Preparatory Colloquium
24-27 April 2013, Moscow (Russia)
Section II: Information Society and Penal Law

UNITED STATES OF AMERICA*

Raneta LAWSON MACK*

(A) INTRODUCTION

The following materials represent the current status of cyber-crime laws in the United States. By most estimates, cybercrime in the U.S. and around the world is on the rise, posing enormous threats to individuals, businesses and national security. Such threats run the gamut from simple Internet scams to complex cyber-attacks aimed at infiltrating military weapons systems. Not only is the threat wide-ranging, but the nature of cyber-crime itself is rapidly evolving, often keeping criminal behavior several steps ahead of detection technologies and the criminal laws designed to deter and punish.

Accordingly, developing laws to address the evolving nature of the cyber-crime threat is no easy task because the laws must define and confront existing criminal conduct while simultaneously anticipating the scope and direction of new challenges. As this report reveals, cyber-crime statutes in the U.S. are keeping pace in some areas, but lagging behind the escalating threat in other key areas.

(B) LEGISLATIVE PRACTICES AND LEGAL CONCEPTS

(1) How are criminal laws related to cyber-crimes codified in your country? Are they contained in a unified title or code or are they to be found in various codes or titles? (Please, provide appropriate citations).

Criminal laws related to cyber-crimes are contained in a variety of codes and titles in the United States. Generally, since the emergence of the first legislation regulating cyber-crimes in the late 1970's, laws in the U.S. have taken a tripartite approach to cyber-crime regulation. Specifically, there are statutes that criminalize the theft of computers or computer equipment as the *object* of the crime. Next, a variety of statutes outlaw direct attacks against computers, i.e. the computer is the *subject* of the crime. Finally, there are statutes designed to address criminal conduct that utilizes computers and other technological devices as *instruments* to carry out criminal activity.[1] Because most cyber-crime statutes contain provisions that overlap these three categories, this report will not separate the laws into those categories. Instead, the key federal cybercrime statutes are set forth below with brief parenthetical explanations discussing their provisions and coverage.

In addition, every state in the U.S. has some form of cyber-crime legislation. Those state statutes are cited in Appendix I.

---

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

* Professor of Law. Creighton University School of Law.

[1] *See* Carucci, Overhuls & Soares, Computer Crimes, 48 Am. Crim. L. Rev. 375, 378-81 (Spring 2011)

Major Federal Cyber-Crime Legislation

- **Controlling the Assault of Non-Solicited Pornography and Marketing** (also known as the "CAN-SPAM Act of 2003"), *15 U.S.C. §§ 7701-7713*. (This Act makes it unlawful to, among other things, "initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading.")

- **Digital Millennium Copyright Act** (DMCA), *17 U.S.C. §§1201-1205.* (This Act prohibits the circumvention of any technological device designed to limit access to copyrighted works. It also forbids the "manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component" designed for the purpose of circumventing copyright protection.)

- **Computer Fraud and Abuse Act**, *18 U.S.C. § 1030.* (This comprehensive Act prohibits a wide range of criminal conduct involving unauthorized access and/or transmission of data designed to cause damage to protected computers.)

- **PROTECT Act of 2003**,[2] *18 U.S.C. §§ 2252 & 2252A.* (This Act forbids the transmission and/or knowing receipt or reproduction of child pornography by computer.) A related statute, *18 U.S.C. § 1466A,* prohibits obscene visual representations of the sexual abuse of children.

- **Electronic Communications Privacy Act**, *18 U.S.C. 2510-2522.* (This Act prohibits the interception and disclosure of wire, oral, or electronic communications.)

- **Communications Decency Act**, *47 U.S.C. § 223.* (The Act forbids the transmission of obscene speech or child pornography to persons under 18 years of age.)

(2) What is the impact of judicial decisions on the formulation of criminal law related to cyber-crimes?

Judicial decisions have had a profound impact on criminal laws related to cyber-crimes in the United States. In particular, criminal laws that touch upon First Amendment values have been especially troublesome for the courts. For example, Congress passed the Child Pornography Prevention Act of 1996 (CPPA), which prohibited the production, transportation or receipt of child pornography. Two sections of the statute specifically prohibited images that "appear" to be or "convey the impression" that minors are engaged in sexually explicit conduct. In Ashcroft v. Free Speech Coalition, the United States Supreme Court determined that those provisions of the statute were overbroad, vague and could stifle works that had legitimate value.[3]

[2] PROTECT is the shortened term for "Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today"

[3] *See,* Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002). According to the Court, the CPPA "prohibit[ed] speech despite its serious literary, artistic, political, or scientific value. The statute proscrib[ed] the visual depiction of an idea–that of teenagers engaging in sexual activity–that is a fact of modern society and has been a theme in art and literature throughout the ages." *Id.* at 246.

United States Supreme Court decisions in the Fourth Amendment sphere have also helped to define (and in some cases confuse) the standards for legitimate expectations of privacy as related to computer technology. Typically, Fourth Amendment challenges are raised when the government searches and/or seizes technology devices (such as computers and cellular telephones) and when computer technology is used as a crime-fighting tool by law enforcement agencies (e.g. intercepting Internet communications or using GPS technology to track movements).[4]

(3) To catch up with changing needs and circumstances and to attain new objectives, some laws are subject to frequent amendment. Normally, such amendments take the form of new laws. In certain cases these new laws, instead of simply modifying the parts of the law that need to be changed, present the required amendments into a consolidated text together with all past amendments. This technique is called recasting. Is that how cyber-crime laws are updated and adapted to changed realities in your country? Please provide appropriate references and citations.

In the United States, cyber-crime legislation is frequently amended as new forms of criminality emerge or when the U.S. Supreme Court declares certain provisions of existing statutes unconstitutional. These amendments are typically added to current statutes (leaving the existing constitutional portions intact), or set forth in entirely new legislation (again, leaving existing constitutional statutes intact).

For example, cyber-bullying legislation has emerged as the new frontier of cyber-crime regulation. In 2009, the "Megan Meier Cyberbullying Prevention Act" was proposed as an amendment to 18 U.S.C. Chapter 41 (Extortion and Threats). The new amendment would have added Section 881, the Cyberbullying Prevention Act. Because 18 U.S.C. Chapter 41 already prohibits a variety of threatening and extortionate communications, the cyberbullying provision seemed a natural amendment to this existing statute. Section 881 would have criminalized transmitting communications "with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using electronic means to support severe, repeated, and hostile behavior."[5]

Another example of the "evolution" of a cyber-crime statute is the Computer Fraud & Abuse Act, 18 U.S.C. § 1030. According to Professor Ellen Podgor:

---

[4] *See, e.g.,* United States v. Jones, 565 US ___, 132 S.Ct. 945 (2012). In *Jones*, the Court grappled with the issue of whether attaching a GPS device to a vehicle violated the Fourth Amendment. The Court concluded that, under the circumstances of the *Jones* case, placement of the GPS device was a warrantless encroachment upon the defendant's legitimate expectation of privacy. What is perhaps more noteworthy about the *Jones* case is the recognition by several members of the Court that greater technological sophistication might need to be met with more comprehensive legislation. According to Justice Alito, "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken…. [But], [i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." *Id.* Alito, J, concurring in the judgment.

[5] Unfortunately, the Cyberbullying Prevention Act amendment was never enacted due to strong concerns about First Amendment rights and a sense that local authorities might be in a better position to address this emerging issue. Indeed, the debate surrounding the proposed legislation did, in fact, prompt many states to legislatively address the topic of cyberbullying.

> The Counterfeit Access Device and Computer Fraud and Abuse Act (1984, P.L. 98-473, 98 Stat. 2190) was the first piece of federal legislation to focus directly on computer abuses. Enacted on October 12, 1984, it provides federal prosecutors with a specific crime titled, "Fraud and related activity in connection with computers" to prosecute criminal computer activity. The act, which can be found in title 18, section 1030 of the United States Code, initially focused on improper computer access. Because it was extremely limited in the conduct it made criminal, amendments to the statute were forthcoming, including a significant amendment in 1986 that broadened its scope to include other forms of computer abuses, and a 1990 amendment that allowed civil actions to be brought under the statute. Section 1030 now criminalizes seven different types of computer activity. Although Congress has enacted other criminal statutes related to computers since 1984, section 1030 remains the key basis for prosecuting federal computer crimes.[6]

Indeed, the legislative history of 18 U.S.C. § 1030 is one in which "Congress has kneaded, reworked, recast, amended and supplemented [the statute] to bolster the uncertain coverage of the more general federal trespassing, threat, malicious mischief, fraud and espionage statutes."[7]

Finally, another example of the cyber-crime legislation amendment process is illustrated by the evolution of the Child Pornography Prevention Act (CPPA). As discussed in Question 2 above, the U.S. Supreme Court struck down two sections of the CPPA as unconstitutional in 2002.[8] To address the Court's concerns regarding actual minors versus visual depictions of minors, Congress enacted the PROTECT Act of 2003. This Act created 18 U.S.C. § 1466A, which prohibits visual depictions of minors or those that appear to be minors when such depictions are obscene or lack serious literary, artistic, political, or scientific value.[9] The PROTECT Act also amended 18 U.S.C § 2252A of the original CPPA to limit its prohibitions to *obscene* visual depictions of minors engaging in sexually explicit conduct or visual depictions of *actual* minors engaging in sexually explicit conduct.

(C) THE SPECIFIC CYBERCRIME OFFENSES

(1) Concerning mens rea, must cybercrime offenses be intentional? Do they require a specific intent?

Most conduct under the **Computer Fraud and Abuse Act** must be committed intentionally. *See*, 18 U.S.C. § 1030. To act intentionally within the meaning of this statute, one must purposefully accomplish the proscribed act. Thus, the actor must act with specific intent to commit the crime.

---

[6] Ellen S. Podgor, Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, in Major Acts of Congress (Brian K. Landsberg ed., Macmillan Reference USA, 2004).
[7] Doyle, Charles, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, Congressional Research Service 1 (December 27, 2010).
[8] *See supra* note 2 and accompanying text.
[9] This new statute directly addressed the Court's concern that the prior law might chill speech that had serious literary, artistic, political, or scientific value.

Examples:

18 U.S.C. §1030(a)(2):

Whoever---

(2) ***intentionally*** accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) [1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer

18 U.S.C. §1030(a)(3):

Whoever---

intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States

18 U.S.C. §1030(a)(7):

Whoever---

(7) with ***intent*** to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

However, some criminal conduct may be accomplished if the actor committed the act ***knowingly***. *See* 18 U.S.C. §§1466A and 2252A. Pursuant to these statutes, ***knowingly*** connotes a conscious awareness of the natural consequences of one's actions.

Examples:

18 U.S.C. §1466A:

Any person who…***knowingly*** produces, distributes, receives, or possesses with intent to distribute, a visual depiction of any kind, including a drawing, cartoon, sculpture, or painting, that—

(1)

(A) depicts a minor engaging in sexually explicit conduct; and

(B) is obscene; or

(2)

(A) depicts an image that is, or appears to be, of a minor engaging in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; and

(B) lacks serious literary, artistic, political, or scientific value;

or attempts or conspires to do so, shall be subject to the penalties provided in section 2252A (b)(1), including the penalties provided for cases involving a prior conviction.

18 U.S.C. §2252A

(a) Any person who—

(1) ***knowingly*** mails, or transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography;

(2) ***knowingly*** receives or distributes—

(A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or

(B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

(3) ***knowingly***—

(A) reproduces any child pornography for distribution through the mails, or using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer; or

(B) advertises, promotes, presents, distributes, or solicits through the mails, or using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any material or purported material in a manner that reflects the belief, or that is intended to cause another to believe, that the material or purported material is, or contains—

(i) an obscene visual depiction of a minor engaging in sexually explicit conduct; or

(ii) a visual depiction of an actual minor engaging in sexually explicit conduct;

(2) Are there also negligent offenses in this field?

Generally speaking, criminal liability on the basis of negligent conduct is frowned upon in U.S. penal law. When negligence is the basis for criminal liability, there usually must be a very high degree of negligence, i.e., typically ordinary negligence will not suffice. Having said that, there is one portion of 18 U.S.C. § 1030 that requires a dual intent to commit the prohibited behavior. One of those intents encompasses negligent behavior. *See* 18 U.S.C. § 1030 (a)(5)(C)

(3) If yes, please, provide a list of those offenses.

18 U.S.C. § 1030 (a)(5)(C) prohibits:

"intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss."

As the terms of the statute indicate, the initial access must be intentional, but the subsequent damage may be caused negligently or accidentally. Thus, while negligence is a basis for liability under this section of the statute, it is a corollary to intentional conduct.

(a) Integrity and functionality of the IT system

1. Illegal access and interception of transmission

a. Object – system or data?

Does your criminal law establish as a criminal offense the serious hindering, without right, of the functioning of a computer and/or electronic system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing information or data from a computer system, software or program?

Yes. **18 U.S.C. § 1030 (a)(5)** prohibits:

(A) knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer;

(B) intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage; or

(C) intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss.

b. Requirement of infringement of security measures?

Is it a requirement of your criminal law that the hacker conduct the hack of the computer system by using one or more software needed to defeat security measures and gain entry-level or higher level of access?

No. The conduct portion of the statute is satisfied when the person accesses the computer system without authorization or exceeds authorized access. The term "exceeds authorized access" is defined as "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter." 18 U.S.C. §1030(e)(6). People who exceed authorized access are generally "insiders" within an organization who have some degree of authorized access to the computer system. While there is no specific definition in the statute of the term "without authorization," it has been interpreted to apply to "outsiders" who have absolutely no right to access the computer system.

2. Data and system interference

a. Object – protection of system/hardware/data?

Does your criminal law define "computer and/or electronic data"? Does this definition include programs or software or similar coding? If you have a definition, please provide it and the reference to the related paragraphs/articles of your code.

Pursuant to **18 U.S.C. § 1030 (e)(1)** the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

b. Act – destruction/alteration/rendering inaccessible?

i. Does your penal law penalize the unauthorized erasure, alteration, rendering inaccessible, acquiring or other similar interference with information or data from a computer or electronic system or program?

Yes. **18 U.S.C. § 1030 (a)(5)(A)** prohibits "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer." Pursuant to **18 U.S.C. § 1030 (e)(8)**, "the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information."

ii. Does your penal law penalize the unauthorized interception of the transmission in any manner or mode of computer or electronic data and/or information?

Yes. See response to **2(b)(i)** above. See also **18 U.S.C. § 2511(a)**, which prohibits the interception and disclosure of wire, oral, or electronic communications. The statute provides, in pertinent part, that criminal liability will be imposed up any person who:

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.

The term "*intercept*" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. **18 U.S.C. § 2510(4)**

The term "*electronic communication*" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) any wire (telephone) or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

18 U.S.C. § 2510(12)

3. Data Forgery

a. Object – authenticity?

Does your penal law define as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data resulting in inauthentic data in order to protect the authenticity of the data to be used or acted upon for legal purposes? If you have a definition, please provide it along with the reference to the related paragraphs/articles of your code and/or special statutes.

Yes. **18 U.S.C. § 1030 (a)(5)(A)** prohibits "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer." Pursuant to **18 U.S.C. § 1030 (e)(8)**, "the term 'damage' means any impairment to the **integrity** or availability of data, a program, a system, or information."

In addition, some states have developed specific computer forgery statutes. For example:

Georgia – Computer forgery statute §16-9-93(d) provides that:

Any person who creates, alters, or deletes any data contained in any computer or computer network, who, if such person had created, altered, or deleted a tangible document or instrument would have committed forgery under Article 1 of this chapter, shall be guilty of the crime of computer forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to the crime of computer forgery if a creation, alteration, or deletion of data was involved in lieu of a tangible document or instrument.

b. Act – alteration/deletion?

Does your penal law penalize as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data/information resulting in inauthentic data/information with the intent that it be considered or acted upon for legal purposes as if it were authentic? If yes, please provide the reference to the applicable paragraphs/articles of your code.

Yes. **See 3(a)** above.

4. Misuse of Devices

a. Object – type of device?

Does your criminal law criminalize the development of a hacker's "tool kit" or any part of it (e.g. password grabbers and key loggers, blue boxing programs, war-dialers, encryption software, program password crackers, security vulnerability scanners, packet sniffers etc.) for the unauthorized access to computer or electronic systems or transmissions?

Yes, but only in a very limited way. **18 USC § 2512(1)(b)** prohibits the manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices. For purposes of this statute, "intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." To be liable under this statute, the person must know or have reason to know "that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications."

The lack of more specific regulation of hacker's toolkits or "cyberweapons" is likely attributable to the widespread use of many of those same devices by "ethical hackers," i.e. those who use toolkits to test the vulnerabilities within their own computer systems. In lieu of such regulation, the focus in the U.S. appears to be on developing effective security countermeasures to hacking and increasing public awareness about the ongoing risks to the privacy and integrity of computers and electronic data.

b. Act – public distribution/transfer to another person?

i. Does your criminal law penalize the unauthorized use of any of the hacker's tools listed above under a?

Yes, but only in a very limited way.

18 USC § 2511(1)(b) imposes criminal liability on any person who:

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce.

Pursuant **18 U.S.C. §2510(5)**, *electronic device* means:

any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than—

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof,

(i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or

(ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties.

*Because there are currently no specific laws addressing the use of hacking toolkits, prosecutors are encouraged to use the provisions set forth above whenever a case involves spyware users and manufacturers, intruders using packet sniffers, persons improperly cloning email accounts, or any other surreptitious collection of communications from a victim's computer.[10]

ii. Does your criminal law penalize the public distribution and/or transfer to other parties of hacked electronic information?

Yes. **18 USC § 2511 (1) (c)** imposes criminal liability upon any person who intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.

c. Possession?

Does your criminal law criminalize the possession of a hacker's "tool kit" or any part of it (e.g. password grabbers and key loggers, blue boxing programs, war-dialers, encryption software, program password crackers, security vulnerability scanners, packet sniffers etc.) for the unauthorized access to computer or electronic systems or transmissions?

Yes. **See response 4 (a)** above.

(b) Privacy

1. Violation of Secrecy of Private Data

a. Object – type of private data?

(Note: private data are data that belong to people's private life but do not identify or make it possible to identify a person, e.g., civil status, sexual orientation, health status, buying habits or preferences)

[10] See *Prosecuting Computer Crimes*, Computer Crime and Intellectual Property Section Criminal Division, published by Office of Legal Education Executive Office for United States Attorneys. http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf

i. Do your country's laws require that data collectors disclose their information practices before collecting private information from consumers like, for example, which information is used, how it is collected and for what purpose, whether it is shared with others and whether consumers have any control over the disclosure of their private data?

While there is no comprehensive statute covering all instances of private data collection, use and sharing, several statutes address this issue.

For example, the **Children's Online Privacy Protection Act (COPPA) 15 U.S.C. § 6501-6506**, regulates activities on websites that knowingly collect information about or target children under the age of 13. Pursuant to **15 U.S.C. § 6502(b)**, operators of any website or online service directed to children that collect personal information from children or operators of any website or online service that has actual knowledge that it is collecting personal information from a child are required:

(i) to provide notice on the website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information; and

(ii) to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children.

The regulations set forth in **15 U.S.C. § 6502(b)** also:

(B) require the operator to provide, upon request of a parent under this subparagraph whose child has provided personal information to that website or online service, upon proper identification of that parent, to such parent—

(i) a description of the specific types of personal information collected from the child by that operator;

(ii) the opportunity at any time to refuse to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child; and

(iii) notwithstanding any other provision of law, a means that is reasonable under the circumstances for the parent to obtain any personal information collected from that child;

(C) prohibit conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and

(D) require the operator of such a website or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

Another privacy statute, the **Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809**, provides that a financial institution must establish appropriate safeguards:

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

According to the statute, "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."

In terms of disclosure obligations, **15 U.S.C. §6803(a)** provides that:

At the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship, a financial institution shall provide a clear and conspicuous disclosure to such consumer, in writing or in electronic form or other form permitted by the regulations…of such financial institution's policies and practices with respect to—

(1) disclosing nonpublic personal information to affiliates and nonaffiliated third parties…including the categories of information that may be disclosed;

(2) disclosing nonpublic personal information of persons who have ceased to be customers of the financial institution; and

(3) protecting the nonpublic personal information of consumers.

Pursuant to **15 U.S.C. § 6803(c)**, such disclosure must include:

(1) the policies and practices of the institution with respect to disclosing nonpublic personal information to nonaffiliated third parties, other than agents of the institution

(A) the categories of persons to whom the information is or may be disclosed, other than the persons to whom the information may be provided pursuant to section 6802 (e) of this title; and

(B) the policies and practices of the institution with respect to disclosing of nonpublic personal information of persons who have ceased to be customers of the financial institution;

(2) the categories of nonpublic personal information that are collected by the financial institution;

(3) the policies that the institution maintains to protect the confidentiality and security of nonpublic personal information.

Finally, the **Health Insurance Portability and Accountability Act (HIPAA) Privacy Rules, 45 C.F.R. Part 160**, regulate the use and disclosure of *protected health information*. Pursuant to the HIPAA regulations, "protected health information" is defined as "any individually identifiable health information." Further, "identifiable refers not only to data that is explicitly linked to a particular individual…[i]t also includes health information with data items which reasonably could be expected to allow individual identification."

Because HIPAA is primarily concerned with *individually identifiable information* it does not appear to meet the definition of "private data" as set forth in the question. Accordingly, the HIPAA provisions will not be discussed in any detail.[11]

[11] However, HIPAA's Privacy Rule does make provisions for a "limited data set," authorized only for public health, research, and health care operations purposes. A limited data set must have all direct identifiers removed, including, among other things, name and social security number, street address, e-mail address, telephone and fax numbers, full face photos and any other comparable images and medical record numbers, health plan beneficiary numbers, and other account numbers. Disclosure of information in the limited data set must be conditioned upon execution of a "data use agreement," which establishes the permitted uses and disclosures of such

ii. Do your country's laws require companies and entities doing business on the internet to inform consumers of the identity of who is collecting the data, if the provision of the requested data is voluntary or required and the steps taken by the data collector to ensure the confidentiality, the integrity and the quality of the data?

Yes. **15 U.S.C § 6502(b)** (see previous question for text of statute); and **15 U.S.C § 6803(a) and (c)** (see previous question for text of statute)

iii. Do your country's laws require websites to display a privacy policy and explain how personal information will be used before consumers enter the purchase process or any other transaction for which they must provide sensitive information?

Yes, see **15 U.S.C § 6502(b)** above.

iv. Does the criminal law of your country penalize failing to provide the disclosures mentioned above (a.i; a.ii and a.iii)?

No, there do not appear to be criminal penalties for failure to provide the disclosures set forth above.

b. Act – illegal use and transfer/distribution?

i. Does the criminal law of your country define the illegal transfer and distribution of private data?

No. However, if private information is transferred illegally, those suffering harm may bring civil actions.

ii. Does the criminal law of your country penalize the illegal use, transfer and/or distribution of private data?

No. However, if an entity is found civilly liable for the illegal use, transfer or distribution of private data, monetary damages may be imposed to compensate victims.

c. Justification?

i. Under which conditions does your country's law allow for the authorized collection, processing, transfer and distribution of private data?

Children's Online Privacy Protection Act (COPPA)

Information may be collected with the consent of the parent. See **15 USC § 6502(b)** However, some circumstances do not require consent. Pursuant to **15 U.S.C. §6502(b)(2)**, consent is not required if:

(A) online contact information collected from a child that is used only to respond directly on a one-time basis to a specific request from the child and is not used to recontact the child and is not maintained in retrievable form by the operator;

(B) a request for the name or online contact information of a parent or child that is used for the sole purpose of obtaining parental consent or providing notice under this section and where such information is not maintained in retrievable form by the operator if parental consent is not obtained after a reasonable time;

---

information by the recipient, consistent with the purposes of research, public health, or health care operations, limits who can use or receive the data, and requires the recipient to agree not to re-identify the data or contact the individuals.

(C) online contact information collected from a child that is used only to respond more than once directly to a specific request from the child and is not used to recontact the child beyond the scope of that request—

(i) if, before any additional response after the initial response to the child, the operator uses reasonable efforts to provide a parent notice of the online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the operator make no further use of the information and that it not be maintained in retrievable form; or

(ii) without notice to the parent in such circumstances as the Commission may determine are appropriate, taking into consideration the benefits to the child of access to information and services, and risks to the security and privacy of the child, in regulations promulgated under this subsection;

(D) the name of the child and online contact information (to the extent reasonably necessary to protect the safety of a child participant on the site)—

(i) used only for the purpose of protecting such safety;

(ii) not used to recontact the child or for any other purpose; and

(iii) not disclosed on the site,

if the operator uses reasonable efforts to provide a parent notice of the name and online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the operator make no further use of the information and that it not be maintained in retrievable form; or

(E) the collection, use, or dissemination of such information by the operator of such a website or online service necessary—

(i) to protect the security or integrity of its website;

(ii) to take precautions against liability;

(iii) to respond to judicial process; or

(iv) to the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety.

The Gramm-Leach-Bliley Act

Financial institutions may disclose nonpublic personal information only after providing notice to its customers and allowing an opportunity to opt out. **15 U.S.C. §6802(a) and (b)** However, there are several exceptions to this requirement. Pursuant to **15 U.S.C. § 6802(e):**

(e) General exceptions

Subsections (a) and (b) of this section shall not prohibit the disclosure of nonpublic personal information—

(1) as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with—

(A) servicing or processing a financial product or service requested or authorized by the consumer;

(B) maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or

(C) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer;

(2) with the consent or at the direction of the consumer;

(3)

(A) to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein;

(B) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;

(C) for required institutional risk control, or for resolving customer disputes or inquiries;

(D) to persons holding a legal or beneficial interest relating to the consumer; or

(E) to persons acting in a fiduciary or representative capacity on behalf of the consumer;

(4) to provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors;

5) to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 [12 U.S.C. 3401 et seq.], to law enforcement agencies, a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;

(6)

(A) to a consumer reporting agency in accordance with the Fair Credit Reporting Act [15 U.S.C. 1681 et seq.], or

(B) from a consumer report reported by a consumer reporting agency;

(7) in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or

(8) to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.

ii. What standard of need is required for an authorized collection and/or distribution (compelling, important, reasonable, convenient)?

The standards of need appear to fall into the two categories of compelling (as in the case of compliance with a subpoena) and/or necessary (to protect the security or integrity of the website).

2. Violation of professional confidentiality

a. Object – type of private data?

i. Do your country's laws require that professionals disclose:

- Their information collection and management practices before collecting personal information from their patients or clients;

Yes, medical and legal professionals must advise patients and clients of their collection and management practices related to personal information.

In the medical arena, doctors have an ethical obligation arising from the American Medical Association Code of Ethics to maintain strict confidentiality with respect to information revealed as part of the doctor/patient relationship. State laws and regulations that create legal obligations buttress this ethical obligation. In addition, HIPAA, a federal law, now provides mandatory patient confidentiality standards for certain protected health information. Patients must be advised of these confidentiality standards.

Lawyers are also bound by ethical obligations arising from the American Bar Association Model Rules and Standards to maintain strict confidentiality with respect to information revealed as part of the attorney/client relationship. In addition, case law and state regulations govern the protection and management of information disclosed during the attorney/client relationship.

- *Their disclosure practices;*

Yes.

- *Their professional ethical obligations;*

Yes.

- *And whether patients or clients have any control over the disclosure of their personal data?*

Yes.

ii. Which data are specifically protected, if any?

In the medical arena, medical information revealed by a patient or discovered by a physician in connection with the treatment of a patient is subject to the strictest confidentiality requirement.

In the legal arena, the confidentiality protection applies to matters communicated in confidence by the client and to all information related to the representation (regardless of whether it came from the client or from another source).

iii. Does your country's penal law allow or even require clinicians, lawyers, priests, etc. to breach the confidentiality in certain situations or for certain reasons established by law? Under which standards would that be done? (e.g. reasonable cause to believe that there is abuse vs. seeing an abused child, women, elderly)?

Yes, confidentiality may be breached under certain circumstances.

According to the American Medical Association, medical personnel may breach confidence when it is:

…ethically and legally justified because of overriding social considerations. If there is a reasonable probability that a patient will inflict serious bodily harm on another person, for example, the physician should take precautions to protect the intended victim and notify law enforcement authorities. Communicable diseases and gunshot and knife wounds should be reported as required by applicable statutes or ordinances. Thus, the physician's duty of confidentiality at times must give way to a stronger countervailing societal interest.[12]

In the legal field:

The exceptions to the confidentiality rule vary somewhat from state to state and reflect different weightings of the balancing process between the several societal goals involved. Most jurisdictions make a specific exception in their ethics rules to permit disclosure that will prevent death or substantial bodily injury. In addition, the ethics rules in most jurisdictions permit and sometimes require a lawyer to disclose information in order to prevent and/or rectify the consequences of a crime or fraud that injures the financial or property interests of another.[13]

b. Subject – Type of perpetrators?

Does the criminal law of your country identify the categories of professionals who are bound by specific confidentiality rules?

Generally, no, with the exception of the HIPAA statutes that punish "covered entities" for disclosing a patient's personally identifiable health information for purposes other than treatment, payment or health care oversight.

c. Act – illegal use and transfer/distribution?

Which acts (e.g. illegal collection, use, transfer and distribution) are specifically penalized by your country's criminal law?

HIPAA 42 USC § 1320d–6 - Wrongful disclosure of individually identifiable health information

(a) Offense

A person who knowingly and in violation of this part—

---

[12] http://www.ama-assn.org/ama/pub/physician-resources/legal-topics/patient-physician-relationship-topics/patient-confidentiality.page

[13] Confidentiality, Privilege: A Basic Value in Two Different Applications. By Sue Michmerhuizen http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/confidentiality_or_attorney.authcheckdam.pdf
The "crime-fraud exception" was established in Clark v. United States, 289 U.S. 1 (1933) (holding that attorneys are required to disclose confidential client information and/or communications to the court when necessary to prevent the client from abusing the attorney-client relationship by using as a means to facilitate criminal activity).

(1) uses or causes to be used a unique health identifier;

(2) obtains individually identifiable health information relating to an individual; or

(3) discloses individually identifiable health information to another person,

shall be punished as provided in subsection (b) of this section. For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation described in section 1320d–9 (b)(3) of this title) and the individual obtained or disclosed such information without authorization.

*Again, it is important to note that HIPAA regulations only apply to *individually identifiable health information*, which may not meet the definition of personal or private data as contemplated by these questions.

3. Illegal processing of personal and private data

a. Object?

Does your criminal law penalize the illegal and unauthorized acquisition, processing, storage, analysis, manipulation, use, sale, transfer etc. of personal and private data?

Yes, but only in the limited circumstances identified in 2(c) above.

b. Subject?

Does your criminal law identify specifically the categories of persons and entities included in this criminal prohibition and sanctions?

Yes. See 2(c) above.

c. Act?

i. Does your criminal law penalize specific acts that constitute all or part of the illegal processing of personal and private data? Reply for each category listed below citing the relevant law and its provisions, if available:

1. Illegal collection Yes. See 2(c) above.

2. Illegal use Yes. See 2(c) above.

3. Illegal retention No.

4. Illegal transfer Yes. See 2(c) above.

ii. Does it make a difference if these personal and private data are used, transferred etc. for police or law enforcement purposes?

Yes. Personal or private data may be disclosed when complying with a court order, subpoena, or summons; when responding to an administrative subpoena, investigative demand, or other administrative request; for a proceeding before a health oversight agency; and for law enforcement purposes.

d. Justification?

i. Under which conditions does your country's law allow for the authorized collection, processing, transfer and distribution of personal and private data?

Typically, collection, processing, transfer and distribution of information may only be done with the consent of the client and/or patient. However, under some circumstances (as identified in 3(c)(ii) above), consent will not be necessary.

ii. What standard of need is required for an authorized collection and/or distribution of personal and private data (compelling, important, reasonable, convenient)?

The need must be compelling as in complying with a court order, subpoena or law enforcement investigative demand.

4. Identity theft

(Note: identity theft occurs when someone appropriates another's personal information without his or her knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business or entity, sometimes as a response to an e-mail solicitation to update billing or membership information, or as an application for a fraudulent Internet job posting or loan.)

a. Object

i. Does your criminal law penalize identify theft? Please, cite the relevant law.

Yes. **18 USC § 1028** - Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information.

ii. Does your criminal law proscribe specific forms of identity theft, like phishing, for example? Phishing is defined as a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent websites which attempt to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc.

No, but phishing conduct is covered by the parameters of the identity theft statute.

18 U.S.C. §1028(a)(7) prohibits: knowingly transfer[ing], possess[ing], or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law

The terms "means of identification" is defined in **18 U.S.C. §1028(d)(7)**:

(7) the term "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—

(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(C) unique electronic identification number, address, or routing code; or

(D) telecommunication identifying information or access device (as defined in section 1029 (e))

b. Subject

Does your criminal law contain penal responsibility connected to a person's digital personality, or to his/her Avatar, or to his/her digital role in an Internet based simulation game (e.g. Cityville, Farmville, etc.)? Please cite the relevant law.

There is no specific law covering "virtual crime." The traditional criminal law comes into play when the conduct involves "real-world" criminal behavior (such as theft, assault, harassment, etc.) committed while using technological devices and/or digital identities.

(c) Protection Against Illegal Content: ICT Related

1. Object

a. Child pornography - images of real or virtual children?

i. Does your penal law criminalize the use of the Internet for the purpose of storing, accessing, and disseminating child pornography? If so, please, cite the relevant law.

PROTECT Act of 2003, 18 U.S.C. § 2252A. This Act forbids the transmission, knowing receipt or reproduction of child pornography by computer. A related statute, **18 U.S.C. § 1466A**, prohibits obscene visual representations of the sexual abuse of children.

ii. In particular, does your criminal law:

- *Create a new offense that targets criminals who use the Internet to lure and exploit children for sexual purposes?*

18 U.S.C. §2422(b) provides that:

Whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title and imprisoned not less than 10 years or for life.

*While the statute is not "new" and does not specifically mention the Internet, its reference to "any facility or means of interstate or foreign commerce" is broad enough to encompass Internet activity.

- *Make it a crime:*

1. to transmit,

2. make available,

3. export

4. and intentionally access child pornography on the Internet

Yes. **18 U.S.C. §2252A** provides criminal liability for the following behavior:

(a) Any person who—

(1) knowingly mails, or transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography;

(2) knowingly receives or distributes—

(A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or

(B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

(3) knowingly—

(A) reproduces any child pornography for distribution through the mails, or using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer; or

(B) advertises, promotes, presents, distributes, or solicits through the mails, or using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any material or purported material in a manner that reflects the belief, or that is intended to cause another to believe, that the material or purported material is, or contains—

(i) an obscene visual depiction of a minor engaging in sexually explicit conduct; or

(ii) a visual depiction of an actual minor engaging in sexually explicit conduct;

…

(5) (B) knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

- *Allow judges to order the deletion of child pornography posted on computer systems in your country*

There is no particular statutory provision that allows judges to order deletion of child pornography on the Internet. However, judges do have discretion when fashioning remedies in criminal cases.

- *Allow a judge to order the forfeiture of any materials or equipment used in the commission of a child pornography offense*

Yes, under **18 USC § 2253 - Criminal forfeiture**

- *Criminalize:*

1. Knowingly accessing child pornography on the Internet

2. Transmitting child pornography on the Internet

3. Exporting child pornography on the Internet

4. Possessing child pornography on the Internet for the purpose of, e.g., transmitting, exporting it…?

Yes, to all of the above. See **18 U.S.C. §2252A** set forth above.

iii. Does your criminal law penalize the online solicitation of children for sexual purposes via social networking websites and chat rooms?

Yes. **18 USC § 2422 - Coercion and enticement**

iv. Is the definition of child pornography in your criminal code close to that contained in international instruments (e.g. EU Directives)?

Yes, the definitions are strikingly similar in coverage.

- **USA**

18 U.S.C. §2256(8) provides:

(8) "child pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where—

(A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

(B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

(C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

18 U.S.C. §2256(2)(B) provides:

"[S]exually explicit conduct" means—

(i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited;

(ii) graphic or lascivious simulated;

(I) bestiality;

(II) masturbation; or

(III) sadistic or masochistic abuse; or

(iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person;

- **The Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography is a protocol to the Convention on the Rights of the Child**

"Child pornography" is any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.

- **EU Directive**

"child pornography" means:

(i) any material that visually depicts a child engaged in real or simulated sexually explicit conduct;

(ii) any depiction of the sexual organs of a child for primarily sexual purposes;

(iii) any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or

(iv) realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes;

v. Is secondary victimization avoided for victims of child pornography in your penal law? In States where prostitution or the appearance in pornography is punishable under national criminal law, it should be possible not to prosecute or impose penalties under those laws where the child concerned has committed those acts as a result of being victim of sexual exploitation or where the child was compelled to participate in child pornography. Is this what your criminal law contemplates?

Yes. In fact, there is a growing trend to allow restitution from defendants to victims of child pornography.[14]

vi. Does your criminal law criminalize "virtual child" pornography? "Virtual child" pornography does not use real children or images of real identifiable children. When the image is not that of a real child, but a combination of millions of computer pixels crafted by an artist, can the government in your country ban this allegedly victimless creation? Please cite the applicable law and/or court decisions.

Yes, but the virtual depiction must be obscene or lack serious literary, artistic, political, or scientific value.

18 USC § 1466A imposes criminal liability upon:

(a) Any person who…knowingly produces, distributes, receives, or possesses with intent to distribute, a visual depiction of any kind, including a drawing, cartoon, sculpture, or painting, that—

(2)

[14] See, e.g., In re Amy Unknown, http://www.ca5.uscourts.gov/opinions%5Cpub%5C09/09-41238-CV2.wpd.pdf

(A) depicts an image that is, or appears to be, of a minor engaging in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; ***and***

(B) lacks serious literary, artistic, political, or scientific value.

vii. Mens rea: To be liable, the person should both intend to enter a site where child pornography is available and know that such images can be found there. Penalties should not be applied to persons inadvertently accessing sites containing child pornography. Are these the requirements of your criminal law?

Yes. The person must "knowingly access with intent to view" child pornography. **18 U.S.C. § 2252A(a)(5)(B)**

b. Any other object where criminalization depends on the use of Information & Communication Technologies (ICT)

Does your criminal law penalize the following conducts? Please cite the relevant law.

1. creation and use of true anonymity sending and/or receiving material on the ICT?

No.

2. cyber-bullying?

Yes. There is currently no federal cyberbullying law. Below is a sampling of state statutes that criminalize harassing/intimidating youth online:

- Arkansas

Ark. Code § 5-27-306 (2005) (criminalizes Internet stalking of a child.)

- Idaho

Idaho Code Ann. § 18-917A (2006) (statute criminalizing peer-on-peer bullying.)

Idaho Code Ann. § 18-7905 (2004) (criminalizes stalking, including adults stalking minors.)

- Kentucky

KRS 525.080 (2008) (prohibits intimidation or harassment of students via the Internet)

- Minnesota

Minn. Stat. § 609.749, subdivision 1 (1), (2) (2007) (prohibits threatening or intimidating behavior via electronic communications)

- Missouri

Mo. Rev. Stat. § 565.225 (2008) (prohibits frightening, intimidating, or emotionally distressing conduct by any means of communication)

- North Carolina

N.C. Gen. Stat. § 14□458.1 (2009) (targets student-on-student bullying behavior online)

- South Dakota

S.D. Cod. Laws §§ 22-19A-1, 22-19A-7 (2006) (prohibits threatening or intimidating behavior via electronic communications)

- Tennessee

Tenn. Code § 39-17-315 (2005) (prohibits threatening or intimidating behavior via electronic communications)

3. cyber-stalking?

18 U.S.C. §875 (prohibits threatening and extortion related interstate communications)

47 U.S.C. §223 (prohibits obscene or harassing communications by telephone or telecommunications devices)

Additionally, several states have enacted cyberstalking statutes.

4. cyber-grooming?

18 U.S.C. § 2422 prohibits using the mail or any facility or means of interstate or foreign commerce…to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity.

18 U.S.C. § 2425 prohibits transmitting information about a minor using the mail or any facility of interstate or foreign commerce with the intent to entice, encourage, offer, or solicit any person to engage in any sexual activity.

2. Act - creation/accession/possession/transfer/public distribution by ICT (give examples)

Cite specific laws that criminalize the creation (even if never used), the accession, the possession (even if only in private), the transfer, and the public distribution through the internet and other electronic means of materials beside those already mentioned above, specifically because of internet/electronic technology use.

None.

(d) ICT Related Violations of Property, Including Intellectual Property

Does your criminal law specifically proscribe and penalize the following conducts perpetrated through the use of the ICT? Please, cite the relevant law.

1. Fraud

18 USC § 1030 - Fraud and related activity in connection with computers

2. Infringement of Intellectual Property IP rights

17 USC § 506 - Criminal offenses (criminal infringement of copyright)

18 USC § 2320 - Trafficking in counterfeit goods or services

18 USC § 1832 - Theft of trade secrets

3. Industrial espionage

18 USC § 1831 - Economic espionage

(e) Criminalization of Acts Committed in the Virtual World

Does your criminal law penalize the commission of crimes committed in the virtual world like, for example, virtual child pornography, virtual violence, virtual graffiti, cyber-defamation, sexual harassment, harassment at work, without any involvement of real persons, only virtual representation? Please cite the relevant law and provide details.

No, with the exception of virtual child pornography, which is punished criminally if it lacks serious literary, artistic, political, or scientific value. **18 USC § 1466A**

(f) Non-Compliance Offenses

Does your criminal law penalize non-cooperation with law enforcement agencies in the field of cybercrime? Duties to cooperate can be duties to retain and store information, to produce/deliver information as required by a production order, to give access to cyber systems to install filters or devices, etc. Is the breach of the duty to cooperate also enforced through administrative sanctions? Cite the relevant law and provide details.

18 USC § 2257 - Record keeping requirements (provides criminal penalties for failure to maintain records related to the production of sexually explicit materials)

In most other instances, law enforcement must present a subpoena or warrant to obtain information or to access cyber systems. Penalties for failing to comply with court orders can range from civil contempt to arrest, imprisonment and fines.

See, for example:

18 USC § 401 - Power of court

A court of the United States shall have power to punish by fine or imprisonment, or both, at its discretion, such contempt of its authority, and none other, as—

(1) Misbehavior of any person in its presence or so near thereto as to obstruct the administration of justice;

(2) Misbehavior of any of its officers in their official transactions;

(3) Disobedience or resistance to its lawful writ, process, order, rule, decree, or command

28 USC § 1826 - Recalcitrant witnesses

(a) Whenever a witness in any proceeding before or ancillary to any court or grand jury of the United States refuses without just cause shown to comply with an order of the court to testify or provide other information, including any book, paper, document, record, recording or other material, the court, upon such refusal, or when such refusal is duly brought to its attention, may summarily order his confinement at a suitable place until such time as the witness is willing to give such testimony or provide such information. No period of such confinement shall exceed the life of—

(1) the court proceeding, or

(2) the term of the grand jury, including extensions,

before which such refusal to comply with the court order occurred, but in no event shall such confinement exceed eighteen months.

(D) COMPLEMENTARY OPTIONAL INFORMATION CONCERNING LAW AND PRACTICE (INCLUDING STATISTICS)

(1) Are cybercrimes included as such in the collection of data on crime in your country?

No. http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2010/crime-in-the-u.s.-2010/offenses-known-to-law-enforcement

(2) Is there in your country a website that provides data and information on the occurrence, seriousness, cost, impact etc. of cyber-crimes in your country? If "yes", provide the website electronic address.

(a) http://www.fbi.gov/about-us/investigate/cyber/cyber

(b) http://www.ic3.gov/default.aspx

(3) Do victimization surveys in your country include questions on cyber-crimes?

Yes. http://www.bjs.gov/index.cfm?ty=tp&tid=41

(4) What types of computer crime / computer fraud are most often reported in your country?

During 2011, FBI-related scams (scams in which the criminal poses as the FBI to defraud victims) were the most reported offense, followed by identity theft and advance fee fraud.[15]

(5) Do law enforcement and prosecution in your country have a computer crimes unit? If so, how many officers/prosecutors are in it?

Yes.

Department of Justice: http://www.justice.gov/criminal/cybercrime/

FBI: http://www.fbi.gov/about-us/investigate/cyber/cyber (collaborative effort with other federal/state agencies and cyber experts)

(6) Does your or any law school in the country offer courses on cyber-crime? Please provide a website address.

A sampling of U.S. Law Schools:

New York Law School: http://www.nyls.edu/academics/catalog_and_schedule/alpha_list/cybercrime_cyberterror_and_digital_law_enforcement/

Lewis & Clark Law School:

https://law.lclark.edu/courses/catalog/law_487.php

Harvard:

[15] IC3 2011 Internet Crime Report, http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf

http://isites.harvard.edu/icb/icb.do?keyword=k74559&pageid=icb.page372431&pageContentId=icb.pagecontent844609&state=maximize

Columbia:

http://www.law.columbia.edu/courses/L9327-internet-and-computer-crimes

Chicago:

http://www.law.uchicago.edu/node/3878/courses

Pennsylvania:

https://www.law.upenn.edu/cf/institutes/claw/courses.cfm

Virginia:

http://www.law.virginia.edu/html/academics/ip/ipcourses.htm

Colorado:

http://lawweb.colorado.edu/courses/courseSection.jsp?id=LAWS6321&term=20117#section_001

North Carolina:

http://www.law.unc.edu/academics/courses/computercrimew/

Georgetown:

http://apps.law.georgetown.edu/curriculum/tab_courses.cfm?Status=Course&Detail=764

Widener:

http://law.widener.edu/Academics/Institutes/AdvocacyandTechnologyInstitute/CriminalLawCertificate.aspx

George Washington:

http://law.widener.edu/Academics/Institutes/AdvocacyandTechnologyInstitute/CriminalLawCertificate.aspx

John Marshall:

https://courses.jmls.edu/Lists/Courses/CustomDispForm.aspx?ID=330&InitialTabId=Ribbon.Read

Washington College of Law

http://www.wcl.american.edu/registrar/coursesapp/inf_course.cfm?number=LAW-836-001&time=spring_2011&srchtxt=ALL

Fordham:

http://www.wcl.american.edu/registrar/coursesapp/inf_course.cfm?number=LAW-836-001&time=spring_2011&srchtxt=ALL

Cooley:

http://www.cooley.edu/prospective/_docs/courses.pdf

Mississippi:

http://www.olemiss.edu/depts/ncjrl/CyberCrimeInitiative/cci_gi.html

Cleveland Marshall

https://www.law.csuohio.edu/academics/curriculum/coursedescriptions-ad#C

Houston:

http://www.law.uh.edu/schedule/class_information.asp?cid=10921

New Hampshire:

http://law.unh.edu/courses/cybercrime/95

(7) Is the subject of cybercrime included in the training and/or continuing education of judges, prosecutors and police?

Yes, in many jurisdictions.

(8) Please identify whether the following forms and means of cybercrime (1) occur frequently, (2) occur infrequently, or (3) have not occurred in your country, by placing an "X" as appropriate in the following table:

Forms and Means of Cybercrime	Occur Frequently	Occur Infrequently	Has not Occurred
Online identity theft (including phishing and online trafficking in false identity information)	X		
Hacking (illegal intrusion into computer systems; theft ofinformation from computer systems)	X		
Malicious code (worms, viruses, malware and spyware)	X		
Illegal interception of computer data	X		
Online commission of intellectual property crimes	X		
Online trafficking in child pornography	X		
Intentional damage to computer systems or data	X		
Others			

(9) In addition, to the above, if there are there any other forms and means of cyber-crime that have occurred (either frequently or infrequently) in your country, please identify them as well as the frequency with which they occur in the following table:

Forms and Means of Conduct	Occur Frequently	Occur Infrequently
Cyberbullying	X	
Cyberstalking	X	

APPENDIX I
STATE CYBER-CRIME LEGISLATION

Alabama

ALA. CODE §§ 13A-8-100 to 13A-8-103 (1994)

Alaska

ALASKA STAT. §§ 11.46.200(a)(3), 11.46.484(a)(5), 11.46.740, 11.46.985, 11.46.990 (2000);

Arizona

ARIZ. REV. STAT. ANN. §§ 13-2301(E), 13-2316 (2000)

Arkansas

ARK. CODE ANN. §§ 5-41-101 to 5-41-108 (1997)

California

CAL. PENAL CODE §§ 502, 1203.047 (West 1998 & Supp. 2004)

Colorado

COLO. REV. STAT. §§ 18-5.5-101 to 5-102 (2000)

Connecticut

CONN. GEN. STAT. §§ 53a-250 to 53a-261 (1999 & Supp. 2001)

Delaware

DEL. CODE ANN. tit. 11, §§ 931-939 (1995 & Supp. 2000)

Florida

FLA. STAT. §§ 815.01-.07 (2000)

Georgia

GA. CODE ANN. §§ 16-9-90 to 16-9-94 (1998)

Hawaii

HAW. REV. STAT. §§ 708-890 to 708-893 (1999)

Idaho

IDAHO CODE ANN. §§ 18-2201 to -2202, 26-1220 (1997)

Illinois

720 ILL. COMP. STAT. 5/16D-1 to -7 (1998 & Supp. 1999)

Indiana

IND. CODE §§ 35-41-2-3, 35-43-1-4 (1998)

Iowa

IOWA CODE ANN. §§ 716A.1-.16 (West 1993 & Supp. 2000)

Kansas

KAN. STAT. ANN. § 21-3755 (1995 & Supp. 1999)

Kentucky

KY. REV. STAT. ANN. §§ 434.840-.860 (1999)

Louisiana

LA. REV. STAT. ANN. §§ 14:73.1-.5 (1997 & Supp. 2001)

Maine

ME. REV. STAT. ANN. tit. 17-A, §§ 431-433 (West Supp. 2000)

Maryland

MD. CODE ANN., CRIM. LAW § 7-302 (West 2004)

Massachusetts

MASS. GEN. LAWS ch. 266, §§ 30, 33A, 120F (1992 & Supp. 2000)

Michigan

MICH. COMP. LAWS §§ 752.791-.797 (1991 & Supp. 2000)

Minnesota

MINN. STAT. §§ 609.87-.894 (1998)

Mississippi

MISS. CODE ANN. §§ 97-45-1 to -13 (2000)

Missouri

Mo. REV. STAT. § 569.095 (1994) (amended by Stolen Property--Services--Penalty Provisions, 2002 Mo. Legis. Serv. 194 (West))

Montana

MONT. CODE ANN. §§ 45-6-310,-311 (1999)

Nebraska

NEB. REV. STAT. §§ 28-1343 to -1348 (1995)

Nevada

NEV. REV. STAT. §§ 205.473-.491 (2007)

New Hampshire

N.H. REV. STAT. ANN. §§ 638:16-19 (1996 & Supp. 2005)

New Jersey

N.J. STAT. ANN. §§ 2A:38A-1 to -6 (West 2000), 2C:20-23 to -34 (West 1995 & Supp. 2000)

New Mexico

N.M. STAT. §§ 30-45-1 to -7 (2006)

New York

N.Y. PENAL LAW §§156.00-.50 (McKinney 2006)

North Carolina

N.C. GEN. STAT. §§ 14-453 to -457 (2005)

North Dakota

N.D. CENT. CODE § 12.1-06.1-08 (1997 & Supp. 2003)

Ohio

OHIO REV. CODE ANN. § 2913.04 (West 2007)

Oklahoma

OKLA. STAT. ANN. tit. 21, §§ 1951-1958 (West Supp. 2001)

Oregon

OR. REV. STAT. §§ 164.125, 164.377 (1999)

Pennsylvania

18 PA. CONS. STAT. ANN. § 7601, 7603, 7611, 7615, 7616 (West Supp. 2003)

Rhode Island

R.I. GEN. LAWS §§ 11-52-1 to -8 (2000)

South Carolina

S.C. CODE ANN. §§ 16-16-10 to -40 (Law. 1985 & Supp. 2000) (amended by Computer Abuse Act of 2002, 2002 S.C. Acts 169)

South Dakota

S.D. CODIFIED LAWS §§ 43-43B-1 to -8 (1997)

Tennessee

TENN. CODE ANN. §§ 39-14-601 to -603 (1997 & Supp. Page 62 2000)

Texas

TEX. PENAL CODE ANN. §§ 33.01-.04 (Vernon 1994 & Supp. 2001)

Utah

UTAH CODE ANN. §§ 76-6-701-705 (1999 & Supp. 2000)

Vermont

VT. STAT. ANN., tit. 13, §§ 4101-4107 (Supp. 1999)

Virginia

VA. CODE ANN. §§ 18.2-152.1 to .15 (1996 & Supp. 2000)

Washington

WASH. REV. CODE §§ 9A.52.110-.130 (1998)

West Virginia

W. VA. CODE. §§ 61-3C-1 to -21 (2000)

Wisconsin

WIS. STAT. § 943.70 (1998)

Wyoming

WYO. STAT. ANN. §§ 6-3-501 to -505 (1999 and Supp. 2000).