International Telecommunication Union

Cybercrime Legislation Resources

ITU TOOLKIT FOR CYBERCRIME LEGISLATION

Developed through the
American Bar Association's Privacy & Computer Crime Committee
Section of Science & Technology Law
With Global Participation

ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Sector

Draft Rev. February 2010

For further information, please contact the
ITU-D ICT Applications and Cybersecurity Division at cybmail@itu.int

Acknowledgements

We are pleased to share with you a revised version of the **ITU Toolkit for Cybercrime Legislation.** This version reflects the feedback received since the launch of the Toolkit in May 2009. If you still have input and feedback on the Toolkit, please do not hesitate to share this with us in the BDT's ICT Applications and Cybersecurity Division at: cybmail@itu.int. (*The deadline for input on this version of the document is 31 July 2010.*)

This report was commissioned by the ITU Development Sector's ICT Applications and Cybersecurity Division.

The ITU Toolkit for Cybercrime Legislation was developed by the American Bar Association's Privacy & Computer Crime Committee, with Jody R. Westby as the Project Chair & Editor.

Denominations and classifications employed in this publication do not imply any opinion concerning the legal or other status of any territory or any endorsement or acceptance of any boundary. Where the designation "country" appears in this publication, it covers countries and territories.

The ITU Toolkit for Cybercrime Legislation is available online at:

www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

This document has been issued without formal editing.

For further information on the publication, please contact:

ICT Applications and Cybersecurity Division (CYB)
Policies and Strategies Department
Bureau for Telecommunication Development
International Telecommunication Union
Place des Nations
1211 Geneva 20
Switzerland
Telephone: +41 22 730 5825/6052
Fax: +41 22 730 5484
E-mail: cybmail@itu.int
Website: www.itu.int/ITU-D/cyb/

Disclaimer

The opinions expressed in this report are those of the author(s) and do not necessarily represent the views of the International Telecommunication Union (ITU) or its membership. The designations employed and the presentation of material, including maps, do not imply the expression of any opinion whatsoever on the part of ITU concerning the legal status of any country, territory, city or area, or concerning the delimitations of its frontiers or boundaries. Mention and references to specific countries, companies, products, initiatives or guidelines do not in any way imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned.

ABBREVIATIONS

ABA	American Bar Association
APEC	Asia-Pacific Economic Cooperation Forum
APIG	All Party Internet Group
ASEAN	Association of Southeast Asian Nations
CFAA	Computer Fraud and Abuse Act (U.S.)
CMA	Computer Misuse Act (U.K.) & Computer Misuse Act (Singapore)
CoE	Council of Europe
DDoS	Distributed Denial of Service
EC	European Commission
EC Regulations	Privacy and Electronic Communications Regulations 2003 (United Kingdom)
ECPA	Electronic Communications Privacy Act (U.S.)
EU	European Union
G8	Group of Eight Nations
GCA	Global Cybersecurity Agenda
IAG	International Assistance Group (Canada)
ICT	Information and Communication Technology
IRG	Gesetz über die internationale Rechtshilfe in Strafsachen
ITU	International Telecommunication Union
OECD	Organization for Economic Cooperation and Development
OWig	Gesetz über Ordnungswidrigkeiten (Germany)
PACC	ABA Privacy & Computer Crime Committee
RIPA	Regulation of Investigatory Powers Act (United Kingdom)
S/S	Search and Seizure
StGB	German Criminal Code (Strafgesetzbuch)
StPO	German Code of Criminal Procedure (Strafprozessordnung)
TKG	German Telecommunications Act (Telekommunikationgesetz)
U.K.	United Kingdom
UN	United Nations
UrhG	German Copyright Act (Urheberrechtsgesecht)
U.S.	United States
WSIS	World Summit on the Information Society

TABLE OF CONTENTS

1. Toolkit for Cybercrime Legislation Project

The *Toolkit for Cybercrime Legislation (Toolkit)* was developed by a global, multidisciplinary team of policy experts, industry representatives, academicians, attorneys, technical experts, and government personnel from around the globe working through the American Bar Association's (ABA) Privacy & Computer Crime Committee (PACC), Section of Science and Technology Law. The project was led by Jody R. Westby, chair of the PACC, and member of the ITU Secretary-General's High Level Experts Group on Cybersecurity. The project vice chair was David Weitzel, PACC vice chair.

2. Introduction

2.1. Background

The interconnected networks of the Internet have enabled unprecedented economic opportunities and linked populations around the globe in ways never before possible. The benefits of the Internet, however, are being undercut by those exploiting its capabilities to the detriment and harm of others. Improvements in security are required in order to ensure the continued positive contributions of the Internet.

Because of the complex characteristics of the Internet and its population of users, multiple security measures – both technical and non-technical – are required to provide adequate protection against its misuse. A necessary and vitally important protection mechanism is a harmonized international legal framework to combat cybercrime. Although such a harmonized framework exists for international trade and services, there is not an equivalent framework applicable to the communications that support these activities.

Today, although every country on the planet is connected to the Internet, many of them do not have a cybercrime law, and among those that do, the conflicts and inconsistencies in the laws make it difficult or impossible to investigate, prosecute, and punish cyber criminal behavior. The lack of a globally harmonized legal framework with respect to cyber criminal activities has become an issue requiring the urgent attention of all nations.

A number of international initiatives aimed at improving the security of cyberspace precede the work of the ITU Toolkit for Cybercrime Legislation project. The United Nations (UN) has been a forerunner in promoting global approaches to cybersecurity and encouraging its Member States to take appropriate action in their countries. As early as 1990 – before the Internet was turned over to commercial providers and before the first browser was invented – UN Resolution 45/121[1] endorsed the recommendations of the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,[2] noting in particular the resolution on computer-related crimes, which called upon Member States to intensify their efforts to combat computer-related abuses more effectively.

In 2001, UN General Assembly Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies"[3] advocated a global framework to counter cybercriminal behavior. This action was

[1] "Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders," United Nations, General Assembly Resolution 45/121, A/RES/45/121, Dec. 14, 1990, http://www.un.org/documents/ga/res/45/a45r121.htm.

[2] *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, Havana, 27 Aug.—7 Sept. 1990, report prepared by the Secretariat (United Nations publication, Sales No. E.91.IV.2).

[3] "Combating the criminal misuse of information technologies," United Nations, General Assembly Resolution 56/121, A/RES/56/121, Jan. 23, 2002, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf ; "Combating the criminal misuse of information technologies," United Nations, General Assembly Resolution 55/63, A/RES/53/63, Jan. 22, 2001, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf .

followed by Resolutions 57/239 in 2002[4] 58/199 in 2004,[5] which encouraged Member States to create a global culture of cybersecurity and to take action regarding the protection of critical infrastructure. Following the 2003 and 2005 World Summits on the Information Society (WSIS), the ITU was entrusted to take the lead as the sole facilitator for Action Line C5, "Building confidence and security in the use of information and communication technologies."[6]

Other multilateral fora also have contributed toward advancing global cybersecurity. For example, the 2002 Organization for Economic Cooperation and Development's (OECD) "Guidelines for the Security of Information and Networks: Towards a Culture of Security,"[7] set forth nine essential principles in creating and maintaining that culture. Other notable actions taken by multilateral organizations include the Council of Europe (CoE) Convention on Cybercrime,[8] the European Union's (EU) Ministers of Justice adoption of the Proposal for a Council Framework Decision on attacks against information systems,[9] the Group of Eight's (G8) Ten Principles to Combat High-Tech Crime, Action Plan to Combat High-Tech Crime, and 24/7 Point of Contact Network, the Asia-Pacific Economic Cooperation (APEC) forum's Cyber Security Strategy,[10] and the APEC Telecommunications and Information Working Group: APEC-ASEAN Joint Workshop on Network Security.[11]

The ITU Global Cybersecurity Agenda, its work in its Telecommunication Development Bureau programme, and other efforts build on all of these activities to boost the state of cybersecurity globally. The ITU Toolkit for Cybercrime Legislation addresses the first of the seven strategic goals of the ITU Global Cybersecurity Agenda (GCA), which is the elaboration of strategies for the development of cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures by providing a model law for countries.

The adoption by all countries of appropriate legislation against the misuse of information and communication technologies (ICTs) for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cybersecurity. Since threats can originate anywhere around the globe, the challenges are inherently international in scope and require international cooperation, investigative assistance, and common substantive and procedural provisions. Thus, it is important that countries harmonize their legal frameworks to combat cybercrime and facilitate international cooperation.

[4] "Creation of a global culture of cybersecurity," United Nations, General Assembly Resolution 57/239, A/RES/57/239, Jan. 31, 2003, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.

[5] "Creation of a global culture of cybersecurity and the protection of critical information infrastructures," United Nations, General Assembly Resolution 58/199, A/RES/58/199, Jan. 30, 2004, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf .

[6] WSIS Action Line, "C5. Building confidence and security in the use of ICTs," World Summit on the Information Society, http://www.wsis-pct.org/security.html.

[7] *OECD Guidelines for the Culture of Information Systems and Networks: Towards a Culture of Security,* Organization for Economic Cooperation and Development, Directorate for Science, Technology, and Industry, http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html; *OECD Implementation Plan for the OECD Guidelines for the Culture of Information Systems and Networks: Towards a Culture of Security,"* Organization for Economic Cooperation and Development, Working Party on Information Security and Privacy, DSTI/ICCP/REG(2003)5/REV1, July 2, 2003, http://www.oecd.org/dataoecd/23/11/31670189.pdf.

[8] Council of Europe *Convention on Cybercrime* – Budapest, 23.XI.2001 (ETS No. 185) (2002), Article 12, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm; Council of Europe *Convention on Cybercrime Explanatory Report*, Nov. 8, 2001, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[9] *Proposal for a Council Framework Decision on attacks against information systems*, Commission of the European Communities, Articles 3-5, Apr. 19, 2002, COM(2002) 173 final, 2002/0086 (CNS), http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=173082; *see also Explanatory Memorandum: Proposal for a Council Framework Decision on attacks against information systems*, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=en&numdoc=52002PC0173.

[10] *APEC Cybersecurity Strategy*, APEC Telecommunications and Information Working Group, Aug. 19-23, 2002, (presented at the APEC 26th Meeting, Moscow, Russia), http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012298.pdf.

[11] Asia-Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group, Apr. 23-27, 2007 (presented at the APEC-ASEAN Joint Workshop on Network Security). ASEAN is an acronym for the Association of Southeast Asian Nations, *see* http://www.aseansec.org/.

2.2. Purpose

The *Toolkit* is intended to advance ITU work in the are of cybercrime, addressing the first of the seven strategic goals of the ITU Global Cybersecurity Agenda (GCA)[12], which calls for the elaboration of strategies for the development of cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures, as well as addressing ITU-D Study Group Q22/1 approach to organizing national cybersecurity efforts

The adoption by all countries of appropriate legislation against the misuse of ICTs for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cybersecurity. Since threats can originate anywhere around the globe, the challenges are inherently international in scope and require international cooperation, investigative assistance, and common substantive and procedural provisions. Thus, it is important that countries harmonize their legal frameworks to combat cybercrime and facilitate international cooperation.[13]

The *Toolkit* aims to provide countries with sample legislative language and reference materials that can assist in the establishment of harmonized cybercrime laws and procedural rules. The Sample Language provided in the *Toolkit*, while not a model law, was developed after a comprehensive analysis of the laws of developed nations and the Council of Europe (CoE) Convention on Cybercrime. The *Toolkit* language is consistent with these laws and is intended to serve as a guide for countries desiring to develop, draft, or modify their own cybercrime laws. The *Toolkit* is intended to advance the global harmonization of cybercrime laws by serving as a central resource to help legislators, attorneys, government officials, policy experts, and industry representatives around the globe move their countries toward a consistent legal framework that protects against the misuse of ICTs.

There is precedent for UN leadership with respect to legal frameworks and the use of the Internet. The UN significantly advanced global connectivity and a harmonized framework to electronic commerce through its Model Law on Electronic Commerce[14] and its Model Law on Electronic Signatures.[15] These documents have assisted numerous countries – developed and developing – in drafting their own national laws and helped promote uniformity for global electronic commerce.

The *Toolkit's* Sample Language may be customized to suit the laws of a particular country, but it is desirable that the resulting statutory language remains consistent with the intent of the Sample Language. Countries that model their cybercrime laws after the *Toolkit's* Sample Language will help advance a harmonized global framework, facilitate international cooperation, resolve jurisdictional and evidentiary issues, and deter cyber criminal behavior. The ABA Privacy and Computer Crime Committee's book, *International Guide to Combating Cybercrime,*[16] discusses the full range of issues that must be considered in effectively countering cybercrime.

In addition to the sample language, the *Toolkit* contains three additional sections of information that serve as practical aids in developing cybercrime legislation: (1) Explanatory Comments regarding certain provisions or aspects of the Sample Language, (2) a Matrix of International Cybercrime Laws that compares the provisions of

[12] *See* "ITU Global Cybersecurity Agenda (GCA): A framework for international cooperation in cybersecurity," http://www.itu.int/osg/csd/cybersecurity/gca/.

[13] ITU-D: ICT Applications and Security Division: Cybersecurity: Legislation and Enforcement," http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

[14] *UNICTRAL Model Law on Electronic Commerce with Guide to Enactment,* United Nations Commission on International Trade Law, 1996, http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html.

[15] *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001,* United Nations Commission on International Trade Law, 2001, http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf.

[16] The *International Guide to Combating Cybercrime*, the *International Guide to Privacy*, the *International Guide to Cyber Security*, and the *Roadmap to an Enterprise Security Program* were developed by the ABA Privacy & Computer Crime Committee and are free to people in developing countries. To receive links to complimentary downloads, send an email to Jody Westby, chair of the Committee, at westby@mindspring.com.

various countries’ laws, including the Council of Europe Convention on Cybercrime, and (3) a listing of useful reference materials of various works, laws, books, and articles that discuss cybercrime laws and issues.

3. Sample Legislative Language

Preamble

This Law is necessary and based upon the common understanding of this country and the global community of nation states that the security and economic well being of all is dependent upon a harmonized global framework that counters cybercrime. Therefore:

Having regard to UN General Assembly Resolutions 45/121, 55/63, 56/121, 57/239, and 58/199 with respect to countering cybercrimes and the misuse of computers and creating cultures of security, and with respect to the extensive work advancing cybersecurity that has been performed by numerous multilateral organizations, such as the Organization for Economic Cooperation and Development, the Asia-Pacific Economic Cooperation forum, the Group of Eight, and the Council of Europe, with particular regard to the Convention on Cybercrime;

Believing that globalization and the use of cyberspace continues to spawn both positive and negative social impacts, resulting in legitimate trade and criminal activities that co-exist in the same network commons;

Realizing that positive impacts of the Internet and ICTs include a limitless possibility for improving human conditions in this and all nations by providing new mechanisms for education, facilitating global trade, meeting the basic needs of people, improving communication and health care, enabling economic benefits, and offering opportunities for upward mobility to underserved populations;

Acknowledging the negative impacts of global connectivity – such as interference with networks and data, theft and/or disclosure of private or protected information, fraud, identity theft, money laundering, phishing, spam, and disruptions to critical infrastructure or cyber warfare – work to prevent many from participating in or realizing the full benefits of the new global community;

Admitting that resources for addressing the problem of cybercrime and assuring the safety and security of networks vary within enterprises and across nations, and that even in the best of circumstances, system administrators are overtaxed and under-prepared to deal with the continuous barrage and evolution of threats;

Understanding that deterring cybercrime is necessary to enabling the benefits of cyberspace for the global population, and that such deterrence requires international cooperation, information sharing, and investigative assistance among all nations and global harmony in legal systems;

Considering that it is necessary to define the behaviors, actions, and activities that can be consistently described as unacceptable, along with the procedures to be followed when these behaviors are observed or investigated;

Realizing that the ability to effectively prosecute cyber criminals—and cyber terrorists—requires common approaches to the criminality of such acts as well as consistency with respect to jurisdictional issues, such as cooperation in investigations, search and seizure of digital evidence, and extradition;

Understanding that harmonizing laws will help to eliminate safe havens for attackers and establish a uniform risk to which they place themselves through their actions;

Desiring to further secure the benefits of cyberspace and a globally connected society for this country through our collaboration, cooperation, and coordination in the investigation and prosecution of cyber criminal acts that occur domestically and across international borders;

Acknowledging that cyberspace requires a framework that can adapt and extend existing legal responses that have been effective in deterring crimes committed offline into the realm of cyberspace; in other cases, new rules must address crimes that have no existing offline counterpart, and thus require a completely new legislative effort;

Concluding that this Law is required in order to enable the people of this country the opportunity to enjoy the benefits of cyberspace and to deter and to punish those who would inflict harm by the use of its networks.

Title 1: Definitions

Section 1. Definitions

For purposes of this Law:

(a) Access

Access means to make use of; to gain entry to; to view, display, instruct, or communicate with; to store data in or retrieve data from; to copy, move, add, change, or remove data; or otherwise make use of, configure, or reconfigure any resources of a computer program, computer, computer system, network, or their accessories or components, whether in whole or in part, including the logical, arithmetical, memory, transmission, data storage, processor, or memory functions of a computer, computer system, or network, whether by physical, virtual, direct, or indirect means or by electronic, magnetic, audio, optical, or other means.

(b) Computer

Computer means an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping or such devices, capable of performing logical, arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device(s), but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

(c) Computer Data

Computer data means any representation of facts, information, concepts, elements, state, or instructions in a form suitable for communications, interpretation, or processing in a computer program or part of a program, computer, or computer system, suitable to cause a computer program, computer, computer system, or network to perform a function, process, and/or operation. Computer data could include flowcharts, architectures, program hierarchies and interfaces, libraries, directories, topologies, taxonomies, process flows, internal controls, metadata, etc.

(d) Computer Program

Computer program means a set of coded instructions, whether in machine readable or human readable formats (source code or object code), that enables a computer, computer system, and/or network to process computer data, traffic data, and/or content data to cause such computer, computer system, and/or network to perform a function and/or operation.

(e) Computer System

Computer System means a computer, physical or virtual, or collection of such computers and any components and/or accessories, temporarily or permanently interconnected or related, and one or more of which contain computer programs, computer data, content data, and/or traffic data, in whatever form, that perform functions, including, but not limited to: logic, arithmetic, information creation, storage, sorting, copying, changing, retrieval, destruction, routing**,** communications, and/or control.

(f) Content Data

Content Data means any data whether in digital, optical, or other form, including metadata, that conveys essence, substance, information, meaning, purpose, intent, or intelligence, either singularly or when in a combined form, in either its unprocessed or processed form. Content data includes any data that conveys the meaning or substance of a communication as well as data processed, stored, or transmitted by computer programs.

(g) Critical Infrastructure

Critical infrastructure means the computers, computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data, content data and/or traffic data so vital to this country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.

(h) Cyberspace

The physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, networks, and their computer programs, computer data, content data, traffic data, and users.

(i) Damage

Damage means any disruption, interception, interference, and/or destruction of computer data, content data, traffic data, a computer program, computer, computer system, or network, including the transmission and/or receipt of computer data, content data, or traffic data by a computer program, computer, computer system, or network.

(j) Disruption

An event that causes a computer program, computer, computer system, network, or component thereof, to be inoperable, or operate in an unintended manner, for a length of time due to destruction of and/or interference with a computer program, computer, computer system, network, computer data, content data, and/or traffic data.

(k) Interception

Interception means the acquisition, viewing, capture, or copying of the contents or a portion thereof, of any communication, including content data, computer data, traffic data, and/or electronic emissions thereof, whether by wire, wireless, electronic, optical, magnetic, oral, or other means, *during transmission* through the use of any electronic, mechanical, optical, wave, electromechanical, or other device.

(l) Interference

Interference means (i) hindering, blocking, impeding, interrupting, or impairing the processing of, functioning of, access to, or confidentiality, integrity, or availability of a computer program, computer, computer system, network, computer data, content data, or traffic data by inputting, transmitting, damaging, deleting, destroying, deteriorating, altering, or suppressing computer data, content data, traffic data, a computer program, computer, computer system, or network, and/or (ii) corrupting, damaging, deleting, deteriorating, altering, or suppressing a computer program, computer data, content data, or traffic data.

(m) Loss

Loss means any reasonable costs, including, but not limited to, the cost of responding to an offense under this Law, conducting an investigation or damage assessment, and/or the cost of analyzing, restoring, replacing, or reproducing computer data, content data, traffic data, a computer program, computer, computer system, or network to its condition prior to the offense, and/or other consequential damages incurred by an individual or entity arising from damage, interference, disruption, interception and/or the destruction of computer data, content data, traffic data, a computer program, computer, computer system, network, and/or other information.

(n) Malware

A program that is inserted into a computer program, computer, or computer system, usually covertly or without authorization, with the intent of compromising the confidentiality, integrity, or availability of the computer program, computer, computer system, network, computer data, content data, or traffic data or of otherwise disrupting the beneficial use thereof.

(o) Network

A group of computers or computer systems of whatever form, topology, or functionality that is connected at points (nodes) which have the capability to transmit, receive, share, or forward information, communication signals, and operational instructions.

(p) Service Provider

Service provider means:

> (i) any public or private entity that provides to users of its service the ability to communicate by means of a computer program, computer, computer system, or network, including the services that support the development or utilization of computer programs and/or the creation, storage, retrieval, processing, management, and deletion of computer data, traffic data, and content data; and/or
>
> (ii) any other entity that processes or stores computer data, content data, or traffic data on behalf of such service (as set forth in (i) of this paragraph) or users of such service.

(q) Subscriber Information

Subscriber information means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services, other than traffic data or content data, and by which can be established: (i) the type of communication service used, the technical provisions taken thereto, and the period of service; (ii) the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, as it is available on the basis of the service agreement or arrangement; and/or (iii) any information regarding the location of installed communications equipment as disclosed in the service agreement or arrangement.

(r) Traffic Data

Traffic data means any computer or other data relating to a communication by means of a computer program, computer, computer system, or network, generated by a computer program, computer, computer system, or network that formed a part in the chain of communication, indicating the communication’s origin, destination, route, format, intent, time, date, size, duration, or type of underlying service. Packet headers or pen register and trap/trace data are typical examples of traffic data.

Title 2: Substantive Provisions; Acts Against Computers, Computer Systems, Networks, Computer Data, Content Data, and Traffic Data

Section 2. Unauthorized Access to Computers, Computer Systems, and Networks

(a) Unauthorized Access to Computers, Computer Systems, and Networks

Whoever, without authorization or in excess of authorization or by infringement of security measures, intentionally accesses in whole or in part, (i) a computer, (ii) a computer system and/or connected system, or (iii) a network, with the intention of conducting any activity within the definition of “Access” in this Title and which is prohibited under this Law shall have committed a criminal offense punishable by a fine of [amount]______ and/or imprisonment for a period of ________.

(b) Unauthorized Access to Government Computers, Computer Systems, and Networks

Whoever commits unauthorized access pursuant to paragraph (a) of this Section to a computer, computer system and/or connected system, or network that is exclusively for the use of the Government of this country, or in the case which such is not exclusively for the use of the Government but is used by or on behalf of the Government of this country and such conduct is intended to affect that use or impact the operations of the Government of this country, a criminal offense shall have committed a criminal offense punishable by a fine of [amount]_______ and/or imprisonment for a period of _________.

(c) Unauthorized Access to Critical Infrastructure

Whoever commits unauthorized access pursuant to paragraph (a) of this Section to a computer, computer system and/or connected system, or network that is exclusively for the use of critical infrastructure operations, or in the case which such is not exclusively for the use of critical infrastructure operations but the computer, computer system and/or connected system, or network is used for critical infrastructure operations and such conduct is intended to affect that use or impact the operations of critical infrastructure, shall have committed a criminal offense punishable by a fine of [amount]_______ and/or imprisonment for a period of ________.

(d) Unauthorized Access for Purposes of Terrorism

Whoever commits unauthorized access pursuant to paragraph (a) of this Section and such conduct is with the intention of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to acts of cyberterrorism, shall have committed a criminal offense punishable by a fine of [amount]_______ and imprisonment for a period of ___________.

Section 3. Unauthorized Access to Computer Programs, Computer Data, Content Data, Traffic Data

(a) Unauthorized Access to Computer Program, Computer Data, Content Data, Traffic Data

Whoever, without authorization or in excess of authorization or by infringement of security measures, intentionally accesses in whole or in part, (i) a computer program, (ii) computer data, (iii) content data, or (iv) traffic data, with the intention of conducting any activity within the definition of “Access” in this Title and which is prohibited under this Law shall have committed a criminal offense punishable by a fine of [amount]_______ and/or imprisonment for a period of ______________.

(b) Unauthorized Access to Protected Government Computer Program or Data

Whoever commits unauthorized access pursuant to paragraph (a) of this Section to a computer program, computer data, content data, or traffic data that has been determined by the Government of this country, pursuant to law or decree, to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any other reason pertaining to national or economic security, a criminal offense shall have been committed, punishable by a fine of [amount]______ and imprisonment for a period of __________, irrespective of whether or not such program or data was communicated, delivered, or transmitted to any person not entitled to receive it or retained by the person who accessed it.

(c) Unauthorized Access to Government Computer Program or Data

Whoever commits unauthorized access pursuant to paragraph (a) of this Section to a computer program, computer data, content data, or traffic data that is used, processed, or stored by any ministry, agency, department, office, or entity of the Government of this country and such data or program is exclusively for the use of the Government of this country, or in the case in which such data or program is not exclusively for the use of the Government but it is used by or on behalf of the Government, and such conduct is intended to affect that use or impact the operations of the Government of this country, a criminal offense shall have been committed, punishable by a fine of [amount] _____ and/or imprisonment of _________.

(d) Unauthorized Access to or Acquisition of Critical Infrastructure Computer Program or Data

Whoever commits unauthorized access pursuant to paragraph (a) of this Section to a computer program, content data, computer data, or traffic data that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but the program or data is used in critical infrastructure operations and such conduct is intended to affect that use or impact the operations of critical infrastructure, a criminal offense shall have been committed, punishable by a fine of [amount]_______ and imprisonment of _______.

(e) Unauthorized Access to or Acquisition of Computer Program or Data of Financial Institution or Illegal Acts

Whoever commits unauthorized access and/or acquisition pursuant to paragraph (a) of this Section and such conduct is with the intention of (i) accessing or acquiring financial data of a financial institution, or (ii) facilitating, advancing, assisting, conspiring, or committing extortion, identity theft, or any other illegal act not covered by provisions within this Law, whether or not via a computer program, computer, computer system, or network, a criminal offense shall have been committed, punishable by a fine of [amount]_______ and/or imprisonment of ______________.

(f) Unauthorized Access to or Acquisition of Computer Program or Data for Purposes of Terrorism

Whoever commits unauthorized access and/or acquisition pursuant to paragraph (a) of this Section and such conduct is with the intention of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to acts of cyberterrorism, a criminal offense shall have been committed, punishable by a [amount]_______ fine and imprisonment for a period of ______________.

Section 4. Interference or Disruption

(a) Interference or Disruption of Computers, Computer Systems, Networks

Whoever, without authorization or in excess of authorization or by infringement of security measures, intentionally causes interference or disruption of a computer, computer system and/or connected systems, or networks shall have committed a criminal offense punishable by a fine of [amount]_______ and/or imprisonment for a period of __________.

(b) Interference or Disruption of Computer Program, Computer Data, Content Data, Traffic Data

Whoever, without authorization or in excess of authorization or by infringement of security measures, intentionally causes interference or disruption of a computer program, computer data, content data, or traffic data shall have committed a criminal offense punishable by a fine of [amount]_________ and/or imprisonment for a period of _____________.

(c) Interference or Disruption With Knowledge of or Intent to Cause Serious Harm or Threaten Public Safety

Whoever commits interference or disruption pursuant to paragraphs (a) or (b) of this Section with the intent to cause or with knowledge that such conduct could cause serious harm to life, limb, or property or threaten public health and/or safety, shall have committed a criminal offense punishable by a fine of [amount]________ and/or imprisonment for a period of ____________.

(d) Knowledge of or Intent to Cause Interference or Disruption of Government Computers, Systems, Networks, Data

Whoever commits interference or disruption pursuant to paragraphs (a) or (b) of this Section with the intent to cause or with knowledge that such conduct could cause interference and/or disruption of computers, computer systems and/or connected systems, networks, computer programs, computer data, content data, or traffic data used by the Government in furtherance of the administration of justice, national security, or national defense shall have committed a criminal offense punishable by a fine of [amount]_______ and imprisonment for a period of ______________.

(e) Knowledge of or Intent to Cause Interference or Disruption of Critical Infrastructure

Whoever commits interference or disruption pursuant to paragraphs (a) and (b) of this Section with the intent to cause or with knowledge that such conduct could cause interference and/or disruption of the computers, computer systems and/or connected systems, networks, computer programs, computer data, content data, or traffic data used by critical infrastructure, shall have committed a criminal offense punishable by a fine of [amount]_________ and imprisonment for a period of ________________.

(f) Intent to Cause Interference or Disruption for Purposes of Terrorism

Whoever commits interference or disruption pursuant to paragraphs (a) and (b) of this Section with the intent of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to acts of cyberterrorism, shall have committed a criminal offense punishable by a fine of [amount]_______ and imprisonment for a period of ______________.

Section 5. Interception

Whoever intentionally and without authorization pursuant to the rules of criminal procedure and any other laws of this country, intercepts, by technical means, transmissions of non-public computer data, content data, or traffic data, including electromagnetic emissions or signals from a computer, computer system, or network carrying or emitting such, to or from a computer, computer system and/or connected system, or network shall have committed a criminal offense punishable by a fine of [amount]__________ and/or imprisonment for a period of ___________.

Section 6. Misuse and Malware

(a) Transmission of Malware and Misuse

Whoever intentionally and without authorization causes the transmission of a computer program, information, code, or command with the intent of causing damage to a network, computer, computer system and/or connected system, computer, computer program, content data, computer data, or traffic data shall have committed a criminal offense punishable by a fine of [amount]_________ and/or imprisonment for a period of ___________.

(b) Production, Sale, Procurement, Distribution of Computer or Computer Program for Access to Data and Misuse

Whoever intentionally and without authorization engages in the production, sale, or procurement for use, import, distribution, or otherwise makes available:

(i) a computer or computer program, designed or adapted primarily for the purpose of committing any of the offenses established in Sections 2 through 5; and/or

(ii) a computer password, access code, command, instruction, or similar data by which the whole or part of any computer, computer system, network, computer program, computer data, content data, or traffic data may be accessed, with the intent that it be used for the purpose of committing any of the offenses established in Sections 2 through 5;

shall have committed a criminal offense punishable by a fine of [amount]________ and/or imprisonment for a period of ____________.

(c) Possession of Computer or Computer Program for Access to Data or Misuse

Whoever is in possession of one or more items referenced in (i) and (ii) of paragraph (b) of this Section with the intent that they be used for the purpose of committing any of the offenses established in Sections 2 through 5 shall have committed a criminal offense punishable by a fine of [amount]________ and/or imprisonment for a period of ____________.

(d) No Penalty Without Intent to Commit Offense

Notwithstanding the foregoing, this Section shall not be interpreted to impose criminal liability where the production, sale, procurement for use, import, distribution, or otherwise making available or possession of the items referenced in (i) and (ii) of paragraph (b) of this Section is not for the purpose of committing any of the offenses established in Sections 2 through 5, such as for the authorized testing or protection of computer systems and data.

(e) Knowledge of or Intent to Cause Physical Injury

Whoever commits an offense under paragraphs (a) or (b) of this Section with the intent to cause or with the knowledge that such conduct could cause physical injury to any person shall be punished by a fine of [amount]___________ and/or imprisonment for a period of __________.

(f) Knowledge of or Intent to Cause Modification or Impairment of Medical Care

Whoever commits an offense under paragraphs (a) or (b) of this Section with the intent to cause or with the knowledge that such conduct could cause the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals shall be punished by a fine of [amount]___________ and/or imprisonment for a period of _____________.

(g) Knowledge or Intent to Cause Threat to Public Safety or Public Health

Whoever commits an offense under paragraph (a) of this Section with the intent to cause or with the knowledge that such conduct could cause a threat to public safety or public health shall be punished by a fine of [amount]___________ and/or imprisonment for a period of _____________.

(h) Intent to Furtherance of Terrorism

Whoever commits an offense under paragraph (a) of this Section with the intent of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to cyberterrorism, shall be punished by a fine of [amount]___________ and imprisonment for a period of _____________.

Section 7. Digital Forgery

Whoever intentionally and without authorization or legal right, engages in the input, acquisition, alteration, deletion, or suppression of a computer program, computer data, content data, or traffic data or otherwise alters the authenticity or integrity of such program or data, with the intent that it be considered or acted upon for legal purposes as though it were authentic or with integrity, regardless of whether or not the program or data is directly readable or intelligible, for any unlawful purpose, shall have committed a criminal offense punishable by a fine of [amount]______ and/or imprisonment for a period of ___________.

Section 8. Digital Fraud, Procure Economic Benefit

(a) Intent to Defraud

Whoever knowingly and with intent to defraud, transfers, or otherwise disposes of, to another, or obtains control of with the intent to transfer or dispose of a computer password, access code, or similar data by which the whole or part of any computer program, computer, computer system, network, computer data, content data, or traffic data may be accessed shall have committed a criminal offense punishable by a fine of [amount]______ and/or imprisonment for a period of ___________.

(b) Loss of Property to Procure Economic Benefit

Whoever intentionally and without authorization or legal right causes the loss of property to another person through:

(i) the input, acquisition, alteration, deletion, or suppression of a computer program, computer data, content data, or traffic data; or

(ii) the interference with the functioning of a computer, computer system and/or connected system, or network;

with the fraudulent or dishonest intent to procure an economic benefit for oneself or another shall have committed a criminal offense punishable by a fine of [amount] ________ and/or imprisonment for a period of ________.

Section 9. Extortion

(a) Acts With Intent to Extort

Whoever knowingly transmits any communication containing any threat to cause damage to a computer, computer system and/or connected system, network, computer program, computer data, content data, or traffic data with the intent to extort from any person any money or other thing of value shall have committed a criminal offense punishable by a fine of [amount]_________ and/or imprisonment for a period of ______________.

Section 10. Aiding, Abetting, and Attempting

(a) Whoever knowingly and intentionally aids or abets the commission of any of the offenses established in Sections 2 thorough 9 shall have committed a criminal offense punishable by a fine of [amount]_________ and imprisonment for a period of ________________.

(b) Whoever knowingly and intentionally attempts to commit any of the offenses established in Sections 2 thorough 9 shall have committed a criminal offense punishable by a fine of [amount]_________ and imprisonment for a period of ________________.

Section 11. Corporate Liability

(a) Acts Committed by Person in Leading Position

Any legal person (corporation, association, or other legal entity) may be subject to civil, criminal, or administrative penalties for any offense established in Sections 2 through 10 if:

(i) the offense was committed by a person holding a leading position in the legal person;

(ii) leading person acted

(A) on his/her authority to represent the legal person,

(B) on the authority vested in him/her to make decisions on behalf of the legal person, or

(C) his/her authority to exercise control within the legal person; and

(iii) the offense was committed for the benefit of the legal person.

(b) Acts Committed by Employee or Agent Through Negligence of Leading Person

Any legal person may be subject to civil, criminal, or administrative penalties for any offense established in Sections 2 through 10 if:

> (i) the offense was committed by an employee or agent of the legal person who was acting within the scope of his authority;
>
> (ii) the offense was committed for the benefit of the legal person; and
>
> (iii) the commission of the offense was made possible by the negligence of a leading person that resulted in the failure to supervise the employee or agent through appropriate and reasonable measures intended to prevent employees or agents from committing criminal activities on behalf of the legal person.

(c) Liability under paragraphs (a) and (b) of this Section shall be without prejudice to the criminal liability of the natural person who has committed the offense.

Title 3: Procedural Provisions for Criminal Investigations and Proceedings for Offenses within this Law

Section 12. Scope of Procedural Provisions

(a) The scope of the procedural provisions herein are for the purpose of specific criminal investigations or proceedings arising from offenses prohibited by Title 2 and the Substantive Provisions of this Law (Sections 2 through 10) and/or the laws of other jurisdictions that prohibit the same or similar actions. Except as provided otherwise in Section 5, pertaining to the interception of computer data, content data, or traffic data, these provisions apply to:

> (i) the criminal offenses established in Section 2 through 10 of this Law;
>
> (ii) other criminal offenses committed by means of a computer, computer system, or network; and
>
> (iii) the collection of evidence in electronic form relating to such offenses.

Section 13. Conditions and Safeguards

(a) Procedural Provisions

The procedural provisions set forth in Title 3 of this Law are subject to the conditions and safeguards provided elsewhere in the Laws of this country, including, but not limited to, judicial or other independent supervision, grounds justifying application, and limitation on the scope and duration of such power or procedure. These procedural provisions are also subject to the conditions and safeguards concerning human rights and liberties guaranteed under the laws of this country and international instruments, treaties, and laws, including the 1966 United Nations International Covenant on Civil and Political Rights.

(b) Principle of Proportionality

The procedural provisions set forth in Title 3 of this Law shall be conducted in compliance with the principal of proportionality, which shall be abided by in all criminal investigation activities performed by competent law enforcement bodies whenever evidence is to be gathered on and/or by means of electronic tools. Such criminal investigation activities include, but are not limited to, inspections, searches, seizure, custody, urgent inquiries, and searches for evidence. The impact of these procedural powers upon the rights, responsibilities, and legitimate interests of third parties alien to the facts investigated shall be considered when conducting such investigative activities.

Section 14. Preservation of Stored Computer Data, Content Data, Traffic Data

(a) The rules of criminal procedure for this country shall enable competent authorities to order or similarly obtain the expeditious preservation of specified computer data, content data, and/or traffic data that has been or may be stored by means of a computer or computer system, particularly when there are grounds to believe that such data is particularly vulnerable to loss or modification.

(b) Where an order is issued to a person to preserve specified computer data, content data, or traffic data in a person's possession or control, that person shall preserve and maintain the integrity of such data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities of this country or of another jurisdiction to seek its disclosure. The integrity of such preserved data shall be documented, including the method used to determining such integrity (such as the use of a mathematical algorithm and resulting hash), and such record maintained along with the preserved data. Competent authorities may request that the preservation order be renewed.

(c) The custodian and any other person ordered to preserve such data shall keep confidential all information regarding such order for the period of time specified by the order or required under the Laws of this country.

(d) The provisions of this Section are subject to the provisions of Sections 12 and 13 of this Law.

Section 15. Expedited Preservation and Partial Disclosure of Traffic Data

(a) The rules of criminal procedure for this country shall provide:

(i) for the expedited preservation of specified traffic data by a competent authority in this country, irrespective of whether one or more service providers are involved in the transmission of the subject communications; and

(ii) the disclosure to competent authorities, or a designate of such authority, of a sufficient amount of traffic data to enable the identification of the service providers and the path through which the communication was transmitted.

(b) The provisions of this Section are subject to the provisions of Sections 12 and 13 of this Law.

Section 16. Expedited Preservation of Computers or Storage Media

(a) The rules of criminal procedure for this country shall enable competent authorities to order or similarly obtain the expeditious preservation of specified computers or storage media in situations in which there is an investigative, forensic, or practical necessity to do so to protect and preserve the computing environment to enable the extraction and examination of data and computing instructions, particularly when there are grounds to believe that such data is particularly vulnerable to loss or modification or when the preserving entity lacks the requisite capability to safely and effectively preserve the computing and/or content data external to the computer or storage media.

(b) Where an order is issued to a person to preserve specified computers and/or storage media in the person's possession or control, that person shall preserve and maintain the integrity of such computers and/or storage media for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities of this country or of another jurisdiction to seek its disclosure. Competent authorities may request that the preservation order be renewed.

(c) The person and custodian ordered to preserve such computers and/or storage media shall keep confidential all information regarding such order for the period of time specified by the order.

(d) The provisions of this Section are subject to the provisions of Sections 12 and 13 of this Law.

Section 17. Production Order

The rules of criminal procedure for this country shall enable a competent authority to order:

(a) a person to submit specified computer data, content data, and/or traffic data in that person's possession or control, which is stored in a computer, computer system, or a computer data storage medium; and

(b) a service provider offering services in this country to submit specified subscriber information relating to such services that is in that service provider's possession or control.

(c) The provisions of this Section are subject to the provisions of Sections 12 and 13.

Section 18. Search and Seizure of Stored Data

(a) Search for Data

The rules of criminal procedure for this country shall enable competent authorities, upon adequate reason and within the scope of legal approval, to search or similarly access:

(i) a specified computer, computer system, computer program, or parts thereof, and/or the computer data, content data, and/or traffic data stored therein; and

(ii) a computer data storage medium on which computer data, content data, or traffic data may be stored in this country.

(b) Search in Connected Systems

When the authorities seeking approval to conduct a search pursuant to paragraph (a) of this Section have grounds to believe that the data sought is stored in another computer system, or part of another system in this country, which is owned by or under the control of the same entity for which the scope of legal approval was granted, and such data is lawfully accessible from or available to the initial system, the rules of criminal procedure shall enable the authorities to expeditiously extend the search or similar accessing to the other system.

(c) Seizure of Data

The rules of criminal procedure for this country shall enable competent authorities to seize or similarly secure computer data, content data, or traffic data accessed pursuant to paragraphs (a) and (b) of this Section, including the power to:

(i) seize or similarly secure a computer or computer system, or part of it, or a computer data storage medium;

(ii) make and retain an image or copy of the computer data, content data, or traffic data; (iii) maintain the integrity of the relevant stored data and document such integrity by means of a mathematical algorithm which shall be maintained along with the stored computer data; and

(iv) render inaccessible or remove those computer data in the accessed computer system.

(d) Protection of Data

The competent authorities in this country may order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs (a) and (b) of this Section.

(e) The provisions of this Section are subject to the provisions of Sections 12 and 13 of this Law.

Section 19. Interception (Real-Time Collection) of Traffic Data

(a) The competent authorities of this country may, upon adequate reason and within the scope of legal approval:

(i) collect or record traffic data in real-time through technical means;

(ii) compel a service provider, within its existing capability, to collect or record such traffic data in real-time or to cooperate and assist the competent authorities in the collection and recording of traffic data;

associated with the specified communications in this country transmitted by means of a computer system and/or network.

(b) Any service provider requested to collect and record such traffic data in real-time or to cooperate or assist with such shall keep confidential the fact of the request and any information related to it.

(c) The provisions of this Section are subject to the provisions of Sections 12 and 13 of this Law.

Section 20. Interception (Real-Time Collection) of Content Data

(a) The competent authorities of this country may, upon adequate reason and within the scope of legal approval, collect or record through technical means, or compel a service provider, within its existing technical capability, to collect or record or to cooperate and assist the competent authorities in the collection and recording of content data, in real-time, of specified communications transmitted by means of a computer system.

(b) Any service provider requested to collect and record such content data in real-time or to cooperate or assist with such shall keep confidential the fact of the request and any information related to it.

(c) The provisions of this Section are subject to the provisions of Sections 12 and 13 of this Law.

Title 4: Jurisdictional Provisions

Section 21. Jurisdiction

(a) Jurisdiction Over Persons and Domestic Acts

This country shall have jurisdiction over any person, irrespective of his nationality or citizenship, who commits any offense established pursuant to Sections 2 through 10 of this Law when the offense is committed (i) within the territory of this country; (ii) using equipment, software, or data located within this country, regardless of the location of the perpetrator, or (iii) directed against equipment, software, or data located in this country, regardless of the location of the perpetrator.

(b) Applicability to Acts on Ships and Aircrafts

This country shall have jurisdiction over offenses committed pursuant to Sections 2 through 10 of this Law if the offense was committed (i) on board a ship flying the flag of this country; or (ii) on board an aircraft registered under the Laws of this country.

(c) Applicability to Acts By Nationals Outside of Country

This country shall have jurisdiction over offenses committed pursuant to Sections 2 through 10 of this Law if the offense was committed by a citizen or resident of this country and (i) if the offense is punishable under criminal law where it was committed; or (ii) if the offense is committed outside the territorial jurisdiction of any country.

(d) Jurisdiction Where Extradition Refused

In instances where an alleged offender is present in this country and this country elects to refuse a request for extradition of the alleged offender to another country on the basis of his or her nationality, jurisdiction over the stated offences shall be established in this country.

(e) Concurrent Jurisdiction

When another country claims jurisdiction over an offense within Sections 2 through 10 of this Law, the officials of the countries involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for the prosecution of the offense.

(f) The Place Where the Offenses Occurred

An offense is committed at every place the perpetrator acted (i) via his or her physical presence;[17] (ii) via the intentional use of equipment, software, or data,[18] or (iii) at any location which the resulting action is an element of an offense pursuant to Sections 2 through 10 of this Law occurred or would have occurred according to the understanding of the perpetrator.[19]

(g) Reservation

In specific cases, this country may reserve the right to apply or not to apply the jurisdictional rules in paragraphs (b) and (c) of this Section.

Title 5: International Cooperation

Section 22. International Cooperation: General Principles

(a) The legal authorities of this country shall cooperate directly and to the widest extent possible with legal authorities of another country and/or with international organizations specializing in criminal matters for purposes of:

(i) investigations or proceedings concerning criminal offenses related to computer programs, computers, computer systems, networks, computer data, content data, and/or traffic data; and/or

(ii) the collection of evidence in electronic or any other form of a criminal offense. Such cooperation shall take place under the conditions of this Law and by observing:

(i) the obligations that this country has assumed under international legal instruments on cooperation in criminal matters that this country is party to;

(ii) arrangements agreed upon on the basis of uniform or reciprocal legislation in this regard; and

(iii) the Laws of this country.

(b) The cooperation, organized and carried out according to paragraph (a) of this Section, may pertain to, as appropriate:

(i) international legal assistance in criminal matters;

(ii) extradition;

(iii) the identification, blocking, seizing or confiscation of the evidence, products, and instruments of the criminal offence;

(iv) the carrying out of common investigations;

[17] This includes, for example, the place where the perpetrator physically typed the command on a computer.

[18] This would include, for example, the place where equipment or software intentionally used or attacked by the perpetrator is located, and thus would cover acts by foreign perpetrators located in another country but using attack servers or botnets located in another country.

[19] This would include locations where the perpetrator thought the attack or action would impact.

(v) the exchange of information;

(vi) technical assistance or assistance of any other nature for the collection of information;

(vii) specialized personnel training; and

(viii) other such activities deemed appropriate.

Section 23. Extradition Principles

(a) Application of Extradition Provisions

This Section applies to extradition between this country and another country, irrespective to whether there is an extradition treaty between this country and the requesting country, for the criminal offenses established pursuant to Sections 2 through 10 of this Law, provided that they are punishable under the laws of both countries and require deprivation of liberty for a maximum period of one year or longer.

(b) Exception to Application of Extradition Principles

Notwithstanding the foregoing, if the authorities of this country and another country agree on a different minimum penalty based upon uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between the countries, the minimum penalty provided for under such agreement or treaty shall apply.

(c) Offenses in this Law are Extraditable

The criminal offenses established pursuant to Sections 2 through 10 of this Law shall be deemed as extraditable offenses under any extradition treaty or agreement to which this country is a party and under all future treaties pertaining to extradition.

(d) Refusal of Extradition

If extradition for a criminal offense pursuant to Sections 2 through 10 of this Law is refused solely on the basis of the nationality of the person sought or because this country desires to have jurisdiction over the offense, the competent legal authorities of this country shall submit the case to the appropriate authorities in this country for the purpose of prosecution and shall report the outcome to the requesting country in due course.

Section 24. Mutual Assistance: General Principles

(a) Authority to Provide Mutual Assistance

The competent authorities of this country shall provide assistance to another country to the widest extent possible for the purpose of investigations or proceedings concerning the criminal offenses established pursuant to Sections 2 through 10 of this Law and for the collection of evidence in electronic or other form. The rules of criminal procedure shall be amended to the extent necessary to support this requirement, including the procedures pertaining to mutual assistance requests in the absence of applicable international agreements.

(b) Expedited Means of Communication

Requests for and responses to requests for expedited mutual assistance may be made to the authorities of this country via the most efficient means, including facsimile or electronic mail, provided that appropriate levels of authentication and security are utilized and formal confirmation follows the request or response. The competent officials of this country shall respond to such requests by any such expedited means of communication.

(c) Refusal to Cooperate

Mutual assistance shall be provided in accordance with this Law or other Laws of this country or by mutual assistance treaties to which this country is obligated, including the grounds on which cooperation may be refused. Such assistance shall not be refused with respect to offenses pursuant to Sections 2 through 10 solely on the grounds that the request concerns a fiscal offense.

(d) Dual Criminality

Where mutual assistance from this country requires the existence of dual criminality, that condition shall be deemed fulfilled by this Law, irrespective of whether the offense in this country is in the same category of offenses or within the same terminology as the requesting country's law, provided that the offense is a criminal offense under the laws of the requesting country.

Section 25. Unsolicited Information

(a) The legal authorities of this country may forward to another country information obtained within its own investigations when it considers that the disclosure of such information may (i) assist the other country in initiating or carrying out investigations or proceedings concerning criminal offenses similar to those established pursuant to Sections 2 through 10 of this Law, or (ii) might lead to further cooperation with that country. Prior to providing such information, the legal authorities of this country may subject the data to confidentiality requirements or other conditions, but shall not forward such information unless such requirements or conditions are accepted by the other country.

Section 26. Procedures for Mutual Assistance

(a) Application of this Section and Central Authority

The rules of criminal procedure for this country shall specify a central authority responsible for sending and answering requests for mutual assistance. Such central authority shall answer requests for mutual assistance, execute such requests, and or transmit requests to the appropriate authorities competent for their execution. Such central authority shall communicate with similar authorities in requesting countries.

If there is a mutual assistance treaty or reciprocal or uniform law between the requesting country and this country, the provisions of this Section may apply upon mutual agreement of this country and the requesting country. If there is no such mutual assistance treaty or reciprocal or uniform law, the provisions of this Section shall apply.

(b) Rules of Procedure for Mutual Assistance

Mutual assistance requests shall be handled according to the procedures of the requesting country unless they are incompatible with the rules of criminal procedure of this country, in which case the rules of this country shall take precedence.

(c) Refusal to Assist

The central authority responsible for sending and answering requests for mutual assistance may refuse to provide mutual assistance if:

(i) such request is against the laws of this country, except refusal shall not be allowed for offenses within Sections 2 through 10 of the Law on the grounds that they are considered a fiscal offense;

(ii) such request concerns an offense which the competent authorities of this country consider a political offense or an offense connected to a political offense; or

(iii) execution of the request is likely to prejudice the sovereignty of this country, its security, public order and safety, or other essential interests.

The central authority may postpone action on a mutual assistance request if such action would prejudice criminal or investigations or proceedings within this country, however, the central authority shall first consider whether the request may be partially granted or subjected to conditions.

(d) Inform of Outcome of Assistance

The rules of criminal procedure shall establish a process for the central authority to promptly inform the requesting country of the outcome of any requests for assistance, with reasons provided for postponement, refusal, or circumstances which would delay the assistance or render it impossible.

(e) Confidentiality of Request

The central authority shall (i) keep confidential the fact of the request and its subject, if so requested by the requesting country, except to the extent necessary to execute the request, or (ii) provide an explanation to the requesting country why such confidentiality is not possible to enable the requesting country to determine if the request should be nevertheless executed.

(f) Urgent Requests or Requests Not Involving Coercive Action

Urgent requests for mutual assistance or requests not involving coercive action may be sent:

> (i) directly by judicial authorities of the requesting country to the competent judicial authority of this country, with a copy of such request sent to the central authorities of both countries, understanding that the judicial authority of this country may, in its discretion, refer the matter to the central authority; or
>
> (ii) to the International Criminal Police Organization (Interpol), with a copy of such request sent to the central authority.

(g) Confidentiality of Information to be Provided

This country may supply the requested information upon the condition that it be kept confidential or that it shall not be used for investigations or proceedings other than those stated in the request. If the requesting country cannot comply with such conditions, the legal authorities in this country shall determine whether the requested information shall nevertheless be provided and the central authority shall communicate such decision to the requesting country. The competent authorities in this country supplying any such information shall require the receiving party to abide by any confidentiality requirements and to provide an explanation regarding the use made of the information provided.

Section 27. Expedited Preservation of Stored Computer Data, Content Data, or Traffic Data

(a) Request for Expedited Preservation

Within mutual assistance, the competent authorities of a country may request the expeditious preservation of specified computer data, content data, or traffic data located within the territory of this country, in respect of which the requesting country intends to submit a request for mutual assistance for the search or for access, seizure, or similar securing or disclosure of the data.

(b) Content of Request for Expedited Preservation

The request for expedited preservation referred to in paragraph (a) of this Section shall specify:

> (i) the authority requesting the preservation;
>
> (ii) the offense that is the subject of a criminal investigation or proceeding and a brief statement of the related facts;
>
> (iii) the stored computer data, content data, and/or traffic data to be preserved and its relationship to the offense;

(iv) any available information identifying the custodian of such stored data or the location of the computer or computer system(s) containing the data;

(v) the necessity of the preservation; and

(vi) that the requesting country intends to submit a request for mutual assistance for the search or for access, seizure, or similar securing or disclosure of the subject data.

(c) Measures to be Taken

Upon receipt of such a request, the competent authorities of this country shall take all appropriate measures to preserve expeditiously the specified data in accordance with the Laws of this country. Dual criminality shall not be required for such preservation.

(d) Refusal of Preservation

A request for preservation may only be refused if the request concerns an offense that this country considers a political offense or an offense connected with such, or this country determines that the execution of the request is likely to prejudice its sovereignty, security, public safety, or other essential interests.

(e) Where Preservation May Not Ensure Availability

Where the competent legal authorities believe that the requested preservation will not ensure the future availability of the data or will threaten the confidentiality or otherwise prejudice the other country's investigation, the legal authorities shall promptly inform the requesting country, which may then determine if the preservation should nevertheless be executed.

(f) Duration of Preservation

No preservation effected under this Section shall be for a period of less than sixty (60) days to enable the requesting country to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such request, the data shall continue to be preserved pending a decision on the request.

Section 28. Expedited Disclosure of Preserved Content Data, Computer Data, or Traffic Data

(a) If, in executing a request for preservation according to Section 27 of this Law, the legal authorities of this country discover that a service provider in another country was involved in the transmission of the communication, the legal authorities shall promptly disclose to the requesting country a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

(b) Disclosure of traffic data, as prescribed by paragraph (a) of this Section, may only be withheld from the requesting country if:

(i) the request concerns an offense that this country considers a political offense or an offense connected with such an offense; or

(ii) the legal authorities of this country consider that the execution of the request is likely to prejudice its sovereignty, security, public safety, or other essential interests.

Section 29. Mutual Assistance Regarding Access to Stored Computer Data, Content Data, or Traffic Data

(a) The competent officials of another country may request the competent officials of this country to search or similarly access, seize or similarly secure, and disclose specified data stored by means of a computer or computer system located within the territory of this country, including data that has been preserved pursuant to

Section 27 of this Law. Such requests shall adhere to the principles pertaining to international cooperation in Section 22 of this Law and shall comply with other relevant provisions of this Law.

(b) Requests pursuant to paragraph (a) of this Section shall be responded to on an expedited basis where (i) there are grounds to believe that the requested data is particularly vulnerable to loss or modification; or (ii) expedited cooperation is provided according the instruments, arrangements, and laws referred to in Section 22 of this Law.

Section 30. Trans-Border Access to Stored Computer Data, Content Data, or Traffic Data

(a) A competent authority may access publicly available (open source) stored computer data, content data, or traffic data regardless of where the data is located geographically.

(b) A competent authority from another country may, without authorization of authorities of this country, have access to and receive, by means of a computer or computer system located on its territory, specified computer data, content data, or traffic data stored in this country if the competent authority from the other country obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to such competent authority through that computer or computer system.

Section 31. Mutual Assistance In Real-Time Collection of Traffic Data

(a) The competent authorities of this country shall provide mutual assistance to the competent authorities of another country with respect to the real-time collection of specified traffic data associated with specified communications in the territory of this country that were transmitted by means of a computer or computer system. Subject to the provisions of paragraph (b) of this Section, this assistance shall be governed by the Laws and rules of criminal procedure for this country.

(b) The competent authorities of this country shall provide assistance pursuant to paragraph (a) of this Section for criminal cases in a manner equal to that which would be available in a similar domestic case.

Section 32. Mutual Assistance Regarding Interception of Content Data or Computer Data

The competent authorities of this country shall provide mutual assistance to the competent authorities of another country in the real-time collection or recording of specified computer data or content data of specified communications transmitted by means of a computer or computer system to the extent permitted under the Laws of this country and treaties to which this country is bound.

Section 33. 24/7 Points of Contact

(a) The competent authorities of this country shall designate points of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offenses related to computers, computer systems, networks, computer data, content data, and/or traffic data, or for the collection of other evidence in electronic form related to a criminal offense. Such assistance shall include facilitating, or if permitted under the Laws of this country and the practices of competent authorities, directly carrying out the following measures:

(i) the provision of technical advice;

(ii) the preservation of data pursuant to Sections 27 and 28; and

(iii) the collection of evidence, the provision of legal information, and locating of suspects.

(b) The points of contact shall have the capacity to carry out communications with the points of contact in other countries on an expedited basis. If the designated points of contact are not responsible for international cooperation and mutual assistance or extradition, the points of contact shall ensure that they are able to coordinate with such authorities on an expedited basis.

(c) The competent authorities of this country shall ensure that all points of contact are properly trained and equipped or that other trained personnel are available to the points of contact to facilitate the operation of the network and compliance with the provisions of this Law.

Title 6: Provisions Applicable to Other Offenses

Section 34. Provisions That Apply to Other Offenses

The competent authorities of this country may, upon adequate reason and within the scope of legal approval and the Laws of this country and/or any legal obligations that this country may be subject to through (a) the Bern Convention for the Protection of Literary and Artistic Works, (b) the Agreement on Trade-Related Aspects of Intellectual Property Rights, (c) the WIPO Copyright Treaty, (d) the International Convention for the Protection of Performers, Producers, Phonograms, and Broadcasting Organization, (e) the WIPO Performance and Phonograms Treaty, and/or (e) any international agreements or treaties pertaining to child pornography may exercise the authority granted in Sections 12-32 of this Law to investigate or assist in the investigation of offenses related to such Laws or legal obligations. The provisions of this Section are subject to the Provisions of Sections 12 and 13 of this Law.

4. Explanatory Comments to Sample Legislative Language

Explanatory Comments provide clarification regarding certain aspects of the Sample Legislative Language. They are not intended to provide a lengthy explanation of the various provisions within the Sample Language.

4.1. Definitions

The definitions in the Sample Language were derived from a review and analysis of similar definitions in various cybercrime laws, including those of Australia, Canada, Council of Europe, U.K., and U.S. (federal and state laws of California, New York, Arkansas). The definitions offered in the Sample Language are consistent with the definitions used and the intent behind similar terms in the cybercrime laws of developed nations and the Council of Europe Convention on Cybercrime (CoE Convention).

The Sample Language contains definitions that were not included in the CoE Convention and which may not be present in cybercrime laws of developed nations, but they are based the commonly understood definition as they pertain to currently known threats.

Definition of Access and Use of Terms "Without Authorization" and "Intent"

Article 2 of the Council of Europe Convention on Cybercrime obligates Parties to establish as a criminal offense the intentional "access to the whole or any part of a computer system without right" The text notes that the offense may be further limited by inclusion of the additional elements of breaching a security system to effect access or effecting such unauthorized access with the intent of obtaining computer data or "other dishonest intent."

Paragraphs 44-50 of the Explanatory Report to the COE Convention discuss the offense to be created under Article 2, and the definition of "access" in some detail. The commentary makes clear that the drafters wished to leave to states the option to criminalize "mere" unauthorized access (hacking) or to limit criminalization to situations where an unauthorized access occurs by circumventing a security system, with intent to commit a wrongful act, or by accessing a specific type of computer system. The term "without authorization" may be deemed to include conduct undertaken without permission or authority (legislative, executive, administrative, judicial, contractual, or consensual) or conduct that is not covered by a legal defense or allowable under domestic law (such as exceptions for approved testing of a computer system).

The *ITU Toolkit* proposes two separate offenses of unauthorized access, each of which takes advantage of the additional elements suggested by the COE text and commentary. Section 2 (a) criminalizes the intentional access to computers, computer systems and networks, either without or in excess of authorization, or by infringing security measures, when the actor has the *intent* to commit any activity prohibited under the Sample Language. Similarly, Section 3(a) criminalizes the intentional access to programs, computer data, content data, or traffic data either without or in excess of authorization, or by infringement of a security measures, if the actor has the requisite intention. A person acts "intentionally" or "with intent" when his/her conscious objective is to cause a certain result.

In comparing the definition of "access" in the *ITU Toolkit* and the definition of "access" in paragraph 46 of the COE Explanatory Report, it is to be noted that, in describing "access" the COE commentary says "… it does not include the mere sending of an e-mail or file to that system." On the other hand, the *Toolkit* definition of "access" in Section 1(a) includes the term "communicate with."

The potential discrepancy is resolved by realizing that it is not "mere" access which is to be criminalized by Sections 2 and 3 of the *ITU Toolkit*, but only access which is unauthorized or infringes security measures, and which is done for a wrongful purpose. Thus, merely sending an e-mail or a file to a computer or computer system would not be a criminal act under either under Article 2 of the Cybercrime Convention or under Sections 2 and 3 of the *ITU Toolkit* absent the other elements of the offense. This is clarified by the insertion of the terms "without authorization or in excess of authorization or by infringement" prior to the words "intentionally accesses" and by the words "with the intention of" and "such conduct is intended to" with respect to conducting a prohibited activity. The requirement of intent ("intentionally accesses") in paragraph (a) of Sections 2 and 3 is carried forward to other paragraphs in each Section through the words "commits unauthorized access" pursuant to paragraph (a) of this Section.

Definition of Computer

The definition of computer is based upon U.S. law and the court decisions interpreting the definition. In *GWR Medical, Inc. v. Baez,* 2008 U.S. Dist. LEXIS 19629, the court determined that a CD-ROM was not a computer because:

> [A] CD-ROM does not, in and of itself, process information. The CD-ROM is analogous to a compilation of documents and training materials, and cannot be considered a computer under the CFAA [Computer Fraud and Abuse Act] without processing capabilities.[20]

In *United States v. Mitra,* 405 F.3d 492, the court determined that a computer-based radio system that spread traffic across twenty frequencies and the radio units used the control channel to initiate a conversation with others on the network, was a computer. The prosecution argued that the radio trunking system was a computer because it contained a chip that performed high-speed processing in response to signals received on the control channel. The defendant, Mr. Mitra, claimed that even if the radio system contained a computer, that every cell

[20] *GWR Medical, Inc. v. Baez,* 2008 U.S. Dist. LEXIS 19629.

phone, cell tower, iPod, and wireless baseless station would also be swept within the CFAA, and Congress surely did not intend the law to be so encompassing when it passed the law in 1984. The court, however, disagreed with this line of thinking, pointing out that legislators know that technology changes rapidly and in ways beyond the imagination of the legislators, thus "they write general statutes rather than enacting a list of particular forbidden acts."[21] The court determined that the radio system was a computer for purposes of the CFAA.

Definition of Computer Data

The definition of computer data includes the word "state" because digital 1s or 0s can be a value whose existence or lack of existence has external significance, such as on or off, present, absent, set, unset, etc.

Definition of Critical Infrastructure

The definition for critical infrastructure is, in large part, taken from U.S. law.[22]

Definition of Disruption and Interference and Discussion of Actions

The use of the term "disruption" is used in the context of rendering a computer, system, network, or computer program (or some component of these) to be inoperable or out of service or operating in an adverse manner for a period of time. A Distributed Denial of Service (DDoS)attack is one example of a *disruption* that is caused by *interference* with a network, computer, computer system, and computer program. This can be caused by an "interference," which is directed at the action and consequence of an event. Actions include imputing, transmitting, damaging, deleting, destroying, deteriorating, altering, suppressing, and corrupting. Consequences of these actions include hindering, blocking, impeding, interrupting, or impairing the actual processing or functioning of a computer, computer system, network, computer program, computer data, content data, or traffic data.

The actions are not specifically defined because the context of these terms can change with the evolution of new technologies and/or threats. Some guidance with respect to the definitions is offered, however, to assist in comprehending the sample language.

- "Altering" may refer to changing, modifying, or adjusting a digital asset.
- "Corrupting" may refer changing data, including computer programs, in storage or transit such that it is unrecognizable or useless or causes unintended actions to be taken by computer systems and programs.
- "Damaging" and "deteriorating" may refer to the negative alteration of the integrity, availability, or confidentiality of any of the named digital assets (network, computer system, computer, computer program, computer data, content data, and traffic data).
- "Deleting" may refer to the erasure of a corporeal thing; the act removes it or makes it unrecognizable.
- "Destroying" may refer to the destruction of a corporeal thing, rendering it unusable.
- "Deteriorating" may refer to the diminishment of the digital asset in some way that renders it less usable or viable than before the action occurred.
- "Inputting" may refer to the insertion or addition of data or instructions into a computer system, computer, or network.

[21] *United States v. Mitra,* 405 f.3d 492.

[22] Homeland Security Act of 2002, Section 2, http://www.whitehouse.gov/deptofhomeland/analysis/; *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (USA PATRIOT Act of 2001), Pub. Law 107-56, Section 1016(e), 42 U.S.C. Section 5195c(e), http://www.dhs.gov/xabout/laws/law_regulation_rule_0011.shtm.

- "Imputing" may refer to the attachment or reflection of responsibility for an act onto another, such as spoofing an email address.
- "Suppressing" may refer to any action that prevents or delays something, such as the availability of data, access to a network or computer, delaying the flow of information through a network, etc.
- "Transmitting" may refer to conveying, causing to spread, sending, or spreading from one point to another, from one device to another, or to multiple places or devices. It can mean to send a signal or data from one place to another.

Definition of Transmission

The definition of transmission is intended to include the installation of a program, code, or other software on a computer or device, irrespective of whether it has been uploaded, downloaded, or copied from a disk or other medium onto the computer or device.

4.2. Substantive Provisions

Terrorism and Acts Against Critical Infrastructure

The substantive provisions in the Sample Language are harmonized with the language and intent of cybercrime laws in most developed nations and the CoE Convention. The provisions go beyond these laws in that they set forth sample provisions for cybercrimes against (a) critical infrastructure; and (b) cybercrimes that are committed with the intent of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to acts of cyberterrorism.

Following U.S. law, there are provisions for cybercrimes against government data and government computers, computer systems and/or connected systems, and networks. There are additional provisions with respect to illegal access to data that has been determined by a government to require protection for reasons pertaining to national or economic security, with reason to believe that such information could be used to injure the country or could be used to the advantage of another country. Cybercrimes involving certain government systems and data, critical infrastructure, and for purposes of terrorism were deemed to be such a threat to the rule of law, public safety, and national and economic security that the *Toolkit* Project Team believed separate provisions should address these crimes and more substantial penalties should apply.

Fraud, Extortion, Other Illegal Acts

Recognizing the increased rise in fraud, identity theft, forgery, and extortion through the use of computers and digital data, provisions addressing these illegal acts are included in the Sample Language. They are consistent with developed country cybercrime laws and the CoE Convention. The use of information and communication technologies (ICTs) to aid and abet crimes is also covered in the Sample Language in a harmonious manner.

Child Pornography and Intellectual Property

The two areas covered by the CoE Convention that are not covered in the Sample Language involve provisions related to child pornography and the infringement of intellectual property (copyrights and related rights). The Project Team believes child pornography is a heinous crime that should be criminalized in every jurisdiction. Although computers, networks, and related technology are used in the production, marketing, distribution, sale, and availability of child pornography, these activities are also undertaken by traditional methods that are beyond the reach of cybercrime laws. Since there is a well-established body of international law regarding copyright and other intellectual property rights and infringement can occur by digital or traditional means, the Project

Team believed that issues involving intellectual property are more appropriately addressed through the legal instruments, treaties, and organizations that have historically dealt with these issues.

There is a well-accepted principle that, to the greatest extent possible, laws should be technology neutral, thus drafting provisions that only applies to cyber technology violates this principle. Therefore, the Project Team was concerned that a provision in the Sample Language related to child pornography and copyright protection might leave the more traditional means of committing these crimes uncovered in some jurisdictions. The Project Team urges every jurisdiction to enact strong criminal laws against child pornography and intellectual property infringement that address all aspects of these crimes, irrespective of whether these illegal acts are committed by cyber or traditional means.

The Project Team took into account the significant amount of electronic data pertaining to these offenses and struck a balance between the CoE Convention and cybercrime laws in developed nations by including in the *Toolkit* a separate provision (Title 6, Section 34) extending the procedural, international cooperation, and mutual assistance provisions to child pornography and intellectual property offenses to assist in the investigation and prosecution of offenders.

Section 5. Interceptions of Non-Public Transmissions

Section 5 applies to interceptions of "transmissions of computer data, content data, or traffic data." This section is intended to apply to *all* communications and transmissions over networks and/or computer systems. It includes transmissions by private providers, such as organizations and universities, as well as electronic communications service providers "to the public," such as Internet Service Providers and cable, satellite, and telephony providers who service the public at large. The Payment Card Industry Standard ("PCI") defines a public network as a network that is established and operated by a telecommunications provider or recognized private company, for the specific purpose of providing data transmission services "to the public."[23]

In the United States, employees have very little right to privacy in the workplace, except personal communications are generally protected under the Electronic Communications Privacy Act. Europe affords more privacy protections in the workplace. In the United States and some other countries, private sector entities sometimes intercept conversations on their own networks for training, quality control, or other purposes, based upon employee consent that the employer may intercept communications over business networks. Consent is usually provided in the form of an employee signature of acceptance of corporate policy, acknowledgement of corporate banners on computer screens, or online acceptance clicks. Such interceptions of voice conversations are allowed in the United States so long as the conversation is not personal in nature, in which case courts have held that the interception must cease the moment the interceptor realizes the conversation is personal. Section 5 is not intended to sweep in communications that are openly available to the public, such as ham radio transmissions, etc.

Section 6. Misuse and Malware

The usage of the term "computer program" in this provision is intended to refer to malware designed to alter or destroy data, interfere with the operation of a computer, computer system, or network, or cause any number of unauthorized actions. The definition of computer includes the word "device" or "grouping of such devices." The term "distribution" refers to the act of forwarding, sending, transmitting, dispersing, spreading , or diffusing such malware to other networks, computer systems, computers, or computer programs. It also is intended to include the use of hyperlinks that facilitate misuse.

[23] PCI Security Standards Council, "Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms," https://www.pcisecuritystandards.org/security_standards/glossary.shtml.

Section 7. Digital Forgery

The usage of the term “without authorization or legal right” is consistent with its use elsewhere in the Sample Language. The term “without authorization” may be deemed to include conduct undertaken without permission or authority (legislative, executive, administrative, judicial, contractual, or consensual) or conduct that is not covered by a legal defense or allowable under domestic law (such as exceptions for approved testing of a computer system).

Section 10. Aiding, Abetting, and Attempting

The usage of the term “knowingly” is used in this provision to ensure that the person acts “knowingly” or with knowledge that his/her conduct is reasonably certain to aid, abet, or attempt to cause a particular crime to be committed. A person acts “intentionally” when his/her conscious objective is to cause such a result.

Section 11. Corporate Liability

The term “leading person” is intended to encompass senior-level personnel in leadership positions, such as officers, directors, and senior executives. The interpretation of “leading person” is not intended to be limited to the chairman, chief executive officer, or senior managing director.

Penalties

All penalties related to cybercrimes in the Sample Language are criminal, except for corporate liability, which, consistent with the CoE Convention, may be administrative, civil, or criminal. Under the Sample Language, penalties for cybercrimes may be monetary fines and/or imprisonment, except for acts of cyberterrorism or acts against critical infrastructure or certain government systems or data, which require both a fine and imprisonment. The CoE Convention requires imprisonment for all cybercrimes, but even the U.S., which has ratified the CoE Convention, has penalties of fines and/or imprisonment.

In addition, the Project Team encourages every country to provide remedies for victims within their legal frameworks for cybercrimes covered pursuant to Sections 2 through 10. Such remedies could include the return of funds and/or property to rightful owners and procedures to seize funds and property from convicted persons. Countries may also want to consider denying Internet access to persons with more than one conviction under their cybercrime laws.

4.3. Provisions Related to Procedural Aspects, Jurisdiction, International Cooperation & Mutual Assistance

The areas that are most problematic with respect to combating cybercrime are the procedural aspects, jurisdictional barriers, gaps in international cooperation, and mutual assistance. This does not in any way intend to trivialize substantive cybercrime provisions; indeed, a harmonized global legal framework with respect to all aspects cybercrimes is critically important. The greatest gaps that make it so difficult to deter, detect, respond to, investigate and prosecute cybercrimes, however, are in areas related to procedural provisions, jurisdiction, international cooperation, and mutual assistance. These are the areas where minutes matter and differences in interpretation can be costly. Thus, similar wording in these provisions helps eliminate confusion or varying interpretations and promotes the end goal. Although countries may vary in how they draft their cybercrime laws, the Project Team encourages them to stay within the intent of the Sample Language and to try to use consistent language.

Since harmonization of procedural laws are critical to effective cyber criminal investigations and prosecution, the provisions in the Sample Language that pertain to procedural, jurisdiction, and international cooperation track fairly closely the provisions in the CoE Convention, although there are deviations to reflect variations in the laws of developed countries and the current threat environment. Many of the provisions in the Sample Language are simplified from those in the CoE Convention, even though they may contain similar phrases.

Section 13. Conditions and Safeguards

In criminal law, the proportionality principle is "the punishment of the offender should fit the crime." In the CoE Convention, however, it restrains actions to only those necessary to achieve the government's objectives. In practice, the proportionality principle restrains jurisdictions from using cybercrime laws to elevate the crimes enumerated in their laws from misdemeanors to felonies, or vice-versa. For example, a hacker, who is an American citizen operating out of his home office, steals the identities of Belgian citizens from their home computers in Brussels. He could be charged in America under its cybercrime law, the Computer Fraud and Abuse Act. If the jurisdictions were reversed and the hacker was the Belgian and Americans were the victims, the Belgian statute may only allow prosecution of the defendant as a misdemeanor. Thus, a two-year jail sentence issued by an American court and a six-month jail sentence issued by a Belgian court would not violate the proportionality principle, because the intent of the model cybercrime statute was satisfied by the respective jurisdictions only to the extent necessary to carry out the respective governments' objectives.

As it pertains to the Sample Language, the proportionality principle protects the sovereignty of nations to determine what punishment applies to crimes, respectively, while executing the intent of the cybercrime laws.[24]

Sections 14. Preservation of Data

The aim of this Section is to provide countries with measures to be taken at the domestic level to enable preserve electronic data relevant to the investigation of or attempts to establish any criminal offense, not just cybercrimes. The terminology “order or similarly obtain” is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or administrative order or directive. Data preservation keeps the stored data’s integrity intact and the data secure in stored form and protected from anything that would cause its current quality and availability to change or deteriorate. It is intended that the preservation of electronic data (which can include computer data, content data, and/or traffic data) be conducted in compliance with the European Telecommunications Standards Institute (ETSI) Technical Standard (TS) 102 656, Lawful Interception (LI): Retained Data.

Sections 15 and 16. Expedited Preservation

There are often several service providers involved in the communication process. This section is intended to affect all service providers within the jurisdiction of this country that was involved in processing and/or transmitting the communications to be preserved. This Section intends that communications providers (irrespective of whether Internet Service Providers, telephony, cable, or satellite) disclose to authorities a

[24] *See* Christopher Kuner, “Proportionality in European Data Protection Law And Its Importance for Data Processing by Companies,” *Privacy & Security Law Report,* Vol. 7, No. 44, Nov. 10 2008, 1615-19.

sufficient amount of traffic data to enable the competent authority to identify other providers and the path through which the communication was transmitted. The aim is to trace the origins of the communication.

Section 17. Production Order

The term "possession or control" mean the physical possession of the data concerned in the ordering country and situations in which the data to be produced is not in the physical possession of the person or service provider but they can order the production of the data.

The term "subscriber information" means any computer data or other form of data (but not traffic data or content data) that is held by a service provider and relates to subscribers of its services and by which can be established (a) the type of communication service used, the technical provisions taken thereto and the period of service, (b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement, or (c) any other type of information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Section 18. Search and Seizure of Stored Data and Use of Term "Upon Adequate Reason"

This section uses the terminology "upon adequate reason and within the scope of legal approval" as a means of indicating that the search and seizure should only be allowed if legal thresholds are met, such as grounds to believe the search and seizure is warranted (e.g., probable cause), and the requisite legal approvals have been obtained. Section 18(c)(ii) refers to making images or copies of computer data, content data, or traffic data. For clarification, an "image" is a duplicate of an entire storage media whereas a copy is a duplication of the data or some subset of it. More detailed guidance regarding best practices in imaging and copying data are noted in the Useful Reference Materials section of this document, especially on point are those from the Scientific Working Group on Digital Evidence and the United States Secret Service pertaining to best practices in computer forensics and search and seizure of digital evidence.

The search and seizure (S/S) of stored data cannot proceed in the same manner as the search and seizure of a tangible object. In the traditional environment, a search for a tangible object involves:

- The investigator searching or inspecting a place or area; and
- The investigator physically seizing and taking away the tangible object.
- The precondition for obtaining legal authority for the search is the existence of grounds to believe that such tangible object exists in a specific location and will afford evidence of a specific criminal offense.

In the electronic environment, the gathering of data occurs during the period of the search and with respect to data existing at that time. There are two main ways of conducting an investigation: accessing and searching data which is contained within a computer system or part of it (such as a connected storage device) or on an independent storage medium (such as a CD-ROM, memory stick, etc.)

Sections 19 and 20. Interception of Traffic Data and Content Data[25]

[25] The following material is from: Jody R. Westby, ed., *International Guide to Combating Cybercrime*, American Bar Association, Privacy & Computer Crime Committee, Section of Science & Technology Law, ABA Publishing, 2003, http://www.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450030 (this publication is available at no cost to people in developing countries by sending an email to Jody Westby at westby@mindspring.com); *see* additional material in this reference for more specific information based upon various jurisdictions.

It is intended that the interception of traffic data and content data be conducted in compliance with ETSI TS 101 331, Lawful Interception (LI): Requirements of Law Enforcement Agencies.

Given the grave privacy intrusion that live interception represents, strict legal standards usually apply to its authorization. Based upon developing national and international standards, it is possible to identify certain common elements that should govern any legal system for live interception:[26]

- Approval should be obtained from an independent official (preferably a judge), based on a written application and manifested in written order.
- Approval should be granted only upon a strong factual showing of reason to believe that the target of the search is engaged in criminal conduct and that the technique is especially needed (that is, interception is reserved for serious offenses and used only when other less intrusive techniques will not suffice).
- Each surveillance order should cover only specifically designated persons or accounts – generalized monitoring should not be permitted.
- The rules should be technology neutral – all one-to-one communications are treated the same, whether they involve voice, fax, images or data, wire line or wireless, digital or analog.[27]
- The scope and duration of the interception is limited, and in no event does the surveillance extend longer than is necessary to obtain the needed evidence.
- In criminal investigations, all those who have been the subject of an interception should be notified after the investigation concludes, whether or not charges result.
- Personal redress or suppression of evidence at trial is provided for violations of the privacy standards.[28]
- Due to the higher privacy interest associated with content data, the investigative measures shall be restricted to a range of serious offenses to be determined by domestic law.

Section 21. Jurisdiction

This Section applies the territoriality principle, giving a country the right to exercise jurisdiction over crimes committed within its borders. According to the ubiquity doctrine, a country can claim jurisdiction over offenses for which the preparatory or initial acts of the offense were committed within its territory, even if the offense was completed outside the country. The effects doctrine allows the country to claim jurisdiction over offenses based on the effect that the offense has on the country (this includes aiding and abetting). The flag principle extends the territorial principle to ships and aircraft flying under the flag of the country.

Section 30. Trans-Border Access to Stored Computer Data, Content Data, or Traffic Data

“Publicly available” refers to data open to the public user, including that obtain through Web sites without access controls or permission required. Such consent is a critical component of this provision. A private party may give data to another party (public or private) without government permission, unless the country of the

[26] These standards may be subject to certain exceptions for consensual searches, serious emergencies, and exigent circumstances on a case-by-case basis.

[27] Under U.S. law, a limited exception exists in 18 U.S.C. Section 2516 which allows the government to intercept voice communications only for certain enumerated felonies, while allowing the interception of electronic communications for any federal felony.

[28] U.S. law allows for both personal redress against individuals who violate the privacy standards and the suppression of evidence in legal proceedings.

disclosing party expressly requires government permission be obtained. If a party needs electronic material that is being processed, stored, or transferred by a computer system located within the territory of another country and does not have the consent of the owner of the system and data, the requesting party should apply the procedures of mutual assistance.

The intent of this provision is to allow consenting parties to provide requested data. It is not intended to circumvent sovereign rights or to allow self-help to data within the borders of another sovereign state unless the data is either openly accessible to anyone or the disclosing party consents to providing the data. In cases of uncertainty, requests should be processed through official channels. The authors of the Toolkit believe there should be additional multilateral discussions on this issue to enable broader clarification and certainty on trans-border access to data.

Section 33. 24/7 Points of Contact

The "24/7 Point of Contact" has two main functions: (1) to speed up the communication process by providing a knowledgeable point of contact, and (2) to speed up the investigations by authorizing the contact point to carry out certain investigative actions immediately, such as the preservation of data, collection of evidence, and location of suspects. If the point of contact does not have the power to order data preservation, it is important that the contact point has the ability to immediately contact the competent authority.

5. ITU Toolkit for Cybercrime Legislation – Country Work Sheet

The following table lists provisions of the sample legislative language in the ITU Toolkit for Cybercrime Legislation. Review your country's cybercrime law(s), both substantive and procedural, and indicate whether a corresponding provision exists in your law(s) and, if so, record the citation for the provision. The Explanatory Comments in the Toolkit will provide helpful guidance.

Next, compare the language of the identified provisions in your law(s) with the sample language in the Toolkit. There are columns on the Worksheet to indicate whether the provision is consistent with or similar to (harmonized) with the Toolkit's sample language, or whether it needs to be amended or deleted from existing language, or whether the provision needs to be added to existing law. Record the reason for the marked action or other notes in the Comments column. It is important that terminology be as consistent as possible across countries' laws. Therefore, if the terminology in your country's law should be updated to be consistent with that used in the sample language and to help advance a harmonized legal framework, mark the provision as needing to be amended and note the change in the comments column.

Provision in sample language	**In local law?**	**Citation of provision**	**Consistent with Toolkit?**	**Needs to be amended?**	**Needs to be deleted?**	**Needs to be added?**	**Comments (reason for amendment or deletion)**
Preamble							
Definitions							
a. Access							
b. Computer							
c. Computer Data							
d. Computer Program							
e. Computer System							
f. Content Data							
g. Critical Infrastructure							
h. Cyberspace							

Provision in sample language	**In local law?**	**Citation of provision**	**Consistent with Toolkit?**	**Needs to be amended?**	**Needs to be deleted?**	**Needs to be added?**	**Comments (reason for amendment or deletion)**
i. Damage							
j. Disruption							
k. Interception							
l. Interference							
m. Loss							
n. Malware							
o. Network							
p. Service Provider							
q. Subscriber Information							
r. Traffic Data							
SUBSTANTIVE PROVISIONS							
2. Unauthorized Access to Computers, Computer Systems, and Networks							
a. Unauthorized Access to Computers, Computer Systems, and Networks							
b. Unauthorized Access to Gov’t Computers, Computer Systems							

Provision in sample language	**In local law?**	**Citation of provision**	**Consistent with Toolkit?**	**Needs to be amended?**	**Needs to be deleted?**	**Needs to be added?**	**Comments (reason for amendment or deletion)**
and Networks							
c. Unauthorized Access to Critical Infrastructure							
d. Unauthorized Access for Purposes of Terrorism							
3. Unauthorized Access to Computer Program, Computer Data, Content Data, Traffic Data							
a. Unauthorized Access of Computer Program, Computer Data, Content Data, Traffic Data							
b. Unauthorized Access to Protected Government Computer Program or Data							
c. Unauthorized Access to Government Computer Program or Data							
d. Unauthorized Access to Critical Infrastructure Program or Data							

Provision in sample language	**In local law?**	**Citation of provision**	**Consistent with Toolkit?**	**Needs to be amended?**	**Needs to be deleted?**	**Needs to be added?**	**Comments (reason for amendment or deletion)**
e. Unauthorized Access to Computer Programs or Data for Financial Data or Illegal Acts							
f. Unauthorized Access to Computer Programs or Data for Purposes of Terrorism							
4. Interference or Disruption							
a. Interference or Disruption of Computers, Computer Systems, and Networks							
b. Interference or Disruption of Computer Program, Computer Data, Content Data, Traffic Data							
c. Interference or Disruption With Knowledge of or Intent to Cause Serious Harm or Threaten Public Safety							
d. Knowledge of or							

Provision in sample language	**In local law?**	**Citation of provision**	**Consistent with Toolkit?**	**Needs to be amended?**	**Needs to be deleted?**	**Needs to be added?**	**Comments (reason for amendment or deletion)**
Intent to Cause Interference or Disruption of Government Computers, Systems, Networks, Data							
e. Knowledge of or Intent to Cause Interference or Disruption of Critical Infrastructure							
f. Intent to Cause Interference or Disruption for Purposes of Terrorism							
5. Interception							
6. Misuse and Malware							
a. Transmission of Malware and Misuse							
b. Production, Sale, Procurement, Distribution of Computer or Computer Program for Access to Data and Misuse							

Provision in sample language	**In local law?**	**Citation of provision**	**Consistent with Toolkit?**	**Needs to be amended?**	**Needs to be deleted?**	**Needs to be added?**	**Comments (reason for amendment or deletion)**
c. Possession of Computer or Computer Program for Access to Data or Misuse							
d. No Penalty Without Intent to Commit Offense							
e. Knowledge of or Intent to Cause Physical Injury							
f. Knowledge of or Intent to Cause Modification or Impairment of Medical Care							
g. Knowledge of or Intent to Cause Threat to Public Safety or Public Health							
h. Intent to Furtherance of Terrorism							
7. Digital Forgery							
8. Digital Fraud, Procure Economic Benefit							
a. Intent to Defraud							

Provision in sample language	**In local law?**	**Citation of provision**	**Consistent with Toolkit?**	**Needs to be amended?**	**Needs to be deleted?**	**Needs to be added?**	**Comments (reason for amendment or deletion)**
b. Loss of Property to Procure Economic Benefit							
9. Extortion							
10. Aiding, Abetting, and Attempting							
11. Corporate Liability							
a. Acts Committed by Person in Leading Position							
b. Acts Committed by Employee or Agent Through Negligence of Leading Person							
PROCEDURAL PROVISIONS							
12. Scope of Procedural Provisions							
13. Conditions and Safeguards							
a. Procedural Provisions							
b. Principle of Proportionality							
14. Preservation of Stored Computer Data, Content Data, Traffic Data							

Provision in sample language	**In local law?**	**Citation of provision**	**Consistent with Toolkit?**	**Needs to be amended?**	**Needs to be deleted?**	**Needs to be added?**	**Comments (reason for amendment or deletion)**
15. Expedited Preservation and Partial Disclosure of Traffic Data							
16. Expedited Preservation of Computers or Storage Media							
17. Production Order							
18. Search and Seizure of Stored Data							
a. Search for Data							
b. Search for Connected Systems							
c. Seizure of Data							
d. Protection of Data							
19. Interception (Real-Time Collection) of Traffic Data							
20. Interception)Real-Time Collection) of Content Data							
JURISDICTIONAL PROVISIONS							
21. Jurisdiction							
a. Jurisdiction Over Persons and							

Provision in sample language	**In local law?**	**Citation of provision**	**Consistent with Toolkit?**	**Needs to be amended?**	**Needs to be deleted?**	**Needs to be added?**	**Comments (reason for amendment or deletion)**
Domestic Acts							
b. Applicability to Acts on Ships or Aircrafts							
c. Applicability to Acts by Nationals Outside of COuntry							
d. Jurisdiction Where Extradition Refused							
e. Concurrent Jurisdiction							
f. The Place Where the Offenses Occurred							
g. Reservation							
INTERNATIONAL COOPERATION							
22. International Cooperation: General Principles							
23. Extradition Principles							
a. Application of Extradition Principles							
b. Exception to Application of Extradition Principles							

Provision in sample language	**In local law?**	**Citation of provision**	**Consistent with Toolkit?**	**Needs to be amended?**	**Needs to be deleted?**	**Needs to be added?**	**Comments (reason for amendment or deletion)**
c. Offenses in this Law are Extraditable							
d. Refusal of Extradition							
24. Mutual Assistance: General Principles							
a. Authority to Provide Mutual Assistance							
b. Expedited Means of Communication							
c. Refusal to Cooperate							
d. Dual Criminality							
25. Unsolicited Information							
26. Procedures for Mutual Assistance							
a. Application of this Section and Central Authority							
b. Rules of Procedure for Mutual Assistance							
c. Refusal to Assist							
d. Inform of Outcome of Assistance							
e. Confidentiality of Request							

Provision in sample language	**In local law?**	**Citation of provision**	**Consistent with Toolkit?**	**Needs to be amended?**	**Needs to be deleted?**	**Needs to be added?**	**Comments (reason for amendment or deletion)**
f. Urgent Request or Requests Not Involving Coercive Action							
g. Confidentiality of Information to be Provided							
27. Expedited Preservation of Stored Computer Data, Content Data, or Traffic Data							
a. Request for Expedited Preservation							
b. Content of Request for Expedited Preservation							
c. Measures to be Taken							
d. Refusal of Preservation							
e. Where Preservation May Not Ensure Availability							
f. Duration of Preservation							
28. Expedited Disclosure of Preserved							

Provision in sample language	In local law?	Citation of provision	Consistent with Toolkit?	Needs to be amended?	Needs to be deleted?	Needs to be added?	Comments (reason for amendment or deletion)
Content Data, Computer Data, or Traffic Data							
29. Mutual Assistance Regarding Access to Stored Computer Data, Content Data, or Traffic Data							
30. Trans-Border Access to Stored Computer Data, Content Data, or Traffic Data							
31. Mutual Assistance In Real-Time Collection of Traffic Data							
32. Mutual Assistance Regarding Interception of Content Data or Computer Data							
33. 24/7 Points of Contact							
34. Provisions That Apply to Other Offenses							

6. Matrix of Cybercrime Laws

The following cybercrime laws were reviewed and analyzed in developing the *Toolkit*. The laws of additional countries were also reviewed with respect to various provisions, but a full comparison against the entire legal framework matrix was not performed.

MATRIX OF PROVISIONS OF LEADING CYBERCRIME LAWS

Legal Provision	CoE	Australia	Canada	EU	Germany	Japan	Mexico	Singapore	UK[29]	US	India	China
Definitions				X					X[30]			

[29] The laws in the United Kingdom that could apply to computer crime offenses are several:

- The *Computer Misuse Act of 1990 (CMA) (chapter 18)* is the primary law regarding computer crimes. It was recently amended through the *Police and Justice Act 2006.*
- The *Regulation of Investigatory Powers Act 2000 (RIPA) (chapter 23)* covers lawful and unlawful interception of communications data, evidence collection and preservation, etc.
- The *Anti-Terrorism, Crime, and Security Act 2001 (chapter 24)* also covers electronic evidence.
- Another law that may apply in computer crime cases is the *Data Protection Act of 1998 (chapter 29*), which makes it illegal to obtain unauthorized access to data (which may be separate from, or not directly involve, unauthorized access to computer systems as covered in the Computer Misuse Act).
- The *Fraud Act 2006 (chapter 35)* includes "any program or data in electronic form" as one of the definitions of "article" in terms of possession and use to commit fraud.
- The *Forgery and Counterfeiting Act 1981 (chapter 45)* covers forgery of electronic instruments that are accepted as payment within the United Kingdom.
- Copyright of works in electronic form is covered by the *Copyright, Design and Patents Act 1988 (chapter 48).*
- The *Theft Act 1978 (chapter number not available)* and the *Theft (Amendment) Act 1996 (chapter 62)* cover theft of services, monetary instruments, or credit.

Also related to computer offenses is the *Privacy and Electronic Communications Regulations 2003 (EC Regulations)*, which involve interception of electronic communications. (This is similar to the Wiretap provisions of the Electronic Communications Privacy Act (ECPA) in the United States.)

The All Party Internet Group (APIG) held meetings in 2004 to discuss the need to amend the Computer Misuse Act. See http://www.out-law.com/page-4670.
One of the most notable missing provisions in the CMA was language that that would include denial of service attacks against computer systems in the category of unauthorized acts. Distributed Denial of Service (DDoS) attacks had become a huge problem for the online gaming industry, which was suffering significant extortionate attacks on their web servers. The original CMA only dealt with unauthorized access and/or modification of computer systems (affecting confidentiality and/or integrity of information and information systems) criminal acts, not disruptive attacks affecting availability. Some of these recommendations were implemented in the Law and Justice Act 2006 (section 27, to be specific, however other issues, such as child pornography images, are included in the statute).

One notable issue that is addressed in UK computer crime laws (specifically the Police and Justice Act 2006, section 27, amendments to the CMA) that is not included in the matrix is the restriction on the manufacture, supplying, or obtaining articles for use in computer misuse offenses (i.e., a "hacking tools" restriction.) Germany also recently passed such legislation. In both cases, critics of these laws suggest that they will have a negative effect on security as they may stifle security research and/or make some tools used in penetration testing and other security services illegal to possess. See http://www.openrightsgroup.org/2006/10/05/computer-misuse-act-potential-disaster-avoided/ .
References to these laws were added to the Wikipedia entry for "Computer Crime" under "United Kingdom" (see http://en.wikipedia.org/wiki/Computer_crime#United_Kingdom).

Legal Provision	**CoE**	**Australia**	**Canada**	**EU**	**Germany**	**Japan**	**Mexico**	**Singapore**	**UK**[29]	**US**	**India**	**China**
Definitions	X			X				X[31]	X[32]			X[33]
Computer System	X	X	X[34]	X				X[35]		X[36]	X[37]	
Computer Data	X	X	X[38]	X	X[39]			X[40]	X		X[41]	
Service Provider	X	X						see[42]	X		X[43]	
Traffic Data	X	X	X[44]	X				see[45]	X	X		
Substantive Criminal Law												
Illegal Access	X	X[46]	X[47]	X	X[48]	X[49]	X	X[50]	X	X[51]	X[52]	X[53]

[30] The CMA itself does not define terms, per se. APIG, in their report on the CMA, stated that it was beneficial to *not have* defined terms, as it allowed the courts to decide on a contemporary basis what the meaning of certain terms should be. This allowed the law to remain flexible in terms of changes in technology, rather than having to be amended frequently as new technologies emerged. The CMA does, however, contain a section dealing with interpretation (s17) that to guide courts in applying the law.

[31] CMA, Section 1.2, ("interpretation").

[32] EC Regulations, Section 2.

[33] Regulations on Safeguarding Computer Information Systems, Article 2, Feb. 1996.

[34] Canada Evidence Act, Sections 31.1-31.8; Canada Criminal Code, Unauthorized Use of Computer, Section 342.1.

[35] CMA, Section 1.2(1) ("computer").

[36] Computer Fraud and Abuse Act (CFAA), 18 U.S.C. Section 1030(e).

[37] Information Technology Act, Sections 2(1)(j), (k), (l) (computer network, computer resource, and computer system).

[38] Canada Evidence Act, Sections 31.1-31.8; Canada Criminal Code, Unauthorized Use of Computer, Section 342.1.

[39] German Criminal Code (Strafgesetzbuch ("StGB"), Section 202a (2).

[40] CMA, Section 1.2(1) ("data")

[41] Information Technology Act of 2000, Section 2(1)(o) ("data").

[42] No, but cf. Electronic Transactions Act (ETA) Ch. 88 Part III. 10, "network service provider" exemption from liability. Term used without definition.

[43] Information Technology Act of 2000, Section 2(1)(w) (defines "intermediary"). Explanation to Section 79 provides that a "network service provider" means an intermediary.

[44] Canada Criminal Code, Section 342.1(2).

[45] No, but cf. "Output" defined broadly as factual representation produced by a computer in Section I.2(1) of CMA.

[46] Cybercrime Act 2001; Div 478.1.

[47] Canada Criminal Code, Theft, Section 326; Canada Criminal Code, Unauthorized Use of Computer, Section 342.1.

[48] StGB, Section 202a (1).

[49] Limited scope—a specific computer connect to another computer via a telecommunication line – must have access control function – does not apply to stand-alone computers.

[50] CMA, Sections II.3, 4 CMA.

[51] Computer Fraud and Abuse Act (USC 18 Section 1030).

[52] Information Technology Act of 2000, Section 43(a), (g) and Section 66 (hacking).

[53] Criminal Law of the People's Republic of China, Article 285.

Legal Provision	**CoE**	**Australia**	**Canada**	**EU**	**Germany**	**Japan**	**Mexico**	**Singapore**	**UK[29]**	**US**	**India**	**China**
Illegal Interception	X	X[54]	X[55]		X[56]		X	X[57]	X[58]	X[59]	X[60]	X[61]
Data Interference	X	X[62]	X[63]	X	X[64]	X[65]	X	X[66]	X	X	X[67]	X[68]
System Interference	X	X[69]	X[70]	X	X[71]	X	X	X[72]	X		X[73]	X[74]
Misuse of Devices	X	X	X[75]	X		?		X[76]	X	X[77]	X[78]	
Computer-related Forgery	X		X[79]	X	X[80]	X		X[81]	X	X[82]	X[83]	X[84]

[54] Cybercrime Act 2001; Div 478.1.
[55] Canada Criminal Code, Interception of Communications, Sections 183-196; Canada Criminal Code, Unauthorized Use of Computer, Section 342.1.
[56] Covered in part by section 201 of StGB as well as section 148 and section 89 of the German Telecommunications Act (Telekommunikationgesetz ("TKG").
[57] Sections II.6 CMA.
[58] RIPA, Section 1.
[59] Wire and Electronic Communications Interception and Interception of Oral Communications, USC 18 Sections 2510-2522.
[60] Information Technology Act of 2000, Section 43(b) and Section 66 (hacking).
[61] Criminal Law of the People's Republic of China, Article 252.
[62] Cybercrime Act 2001; Div. 478.3.
[63] Canada Criminal Code, Mischief, Section 430; Security of Information Act, Section 3(1)(d).
[64] StGB, Section 303a.
[65] Limited to interference with a business transaction done with a computer system.
[66] CMA, Sections II.5, 7.
[67] Information Technology Act of 2000, Section 43(a) and Section 66 (hacking).
[68] Criminal Law of the People's Republic of China, Article 286.
[69] Cybercrime Act 2001; Div. 478.2.
[70] Canada Criminal Code, Interception of Communications, Sections 183-196.
[71] StGB, covered in part by Section 303b.
[72] CMA, Section II.7.
[73] Information Technology Act of 2000, partly covered in Section 43 and Section 66 (hacking).
[74] Criminal Law of the People's Republic of China, Article 286.
[75] Canada Criminal Code, Unauthorized Use of Computer, Section 342.1.
[76] CMA, Section II.6.
[77] Computer Fraud and Abuse Act, 18 USC Section 1030.
[78] Information Technology Act of 2000, partly covered in Section 43 and Section 66 (hacking).
[79] Not specifically covered but general provisions on this topic are probably broad enough to encompass this item.
[80] StGB, Section 269.
[81] Cf. Penal Code (Forgery), Section 463.
[82] Computer Fraud and Abuse Act, 18 USC Section 1030.
[83] Partly covered in Section 43 and Section 66 (Hacking) of the Information Technology Act, 2000
[84] Criminal Law of the People's Republic of China, Article 287 ("or other crimes").

Legal Provision	CoE	Australia	Canada	EU	Germany	Japan	Mexico	Singapore	UK[29]	US	India	China
Computer-related Fraud	X		X[85]		X[86]	X		X[87]	X	X[88]	X[89]	X[90]
Offences Related to Child Pornography	X		X[91]	X	X[92]	X?	X	X[93]	X	X[94]	X[95]	X[96]
Offenses Related to Infringements of Copyright And Related Rights	X		X[97]	X	X[98]	X[99]	X	X[100]	X	X		X[101]
Attempt and Aiding	X		X[102]	X	X[103]	X[104]		X[105]	X	X[106]	X[107]	X[108]

[85] Not specifically covered but general provisions on this topic are probably broad enough to encompass this item.

[86] Section 263a StGB.

[87] Section II.4 CMA.

[88] Computer Fraud and Abuse Act (USC 18 Section 1030)

[89] Information Technology Act of 2000, partly covered in Section 43 and Section 66 (hacking).

[90] Criminal Law of the People’s Republic of China, Article 287 (“or other crimes”).

[91] Canada Criminal Code, Offenses Tending to Corrupt Morals (§§163-164).

[92] StGB, covered in part by section 184b.

[93] Cf. broad language of Children & Young Persons’ Act, Ch. 38. Does not specifically reference child pornography but would likely serve as basis for prosecution. Cf. Broadcasting Act (Cap. 28), establishing Media Dev. Authority of Singapore Licensing body Internet Code of Practice.

[94] Sexual Exploitation of Children, 18 USC Section 2251.

[95] Information Technology Act of 2000, Section 67, deals with publication of obscene information in general, while proposed amendments to the Act include addition of Section 67(2) which deals with child pornography in particular (the amendment is pending before the Indian Parliament and has not yet come into force yet.)

[96] Criminal Law of the People’s Republic of China, Articles 363, 366, 367.

[97] Federal prosecution under the Copyright Act.

[98] German Copyright Act (Urheberrechtsgesecht (“UrhG”), Section 106 ff.

[99] Limited: facilitating unauthorized access, attempt to commit fraud or threatening; attempt at illegal production and use of an electro-magnetic record on a payment card.

[100] Copyright Act, Ch. 63, Part II, Sections 7A, 17 (embraces “computer program” and works “stored in a computer program,” etc.).

[101] Criminal Law of the People’s Republic of China, Articles 217, 218, 220; Article 1 (“protecting the copyright of authors in their literary, artistic, and scientific works and the copyright-related rights and interests”) of Copyright Law of the People’s Republic of China. See also Articles 3, 9, 10(5) (“by any other means”), Article 10(6) (“the right of distribution”). Also see Articles 10(2)-10(11-12), (15); Article 12 (“adaptation, translation” of Copyright Law of the People’s Republic of China; Article 11 (“the copyright in a work shall belong to its author”) and Articles 20, 24(2).

[102] Canada Criminal Code, Parties to the Offenses, Sections 21-24.

[103] StGB, Sections 22-24 (attempt), Sections 26-27 (aiding and abetting).

[104] Limited to: unauthorized access, facilitating unauthorized access, revealing secrets, destruction of private electronic record, destruction of official electronic records, computer fraud.

[105] CMA, Section 11.10.

[106] Computer Fraud and Abuse Act, 18 USC Section 1030.

Legal Provision	**CoE**	**Australia**	**Canada**	**EU**	**Germany**	**Japan**	**Mexico**	**Singapore**	**UK[29]**	**US**	**India**	**China**
And Abetting												
Corporate Liability	X		X[109]	X	X[110]						X[111]	X[112]
Sanctions and Measures	X	X[113]	X	X	X[114]			X[115]	X		X[116]	X[117]
Procedural Law							X					
Scope of Procedural Provisions	X		X[118]	X						X		
Conditions and Safeguards	X	X	X[119]	X				X[120]	X[121]	X		
Expedited Preservation of Stored Computer Data	X	X	X[122]	X	X[123]					X		
Expedited Preservation and	X			X	X[124]					X		X[125]

[107] Information Technology Act of 2000, Section 43(g) (covers cases of providing any assistance. Apart from that the general principles of Indian Penal Code that cover attempt, aiding and abetting will apply).

[108] Criminal Law of the People's Republic of China, Articles 22, 23, 24, 27, 29.

[109] Personal Information Protection and Electronic Documents Act.

[110] German Regulatory Offences Act (Gesetz über Ordnungswidrigkeiten ("OWig"), Sections 30 and 130.

[111] Information Technology Act of 2000, Section 85.

[112] Criminal Law of the People's Republic of China, Articles 30, 31.

[113] Cybercrime Act of 2001.

[114] StGB, Sections 202a, 202b, 202c, 263a, 269, 303a, Article 13(1); OWig, Section 30 OWig, Article 13 (2).

[115] Sanctions specified for each offense in CMA.

[116] Sanctions specified fro each offence in the Information Technology Act, 2000

[117] Criminal Law of the People's Republic of China, Articles 32, 33, 34.

[118] Canada Criminal Code, Section 184.2.

[119] Canada Criminal Code, Section 184.2.

[120] No, but cf. Section III.14 CMA (limiting law enforcement investigations to "lawful" exercise of powers conferred under written law).

[121] EC Regulations, Sections 6, 7, and 8.

[122] Canada Criminal Code, Part XV 487, Special Procedures and Powers Search Warrant.

[123] German Code of Criminal Procedure (Strafprozessordnung ("StPO"), Sections 94-95, 98.

[124] StPO, Sections 100g and 100h.

Legal Provision	**CoE**	**Australia**	**Canada**	**EU**	**Germany**	**Japan**	**Mexico**	**Singapore**	**UK[29]**	**US**	**India**	**China**
Partial Disclosure of Traffic Data												
Production Order	X		X[126]	X	X[127]			X[128]	X	X		
Search & Seizure of Stored Computer Data	X	X	X[129]	X	X[130]			X[131]		X	X[132]	X[133]
Real-time Collection of Traffic Data	X		X[134]	X	X[135]				X	X		X[136]
Interception of Content Data	X	X	X[137]	X	X[138]				X	X		X[139]
Jurisdiction												
Jurisdiction	X		X[140]	X	X[141]			X[142]	X			X[143]

[125] Regulation on Internet Information Service of the People’s Republic of China, Article 14; Working Rules on Interim Regulation of International Networking of Computer Information Network, Article 19; Regulations on Internet Surfer Service Sites, Article 10; Provisions for the Administration of Internet Electronic Bulletin, Articles 14, 15.

[126] Canada Criminal Code, Section 487.

[127] StPO, Section 95, Article 18(1) lit. a); TKG, Sections 112-113, Article 18(1) lit. b.

[128] Cf. Section III.15 CMA (repealed) now cf. III.14 CMA (subject to Criminal Procedure Code).

[129] Canada Criminal Code, Section 487(2)1.

[130] StPO, Sections 94-95, 102-103, 105, 161, 163, Article 19(1) and 19(3).

[131] Section III.15 CMA (repealed) now cf. III.14 CMA (subject to Criminal Procedure Code)

[132] Information Technology Act of 2000, Section 76 (Confiscation) and S 80 (power of police officer to enter and search).

[133] Criminal Law of the People’s Republic of China, Article 116; People’s Procuratorate Rules of Criminal Procedure, Articles 188, 192; Procedural Rules for Criminal Cases by Public Security Organs, Articles 57, 58.

[134] Canada Criminal Code, Sections 183-196, Interception of Communications, Wiretap Legislation.

[135] StPO, Covered in part by section 100g StPO.

[136] State Security Law of the People’s Republic of China, Article 10; People’s Police Law of the People’s Republic of China, Article 16.

[137] Canada Criminal Code, Section 487(2)1.

[138] StPO, Sections 100a and 100b.

[139] State Security Law of the People’s Republic of China, Article 10; People’s Police Law of the People’s Republic of China, Article 16.

[140] Canada Criminal Code, Section 7(4).

[141] StGB, Sections 3-9.

[142] CMA, Section III.12.

Legal Provision	**CoE**	**Australia**	**Canada**	**EU**	**Germany**	**Japan**	**Mexico**	**Singapore**	**UK**[29]	**US**	**India**	**China**
International Cooperation			X[144]									
General Principles Relating To International Cooperation	X			X					X			
Extradition	X			X	X[145]	X[146]	X		X			X[147]
General Principles Relating To Mutual Assistance	X			X	X[148]	X?			X			
Spontaneous Information	X			X	X[149]							
Procedures Pertaining to Mutual Assistance Requests In the Absence of Applicable International Agreements	X			X	X[150]				X			
Confidentiality & Limitation On Use	X			X	X[151]				X			
Expedited Preservation of	X			X	X[152]							

[143] Criminal Law of he People's Republic of China, Articles 6—12.

[144] Multilateral Assistance Treaty (MLAT) specifically codified if Canadian commits an offense in another country; cannot subpoena in another country. Federal Prosecutions Service Deskbook, Part VIII, MLAT is carried out through International Assistance Group (IAG). In 1988, the IAG was established as part of the Department of Justice Criminal Law Branch. The IAG was established, in part, to carry out the functions assigned to the Minister of Justice as Central Authority under the Act and related treaties. All offenses are covered under Section 7 of MLAT through IAG in Ottawa on a 24/7 basis.

[145] Gesetz über die internationale Rechtshilfe in Strafsachen ("IRG"), Sections 2-3 of the Act on International Legal Assistance in Criminal Matters.

[146] By treaty – with the United States and Republic of Korea

[147] Extradition Law of the People's Republic of China, Articles 3,4,5,7,8,9.

[148] IRG, various sections.

[149] IRG, Sections 61a and 83j.

[150] IRG, Section 59ff.

[151] *Id.*

[152] IRG, Section 66f.

Legal Provision	CoE	Australia	Canada	EU	Germany	Japan	Mexico	Singapore	UK[29]	US	India	China
Stored Computer Data												
Expedited Disclosure of Preserved Traffic Data	X			X	X[153]							
Mutual Assistance Regarding Accessing of Stored Computer Data	X			X	X[154]							
Trans-border Access to Stored Computer Data With Consent on Where Publicly Available	X			X	X[155]							
Mutual Assistance in the Real-Time Collection of Traffic Data	X			X	X[156]				X			
Mutual Assistance Regarding The Interception of Content Data	X			X	X[157]				X			
24/7 Network	X			X	X[158]							

[153] IRG, Section 59ff.
[154] IRG, Section 66.
[155] StPO, Section 94.
[156] IRG, Section 59ff.
[157] IRG, Section 59ff.
[158] Germany has established a 24/7 contact within the Bundeskriminalamt; also Germany is a member of the 24/7 network of the G8 High-Tech Crime Subgroup and of the ICPO Interpol.

Legal Provision	**CoE**	**Australia**	**Canada**	**EU**	**Germany**	**Japan**	**Mexico**	**Singapore**	**UK**[29]	**US**	**India**	**China**
Final Provisions												
Signature & Entry into Force	X					X[159]			X			
Other		X[160]										

[159] Signature, not ratification. Amendments to put it into synch with the CoE Convention delayed in the Parliament (Diet) since 2004.
[160] Provisions of Cybercrime Law – The Commonwealth of Australia:

BACKGROUND
Australia is a Commonwealth *realm*, one of 16 within the Commonwealth of Nations. The Commonwealth of Nations, usually known as the Commonwealth, is a voluntary association of 53 independent sovereign states, most of which are former British colonies (the exceptions being the UK itself and Mozambique). Queen Elizabeth II of the UK is Head of the Commonwealth. The Commonwealth of Australia is a constitutional monarchy with a parliamentary system of government. Australia consists of six states, two major mainland territories, and other minor territories. (Australia is similar in population to the state of Texas, but with 10 times the geographic area.)

Australia is a founding member of the UN, a member of the OECD and the WTO. It has pursued several major bilateral free trade agreements, most recently the Australia-US Free Trade Agreement. Australia led the formation of the Cairns Group (a coalition of 19 agricultural exporting countries) and Asia-Pacific Economic Cooperation (APEC). Through its Telecommunications Working Group, APEC has been very active in support of strengthening critical infrastructures.

The Commonwealth of Australia is currently in transition from the common law model to the code model. Although all six states have some legislation on the criminal law, in some states criminal law has been codified whereas in others the bulk of the law is based on the common law. In 1994, both the Commonwealth Government and the State and Territory Premiers' Leaders Forum endorsed a "Model Criminal Code" project as one of national significance. The Commonwealth Criminal Code Bill was passed by the Commonwealth Parliament in March, 1995. The Model Criminal Code Officers Committee (MCCOC) released the final report entitled Theft, Fraud, Bribery and Related Offences in December 1995.

ACTIVITIES REGARDING LEGAL PROVISIONS
- Customs Act 1901
- Crimes Act 1914
- Commonwealth Criminal Code Act 1995, enacted from the Model Criminal Code project report
- Crimes Amendment (Forensic Procedures) Act 2000, Model Forensic Procedures Bill and the Proposed National DNA Database in May 1999 (report February 2000).
- Cybercrime Act 2001 [http://www.cybercrimelaw.net/laws/countries/australia.html], based entirely on the recommendations of the MCCOC report Chapter 4. [Steel, A. (2001).

The New Computer Crimes. *Criminal Law Journal*.] The Cybercrime Act is "An Act to amend the law relating to computer offences and for other purposes." [MCCOC. (2001). Chapter 4: Damage and Computer Offences. In *Model Criminal Code*. Canberra: Standing Committee of Attorneys-General, Commonwealth of Australia.].

<u>Computer offences</u>
- Australian Security Intelligence Organization Act 1979, Substitute "Part 10-7 of the Criminal Code" for "section 76D or 76E of the Crimes Act 1914.
- Crimes Act 1914, Repeal Part VIA
- Criminal Code Act 1995, Repeal and substitute paragraphs for 4.1(1)(b) and (c); Insert "Part 10.7 – Computer offenses Division 476 – Preliminary (see definitions, jurisdiction, etc. below), Division 477 – Serious computer offences (categorized below), Division 478 – Other computer offences (categorized below)"

- Education Services for Overseas Students Act 2000, Repeal and substitute "…"
- Telecommunications (Interception) Act 1997, Omit and substitute "…"

LAW ENFORCEMENT POWERS RELATING TO ELECTRONICALLY STORED DATA

- Crimes Act 1914
- Customs Act 1901
- Australian Crime Commission Act 2002, established the Australian Crime Commission (ACC) as an intelligence collection and dissemination body for cybercrime offences (among others).
- Credit Card Skimming Offences 2004.
- Australian Anti-Terrorism Act 2005. National Identity Security Strategy report issued April 2007. The Council of Australian Governments (COAG) considered identity security at its special meeting on Counter-Terrorism on 27 September 2005. COAG agreed to the development and implementation of a national identity security strategy, underpinned by an inter-governmental agreement (IGA).

Australian Government e-Authentication Framework, AGIMO (Department of Finance and Administration), 2005; http://www.agimo.gov.au/infrastructure/authentication/agaf
Australian Government Smartcard Framework, AGIMO (Department of Finance and Administration), 2006; http://www.agimo.gov.au/infrastructure/smart_cards
Gatekeeper Framework, AGIMO (Department of Finance and Administration), 2006; http://www.gatekeeper.gov.au
Australian Government Protective Security Manual, Attorney-General's Department, *2005;* http://www.ag.gov.au/agd/www/protectivesecurityhome.nsf/Page/Protective_Security_Manual
Australian Government Information and Communications Technology Security Manual, Defence Signals Directorate, Sep 2006; http://www.dsd.gov.au/library/infosec/acsi33.html.
Section 85ZE of the Crimes Act 1914 makes it an offence to use email in a manner that is menacing, harassing or offensive.

7. USEFUL REFERENCE MATERIALS

- *Best Practices for Seizing Electronic Evidence*, U.S. Secret Service, http://www.ustreas.gov/usss/electronic_evidence.shtml.

- Clay Wilson, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Service, RL32114, Nov. 15, 2007, http://www.fas.org/sgp/crs/terror/RL32114.pdf.

- *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, U.S. Government Accountability Office, GAO-07-705, June 2007, http://www.gao.gov/new.items/d07705.pdf.

- David A. Dittrich, "Developing an Effective Incident Cost Analysis Mechanism," *SecurityFocus*, June 12, 2002, http://www.securityfocus.com/infocus/1592

- *Electronic Crime Scene Investigation: A Guide for First Responders*, National Institute of Justice, NCJ 187736, 2001, http://www.ncjrs.org/pdffiles1/nij/187736.pdf.

- *First Responder's Manual*, U.S. Department of Energy Computer Forensic Laboratory, http://www.linuxsecurity.com/resource_files/documentation/firstres.pdf.

- *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, National Institute of Justice, NCJ 199408, 2004, http://puborder.ncjrs.org/Content/ItemDetails.asp?strItem=NCJ+199408.

- *Guidance on Preparing a Complete & Sufficient Suspicious Activity Report (SAR)*, Financial Crimes Enforcement Network, November 2003, http://www.irs.gov/pub/irs-tege/itg_sarc_prep.pdf.

- *Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries*, European Union, 2005, http://europa.eu.int/information_society/eeurope/2005/all_about/security/handbook/text_en.htm.

- Hossein Bidgoli, editor, *Handbook of Information Security*, chapter *Active Response to Computer Intrusions*, by David Dittrich and Kenneth Einar Himma, John Wiley and Sons, 2005, http://books.google.com/books?id=0RfANAwOUdIC&pg=PA664

- Incident Cost Analysis and Modeling Project (ICAMP) Final Reports 1 and 2, http://connect.educause.edu/Library/Abstract/IncidentCostAnalysisandMo/35282?time=1225691051
- http://connect.educause.edu/Library/Abstract/IncidentCostAnalysisandMo/35283?time=1225690927.

- Jelena Mirkovic, Sven Dietrich, David Dittrich, and Peter Reiher, *Internet Denial of Service: Attack and Defense Mechanisms*, Prentice Hall PTR, 2004, http://my.safaribooksonline.com/0131475738/ch08.

- Jody R. Westby & Julia Allen, *Governing for Enterprise Security Implementation Guide*, Carnegie Mellon University, Software Engineering Institute, 2007, http://www.cert.org/governance.

- Jody R. Westby, ed., *International Guide to Cyber Security*, American Bar Association Publishing, 2003, http://abastore.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450036 (this reference is free to people in developing countries; send an email to Jody Westby at westby@mindspring.com).

- Jody R. Westby, ed., *International Guide to Privacy*, American Bar Association Publishing, 2004,http://abastore.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450037 (this reference is free to people in developing countries; send an email to Jody Westby at westby@mindspring.com).

- Jody R. Westby, ed., *International Guide to Combating Cybercrime*, 2004, http://abastore.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450030 (this reference is free to people in developing countries; send an email to Jody Westby at westby@mindspring.com).

- Jody R. Westby, ed., *Roadmap to an Enterprise Security Program*, 2005, http://abastore.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450039 (this reference is free to people in developing countries; send an email to Jody Westby at westby@mindspring.com).

- Lorenzo Valeri, Geert Somers, et al, *Handbook of Legal Procedures of Computer and Network Misuse in EU Countries*, Technical Report prepared for the European Commission, Rand Corporation (Rand Europe), 2006, http://www.rand.org/pubs/technical_reports/TR337/.

- Orin Kerr, *Computer Crime Law*, Thomson-West, 2006, http://west.thomson.com/productdetail/136663/40077154/productdetail.aspx. Orin Kerr, *Computer Crime Law 2008 Supplement.*

- Pauline C. Reich, ed., *Cybercrime and Security*, Oxford University Press (ongoing looseleaf series, updated quarterly).

- Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy, Business Lawyer*, University of Washington School of Law, Vol. 62, 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1097469.

- *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Computer Crime and U.S. Department of Justice Intellectual Property Section, Criminal Division. http://www.cybercrime.gov/s&smanual2002.htm and updated Appendix F (2006), http://www.cybercrime.gov/s&sappendix.htm#_F_.

- Stein Schjolberg, Cybercrime Law Website, http://www.cybercrimelaw.net.

- Susan Brenner, CYB3RCRIM3, http://cyb3rcrim3.blogspot.com/.

- Susan Brenner, *Emerging Fault Lines of the Nation-State*, Oxford University Press, 2009, http://www.amazon.com/Cyberthreats-Emerging-Fault-Lines-Nation/dp/0195385012/ref=sr_1_1?ie=UTF8&s=books&qid=1239539217&sr=1-1.

- Susan Brenner, "Fantasy Crime, 11 *Vanderbilt Journal of Entertainment and Technology Law* 1, 2008, http://works.bepress.com/susan_brenner/1/.

- Susan Brenner, "at light speed: Attribution and Response to Cybercrime/terrorism, warfare," 97 *Journal of Criminal Law & Criminology* 379, 2007, http://www.amazon.com/Law-Smart-Technology-Susan-Brenner/dp/0195333489/ref=sr_1_2?ie=UTF8&s=books&qid=1239539217&sr=1-2.

- Susan Brenner, *Law in an Era of "Smart" Technology*, Oxford University Press, 2007, http://www.amazon.com/Law-Smart-Technology-Susan-Brenner/dp/0195333489/ref=sr_1_2?ie=UTF8&s=books&qid=1239539217&sr=1-2.

- Susan Brenner, "Should Online Defamation be Criminalized?" 75 *Mississippi Law Journal* 1, 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=982418.

- Susan Brenner (with Leo L. Clarke), "Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data," *West Search and Seizure Law Report*, Feb. 2007.

- Susan Brenner, "Cybercrime: Rethinking Crime Control Strategies," *Cybercrime Online*, 2006.

- Susan Brenner, "Cybercrime Jurisdiction," 45 *Crime, Law and Social Change*, Spring 2006.

- Susan Brenner and Bert-Jaap Koops, eds., *Cybercrime and Jurisdiction: A Global Survey*, The Hague: Asser Press, 2006, http://www.amazon.co.uk/Cybercrime-Jurisdiction-Global-Information-Technology/dp/9067042218.

- Susan Brenner (with Leo L. Clarke), "Distributed Security: Preventing Cybercrime," 23 *John Marshall Journal of Computer and Information Law* 659, 2005, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=845085.

- Susan Brenner, "Why the Law Enforcement Model is a Problematic Strategy for Dealing with Terrorist Activity Online, 99 *Proceedings of the American Society of International Law* 108, 2005.

- Susan Brenner, "Requiring Protocols in Computer Search Warrants," 2 *Digital Investigation* 1, 2005 (Reed Elsevier, United Kingdom).

- Susan Brenner, "Distributed Security: Moving Away from Reactive Law Enforcement," 9 *International Journal of Communications Law and Policy* 1, 2005, http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID623283_code342087.pdf?abstractid=623283&mirid=1.

8. TOOLKIT FOR CYBERCRIME LEGISLATION PROJECT ORGANIZATION

The *Toolkit* was developed by a global, multidisciplinary team of policy experts, industry representatives, academicians, attorneys, technical experts, and government personnel from around the globe working through the American Bar Association's (ABA) Privacy & Computer Crime Committee (PACC), Section of Science and Technology Law.

The project was led by Jody R. Westby, chair of the PACC, and member of the ITU Secretary-General's High Level Experts Group on Cybersecurity. The project vice chair was David Weitzel, PACC vice chair.

8.1. Toolkit Leadership

Chair: **Jody R. Westby, Chair, ABA Privacy & Computer Crime Committee, & CEO, Global Cyber Risk LLC**

Vice Chair: **David Weitzel, Vice Chair, ABA Privacy & Computer Crime Committee & MITRE Corporation**[161]

Purpose (Preamble) Working Group:

Co-Chair: Pamela Hassebroek, Ph.D., Science and Technology Policy Fellow, The National Academies, Computer Science and Telecommunications Board, U.S.A.

Co-Chair: Pauline Reich, Professor, Waseda University School of Law, Tokyo, Japan; Director, Asia-Pacific Cyberlaw, Cybercrime and Internet Security Research Institute

Definitions Working Group:

Co-Chair: Susan Brenner, NCR Distinguished Professor of Law & Technology, University of Dayton School of Law

Co-Chair: John Nugent, Assistant Professor, University of Dallas Graduate School of Management

Substantive Criminal Law Working Group:

Co-Chair: Drew C. Arena, Vice President and Associate General Counsel, Law Enforcement and National Security Compliance, Verizon Communications

Co-Chair: Jody R. Westby, CEO, Global Cyber Risk LLC

Procedural Law Working Group:

Co-Chair: Dave Dittrich, Security Consultant

Co-Chair: David Ward, Senior Legal Advisor – Policy Division, Public Safety and Homeland Security Bureau, U.S. Federal Communications Commission & Professor of Practice, Capitol College

[161] David Weitzel's affiliation with the MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed in this document. Likewise, the affiliations noted for other participants is provided for identification purposes only, and is not intended to convey or imply their organizations' concurrence with, or support for this document.

Co-Chair: Joseph J. Schwerha, IV, Associate Professor, Department of Business & Economics, California University of Pennsylvania

Jurisdiction and Implementation Working Group:

Co-Chair: Richard Gordin, Partner, Armstrong Teasdale LLP

Co-Chair: Tom Smedinghoff, Partner, Wildmann, Harrold LLP

International Cooperation Working Group:

Co-Chair: Don M. Blumenthal, Senior Principal, Global Cyber Risk LLC

Co-Chair: Joseph P. Richardson, Consultant

8.2. Toolkit Participants

The following participants, although not all members of the ABA, provided information and assistance in the development of the *Toolkit*. The language and statements expressed in the *Toolkit* are not necessarily endorsed by them or their employers or the ABA.

Sylna Ambris-Dick		
Nishant Anand	Mays Business School, Texas A&M University	U.S.
Ali Reza Arasteh	Research in Motion	Canada
Drew C. Arena	Verizon Communications	U.S.
Vikas Arora		India
Jerry Bakut	University of Strathclyde	Scotland
William Barletta	Massachusetts Institute of Technology	U.S.
Lee Barken	San Diego State University	U.S.
James Barnes	Metta Communications, LLC	U.S.
Michael Bennett	Wildmann Harrold LLP	U.S.
Allan Berg	Capitol College	U.S.
Don M. Blumenthal	Global Cyber Risk LLC	U.S.
William C. Boni	Motorola Information Protective Services	U.S.
Susan W. Brenner	University of Dayton School of Law	U.S.
Steven Brower	Stephan, Oringler, Richman, Theodora & Miller	U.S.
Bryan A. Carey	Kellogg, Huber, Hansen, Todd, Evans & Figel	U.S.
William E. Carter	Hartford Financial Services Group	U.S.
Aldo F. Castaneda		U.S.
Denley Chew	Federal Reserve Bank of New York	U.S.
John R. Christiansen	Christiansen IT Law	U.S.

Dave Cullinane	Ebay	U.S.
George F. Curtis	Center for Economic Crime & Justice Studies, Utica College	U.S.
Isabel Davara	Davara Abogados S.C.	Mexico
David Dittrich	Security Consultant	U.S.
Gitanjli Duggal		India
Christian C. Ekeigwe	ISACA Lagos Chapter & IT Committee of Institute of Chartered Accountants of Nigeria	Nigeria
Bart Epstein	Tutor.com, Inc.	U.S.
Jayantha Fernando	Information and Communication Technology Agency of Sri Lanka	Sri Lanka
Richard L. Field	Law Offices of Richard Field	U.S.
Mathew Flaminio	Thomas M. Cooley Law School	U.S.
Richard H. Gordin	Tighe Patton	U.S.
Robert Foehl	Target Corporation	U.S.
Mark F. Foley	Foley & Lardner	U.S.
Scot Ganow	Verispan	U.S.
Arlan Gates	Baker & McKenzie	Canada
N.K. Ghosal	Consultant	India
Edward F.X. Gilbride	Federal Deposit Insurance Corporation	U.S.
Alan Stuart Goldberg	Goldberg Law Office	U.S.
Seymour E. Goodman	Georgia Institute of Technology	U.S.
Bryan Griffith	University of Toledo School of Law	Canada
Judyth Gulden	University of Tulsa School of Law	U.S.
Zvi Joseph	Amdocs	U.S.
Pamela Hassebroek	The National Academies	U.S.
Kirk Herath	Nationwide Insurance Companies	U.S.
Janine Hiller	Virginia Tech	U.S.
Daniel C. Hurley, Jr.	U.S. Department of Commerce, National Telecommunications & Info Admin.	U.S.
Zahid Jamil	Jamil & Jamil	Pakistan
Anand Prakash Jangid	Infosys Technologies, Ltd.	India
Odia Kagan	Shavit Bar-On-Gal-On Tzin Nov Yagur Law Offices	Israel
William Karam	Baker & McKenzie	Canada

Tom Kellermann	Core Security Technologies, Inc.	U.S.
Abdus Sami Khan	National Clearing Company of Pakistan, Ltd.	Pakistan
Uldis Kinis	Constitutional Court of the Republic of Latvia & Int'l Tribunal for Former Yugoslavia	Latvia
Axel H.R. Lehmann	Universitaet der Bundeswehr Muenchen	Germany
Theodore C. Ling	Baker & McKenzie	Canada
Arnold T.J. Mabere	Dimension Data	South Africa
Kathy Macdonald	Global Centre for Securing Cyberspace & Calgary Police	Canada
Stuart MacLennan	University of Strathclyde	Scotland
Fernando Maresca	National Office of Information Technology	Argentina
Ignacio A. Marino	U.S. Secret Service	U.S.
Gilberto Martins		
Mandana Massiha	MTV2 Affiliates	U.S.
Douglass McCollum	Neustar	U.S.
William McComas	Shapiro Sher Guinot & Sandler	U.S.
Dimo Michailov	Bingham McCutchen LLP	U.S.
Raman Narasimhan	Perot Systems	India
Jorge Navarro	Molina Salgado & De Alva	Mexico
Paul Neff	Williams Lea	U.S.
Robert K. Nied	Robert Nied Consultancy Group	U.S.
John H. Nugent	University of Dallas, Center for Information Assurance	U.S.
Sharon O'Bryan	OAS, Inc.	U.S.
Justice Ogoroh	University of Strathclyde	Scotland
Oluwaseyi Oni	University of Strathclyde	Scotland
Ivan Orton	King County Prosecutor's Office	U.S.
Therese R. Perera	Legal Draftsman	Sri Lanka
Timothy Phillips	Information Assurance Solutions	Canada
David Polinsky	Attorney, Mediator	U.S.
Mark Pollitt	National Center for Forensic Science, University of Central Florida	U.S.
Rajnish Popat	Popat & Popat	India
Richard Power	Carnegie Mellon CyLab	U.S.
Michael Rasmussen	Corporate Integrity LLC	U.S.

Miguel Recio	Attorney	Spain
Pauline Reich	Waseda University School of Law	Japan
Joseph P. Richardson	Consultant	U.S.
Audrey Rogers	Pace University	U.S.
Robin Ruefle	Carnegie Mellon University, Software Engineering Institute	U.S.
Tony Rutkowski	Netmagic Associates LLC	U.S.
Assaad Sakha	Concordia Institute for Info. Systems Engineering, Concordia University	Canada
Nandkumar Saravade	Indian Police Service (Ret'd)	India
A.K. Saushik	Ministry of Communication & Information Technology, E-Security Division	India
Bradley J. Schaufenbuel	Midwest Banc Holdings, Inc.	U.S.
Joseph J. Schwerha	Trace Evidence LLC & California University of Pennsylvania	U.S.
Ken M. Shaurette	Financial Institution Products Corporation	U.S.
Christopher Sloan	Liberty Mutual Insurance Company	U.S.
Thomas J. Smedinghoff	Wildmann Harrold LLP	U.S.
Michael Spadea	Barclay's Bank	U.K.
Jon C. Stanley	Law Office of Jon Stanley	U.S.
Jacky Sutton	UNDP	Iraq
Louis Tinto	Jefferson Wells International	U.S.
Steven Tseng	John Marshall Law School	U.S.
James Vigil, Jr.		U.S.
David Ward	Federal Communications Commission & Capitol College	U.S.
Henning Wegener	World Federation of Scientists' Permanent Monitoring Panel on Information Security	Germany & Spain
Michael Weil	Huron Consulting Group	U.S.
Justin B. Weiss	Digital Policy Group	U.S.
David Weitzel	MITRE Corporation	U.S.
Alan S. Wernick	Wernick & Associates	U.S.
Jody R. Westby	Global Cyber Risk LLC & Global Cyber Legal LLC	U.S.

Christine Whalley	Pfizer, Inc.	U.S.
Peter Winn	University of Washington	U.S.
Michelle Wisdom	University of Missouri – Columbia	U.S.