, if investigators have identified an account at an Internet service provider as an account being used to distribute images of child pornography, the next step is to seek disclosure of logs that show what telephone number was used to access the account. Only by having the authority to compel disclosure of logs that record this information can they complete the trace and identify the perpetrator.

*Examples of Laws*. Although laws could treat all kinds of traffic data equally, they need not do so; some kinds of non-content data raise fewer privacy concerns than others. For example, laws could differentiate between basic information about the customer of an Internet service provider – such as the customer's name, home address, and the means used to pay for the account – from records that show all of that individual's activities in using the account – such as to whom he or she sent e-mails and from whom he or she received them. Indeed, the United States Code makes exactly this distinction. Investigators can obtain information identifying the subscriber with legal process that requires only that the information be "relevant" to the investigation, but must justify to a court on the basis of "specific and articulable facts" the need for the latter information.

*Preservation of Stored Records and Information*. One final consideration involves the preservation of records. Electronic evidence in general, and log records containing traffic information in particular, are all quite ephemeral. Providers often do not want to bear the expense of storing such records, and some do not even keep such records at all. These records can be easily deleted in the ordinary course of the provider's business (quite apart from criminals who delete the logs with ill intent), and it is not unusual for providers to keep them for a matter of days or weeks. In addition, investigators do not always know that a crime has been committed until days or weeks have passed, making it likely that the provider has deleted the records the investigators need to trace the communications and identify the criminal. Moreover, the legal procedures for obtaining these records often remain quite slow.

One tool that eases these investigative burdens is the power to compel a provider to preserve – but not yet disclose – records and other information that pertain to a criminal investigation. Because the evidence can be destroyed so quickly, if such an authority is to have any meaningful effect, it must be very fast and not involve the prior approval of a neutral magistrate. Such an

approval is unnecessary, however, since the privacy concerns relating to preservation are quite minimal because no information is disclosed until the regular legal procedure is followed. The request for preservation simply freezes the evidence so that it will not disappear while the investigators complete the necessary legal procedures. If they cannot later justify their need for the information or meet whatever legal restrictions apply, then the provider never discloses the evidence to them.

The United States Code provides an example of this sort of provision. By merely making a written or oral request, a law enforcement investigator can require a provider to "take all necessary steps to preserve records or other evidence in its possession pending the issuance of a court order or other process." 18 U.S.C. § 2703(f). Such a preservation request freezes the information for 90 days and can be renewed.

## VII. Compelling Disclosure of Electronic Evidence in the Possession of the Target

This final section provides a brief overview of the authorities needed to search for or seize electronic evidence in the control of the target of an investigation. As a general matter, most countries have laws that allow for the search and seizure of physical objects and documents that provide evidence of the commission of a crime. Law makers need to consider, however, how well these authorities apply to the seizure of intangible evidence, such as information stored on a computer hard drive.

Law enforcement plainly needs the authority to search for or seize computers and electronic evidence in the hands of criminals. In crimes facilitated by the Internet, for example, investigators generally need to trace the communications back to their origin. Once they have identified the home or business computer that sent the electronic communications, they generally need to seize it in order to confirm the clues they have previously gathered and identify the individual who sent the communications. Thus, if a bank computer is penetrated and money is stolen, investigators need to examine the bank computer's log records, trace the communications back to an Internet service provider, and finally locate the particular place from which the hacker committed the crime. As the final step in such an investigation, investigators generally will search that location, seize the computer or its electronic information, and arrest the perpetrator. Article 19 of the Council of Europe Cybercrime Convention requires parties signing the convention to have laws that law enforcement the authority to make such seizures.

*Seizing Computers vs. Seizing Electronic Data*. Often, investigators need to seize the computer hardware itself. This may be necessary, for example, so that they can have it examined in a computer forensic lab or because it contains contraband, such as child pornography. In such cases, the computer should be treated like any other physical object, and the traditional rules for seizure of physical evidence should probably apply.

If, on the other hand, investigators do not need to seize the hardware itself but instead merely need to copy files on the computer or even make an exact copy of the entire electronic storage device, the question becomes less clear. In this scenario, the investigators do not remove any physical thing from the premises, nor do they deprive the owner of the use of that information. On the surface, it may appear that these considerations make such a action less invasive or less detrimental to the rights of the computer owner. Yet data stored in a home or business can be very sensitive, including such items as a diary, a will, or corporate financial or proprietary information. A good argument can be made that such information should be treated in a single way, regardless of whether it is stored on paper or in an electronic form.

Thus, law makers should strongly consider making the rules for copying data equivalent to those for seizing the computer hardware that contains that electronic data. Using accepted rules and procedures provides balance and certainty to the investigatory process. Of course, if investigators meet whatever legal rules apply, copying of information in lieu of seizing a computer should be a permissible search and seizure method. Moreover, to the extent that exceptions to the traditional rules exist – perhaps for cases in which law enforcement officers have the consent of the property owner or where there is an emergency threatening public health or safety – these exceptions should also apply to the copying of data or the seizure of computer hardware.

## VIII. Conclusion

In order to be able to combat cybercrime within its jurisdiction and assist in criminal investigations that cross borders, each country must have procedural laws in place that allow law enforcement investigators to collect various kinds of electronic evidence. If a country implements these authorities without any oversight or restrictions on their use, however, they can infringe on the privacy rights of citizens and chill economic development. Thus, law makers must consider many factors when fashioning appropriate laws, taking into account the needs of the country, the privacy expectations historically held by the people, and legal context in which such laws will be enacted.