Chapter 5: Legislative Initiatives and Technical Measures

5.1 Introduction

From logical and pragmatic perspectives, knowing the problem, risks associated therewith, and the ills resulting from online phishing is an important step towards a possible solution. Furthermore, such determination constitutes an integral part of devising effective vaccines and serums to eradicate and prevent this crime. Having described the problem and the diverse types of online phishing, we shall now address some of the potential solutions thereto. Thus, we shall first analyze the American approach, United Kingdom, and Singapore before we move to the technical solutions that aim to enhance privacy and provide a secure medium for data transfer in a manner that protects the confidentiality and integrity of personal information.

5.2 Legislative Initiatives

5.2.1 The United States

The United States is a Federal Republic and its Constitution allocates lawmaking authority between the federal and state levels in accordance with certain principles.[118] Federal legislative jurisdiction is limited and is exercised only where intervention at that level is required such as where problems are national in scope and the solution lies in a uniform and consistent law that is common to all states. In that sense, computer crimes and cyber crimes that are easily perpetrated across borders and that are considered illegal in all states is a good example of an area of law that is susceptible to federal treatment. In actual fact, computer crime and cyber crime legislation have been formulated and adopted at both federal and state levels.

[118] See, U.S. CONST. Art. I § 8, which lists the United States Congress' power to legislate in various areas; and U.S. CONST. Amend. X, which states that: "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."

Due to the USA political structure, computer-related crime legislation and enforcement remain largely under state jurisdiction of prescription, adjudication and enforcement.[119] Each state has its own unique set of criminal legislation and there is no formal mechanism compelling them to adopt uniform or consistent laws.[120]

The United States Department of Justice (DOJ) has defined "computer crime" as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution",[121] which for our purposes would be the same as "computer-related crime". However, the DOJ had also further divided computer-related crimes into three categories according to the computer's role in the particular crime: The computer as the "object" of a crime, as the "subject" of a crime (i.e. computer crimes for which there is no analogous traditional crime and for which special legislation is needed), or as an "instrument" of traditional crimes.[122] This compartmentalization resembles the categorizations made under Part1.

Since 1984, the United States Congress has pursued a dual approach to combating computer crime.[123] The Counterfeit Access Device and Computer Fraud and Abuse Law of 1984 and subsequent amending Acts address crimes in which the computer is the "subject". This line of statutes culminated in the National Information Infrastructure Protection Act of 1996 (NIIPA).[124]

The federal government's approach to regulating crimes involving the computer as an "instrument" has been to update traditional criminal statutes in order to reach similar crimes

---

[119] See, Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey*, 7 RICH. J.L. & TECH. 28 (Winter 2001), available at http://www.richmond.edu/jolt/v7i3/article2.html.

[120] Except, for example, insofar as federal legislation preempts state laws where they conflict. However, there are many non-mandatory instruments that seek to persuade states to adopt laws in as similar a fashion as possible, including Restatements of Law, Uniform Acts and the Model Laws (e.g. the Model Penal Code).

[121] NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUST., COMPUTER CRIME: CRIMINAL JUST. RESOURCE MANUAL 2 (1989).

[122] *Ibid.* at Note 1.

[123] See, Dana L. Bazelon, Yun Jung Choi and Jason F. Conaty, *Computer Crimes*, 43 Am. Crim. L. Rev. 259, 264 (2006).

[124] 18 U.S. Code § 1030. The latest amendments came from the infamous Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) as well as from the Cyber Security Enhancement Act of 2002 and the Computer Software Privacy and Control Act of 2004. *Ibid.* at 265-273.

involving computers. The federal government has also used the United States Sentencing Guidelines (USSG) to enhance sentences for traditional crimes committed with the aid of computers. In fact, there have already been initiatives at the federal level to deal with cyber crimes and crime-specific legislation continues to surface at the national level that is worth serious consideration.[125]

There are several federal computer crime and cyber crime statutes including the omnibus federal computer crime/cyber crime statute which makes it an offence to, among other things, gain unauthorized entry to a computer and thereby gain access to information to which the perpetrator is not entitled to have access; and to gain unauthorized access to a computer and thereby further the perpetration of a fraud.[126] These are essentially computer crime offences that are *relevant to* but not specifically applicable to phishing scams and other fraud schemes involving identity theft and, in certain cases, to further the objective of financial cheating or stealing from the primary target.

[125] *Ibid.* at 273-290 (discussing the most prominent statutes that are used to prosecute traditional crimes committed with the aid of a computer). In relation to phishing and its relation to identity theft in particular, any number of federal legislation may be implicated depending on the method and objective of the perpetrator including statutes relating to wire fraud, credit card fraud, bank fraud, computer fraud, anti-spam and consumer protection. See, Matthew Bierlein and Gregory Smith, *Internet: Privacy Year in Review: Growing Problems with Spyware and Phishing, Judicial and Legislative Developments in Internet Governance, and the Impacts on Privacy*, 1 ISJLP 279, 308-309 (2005).

[126] 18 U.S. Code § 1030. The statute contains other computer-related offences as well. Other statutes include 18 U.S. Code § 1028 (making it a crime to produce, transfer or possess a device, including a computer, that is intended to be used to falsify identification documents); and 18 U.S. Code § 2319 (making it a federal offense to infringe a valid copyright.). Other existing criminal statutes and provisions may also apply to computer-related transactions as well. For example, sex-related statutes such as 18 U.S. Code § 1462-1463 (prohibiting the use of a computer to import obscene material into the United States or to transport such material in interstate or foreign commerce); 18 U.S. Code 2251-2252A (making it a crime to employ or to induce participation by a minor in the making of a visual depiction of a sexually explicit act if it was created using materials that had been transported, including by electronic means, in interstate or foreign commerce; prohibiting the use of a computer to sell or transfer custody of a minor knowing the minor will be used to create a visual depiction of sexually explicit conduct; and making it a crime to use a computer to transport child pornography in interstate or foreign commerce). For more on the Computer Fraud and Abuse Act, see Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 Berkeley Tech. L.J. 909 (2003); and Jo-Ann M. Adams, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 Santa Clara Computer & High Tech. L.J. 403, 409 (1996). See also Sara R. Paul, *Identity Theft: Outline of Federal Statutes and Bibliography of Select Resources* (LLRX.com, 18 September 2005), available at: http://www.llrx.com/features/idtheftguide.htm.

More specifically in relation to phishing practices, a new federal law that is already in effect that is relevant to phishing, albeit *indirectly*, is the Identity Theft Penalty Enhancement Act of 2004 (ITPEA),[127] which establishes the federal criminal offense of aggravated identity theft and creates more stringent means and stronger penalties to punish phishers. Legislation aimed *directly* at phishing practices was first introduced to the United States Congress in 2004,[128] and again in 2005 in the form of the Anti-Phishing Act of 2005. [129] The Bill targets the entire scam process from the sending of the email to the creation of fraudulent sites.[130] It stipulates that the perpetrator must have the specific criminal purpose of committing a crime of fraud or identity theft before an offence is made out.[131]

A feature of the bill that is worth promoting as a model for other jurisdictions for any international treaty on such offences is that it criminalizes the bait. This 'poisoned bait' approach criminalizes the conduct engaged in before the actual commission of the fraud. For example, it makes it illegal to knowingly send out spoofed email that links to false web sites, with the intention of committing a crime. It also criminalizes the operation of such

[127] 18 U.S Code § 1028A. An individual commits aggravated identity theft if, while engaging in an enumerated identity theft related offense, the individual "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person." The commission of aggravated identity theft results in a mandatory minimum sentence of 2 years imprisonment in addition to the punishment imposed for the original offence. *Ibid*. at subsection (a)(1). *See also* DEPARTMENT OF JUSTICE, CRIMINAL DIVISION, SPECIAL REPORT ON "PHISHING", *available at* http://www.usdoj.gov/criminal/fraud/Phishing.pdf.

[128] It was introduced by Democratic Senator Patrick Leahy of Vermont as an Act to criminalize Internet scams "involving fraudulently obtaining personal information, commonly known as phishing". S. 2636, 108th Cong. (2004), available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:s2636is.txt.pdf. See U.S. Senator Patrick Leahy, *Senate Floor Speech: New Leahy Bill Targets Internet "PHISHING" And "PHARMING" That Steal Billions Of Dollars Annually From Consumers* (28 February 2005), available at: http://leahy.senate.gov/press/200503/030105.html. For an overview, see Robert Louis B. Stevenson, *Plugging the "Phishing" Hole: Legislation Versus Technology*, Duke L. & Tech. Rev. 6 (2005), available at: http://www.crime-research.org/analytics/phishing_duke/.

[129] The 2005 Bill was similarly introduced by Democratic Senator Patrick Leahy of Vermont for the same objective as the 2004 version. S. 472, 109th Cong. (2005), available at: http://thomas.loc.gov/cgi-bin/bdquery/z?d109:S.472: and http://www.theorator.com/bills109/s472.html. See also, Grant Gross, *Proposed Law Aims to Fight Phishing: Anti-Phishing Act of 2005 Allows for Prison Time and Hefty Fines* (IDG News Service, 5 March 2005), available at: http://www.pcworld.com/news/article/0,aid,119912,00.asp; Gearhead, *Will the Anti-Phishing Act Make a Difference* (NetworkWorld.com, 18 March 2005), available at: http://www.networkworld.com/weblogs/gearblog/2005/008234.html and http://www.internetnews.com/security/article.php/3487271.

[130] The 2005 Bill is similar to the 2004 version and covers both phishing and pharming scams. Parody web sites, both commercial and political, are exempted from the penalties in the bill, thereby avoiding free speech issues and Constitutional impediments.

[131] The statute seeks to amend the fraud and identity statute by including specific provisions on Internet fraud. The statute is directed at those with the intention of carrying on any activity that would be a federal or state crime of fraud or identity theft. If an individual knowingly engages in cybersquatting or spoofs a domain name to induce or solicit an individual to provide information, he may be subject to a fine, imprisonment, or both. If an individual sends an email or other Internet communication, which falsely represents itself as being sent by a legitimate business, refers or links users to a cybersquatted or spoofed location, and induces or solicits personal information, he may be subject to the same punishment. For other relevant legislation, see also, the Internet False Identification Prevention Act of 2000 and the Fraudulent Online Identity Sanctions Act of 2004 (proposed amendment to the Trademark Act of 1946).

web sites that are the *locus* of the wrongdoing. This creates an opportunity to prosecute before the actual fraud takes place, not just to successful phishing occurrences. It thus has a pre-emptive effect to such crimes and emphasizes the importance of deterrence and crime prevention.[132] The penalty of imprisonment and fine are also appropriately strong and will, hopefully, provide greater deterrent effect. But even then there continue to exist territorial limitations, both in law (i.e. the reach of the legislation) and in fact (i.e. in actual and effective implementation and enforcement).[133] The bill has also yet to be passed.[134]

The United States will continue to produce state-centric computer-related crime legislation as it does for other laws. However, two idiosyncrasies of cyberspace support greater federal involvement in computer-related criminal law making. First the 'borderless' nature of such criminal activities and the fact that jurisdictional rules that function effectively for physical activities do not translate well to the cyber realm.[135] Second, the diversity in procedural augmentation has led to a confusing cacophony of state laws that exacerbates the jurisdictional problems of adjudication and enforcement.[136] Seeking a consistent solution at

[132] The deterrent cum preventative aspect of legislation is very important, particularly to the primary policy objective of protecting and rebuilding trust and integrity in the Internet system of transaction. See Jennifer Lynch, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 Berkeley Tech. L.J. 259 298-299 (2005). See also Anita Ramasastry, *The Anti-Phishing Act of 2004: A Useful Tool Against Identity Theft* (Findlaw Comentary, 16 August 2004), available at: http://writ.news.findlaw.com/ramasastry/20040816.html. Criminalizing after the fact and low rates of reporting and enforcement action makes existing federal laws that indirectly criminalizes phishing acts inadequate.

[133] Another valid criticism is that currently many of the proposed solutions to phishing relates to the technique in general rather than the offence in particular. See Matthew Bierlein and Gregory Smith, *Internet: Privacy Year in Review: Growing Problems with Spyware and Phishing, Judicial and Legislative Developments in Internet Governance, and the Impacts on Privacy*, 1 ISJLP 279, 308-309 (2005). "[Many proposed solutions are still targeting spam in general and not the specific bad acts presented by phishing." *Ibid*. at 280. This can be limiting particularly when technology and techniques vary and change.

[134] Meanwhile, some states have already produced specific anti-phishing legislation. At the National Conference of State Legislatures web site at: http://www.ncsl.org/programs/lis/phishing06.htm, statistics show that as of 13 July 2006, ant-phishing bills have been introduced in at leas ten states and enacted in at least six states. See also, Hohn D. Saba, *The Texas Legislature Goes Phishing*, 68 Tex. B.J. 706 (2005); and HNS Staff, *Details From the Anti-Phishing Act of 2005*, (Net-Security.org, 5 October 2005) on California as the pioneering state to legislate against phishing.

[135] E.g. where is a "harm caused"? Where is a criminal offence "committed"?

[136] States have to varying extents amended or adopted legislation that target procedural and substantive issues relating to computer-related crime. Some have amended existing legislation in an attempt to update crime-specific statutes or general criminal statutes, while others have enacted entirely new laws. Jurisdiction, definitions and penalty provisions are just some of the changes made in an attempt to make their criminal law relevant to electronically perpetrated crimes. As one of the more technologically advanced countries in the world, the non-uniformity of treatment and lack of comprehensiveness of its substantive computer-related crime legislation is disappointing. The way the United States and many other jurisdictions have dealt with computer-related crime, that is, piecemeal and as it arises, can be analogized to how Microsoft continues to issue "patches" for its programs. It works to some extent, but not in a particularly satisfactory manner.

the national level is preferable to sub-national efforts with varying degrees of effectiveness,[137] particularly if the objectives of eliminating or at least reducing computer-related crimes, through deterrence and punishment of offenders, are to be met.[138] Years after the United States signed the Cybercrime Convention; the United States Senate finally ratified the Convention in August 2006 becoming the sixteenth country to do so.[139] The significance of its ratification will only become apparent in time.[140]

5.2.2 The United Kingdom

The European community and its neighbouring countries influence the public policy and laws of the United Kingdom. The Council of Europe (CoE) has issued a number of documents, which have influenced the British criminal justice system. For example, through its acknowledgement of the standards set by the CoE in its Cybercrime Convention as a signatory state, the United Kingdom signified its intention to bring the provisions under the Convention into effect within the country.[141] The reason for the influence is the

[137] Indeed, the United States has produced more than forty different federals statutes that contain criminal provisions for computer-related crimes. See, Heather Jacobson and Rebecca Green, *Computer Crimes*, 39 Am. Crim. L. Rev. 273, 287-304 (2002); Eric J. Bakewell, Michelle Koldaro and Jennifer M. Tjia, *Computer Crimes*, 38 Am. Crim. L. Rev. 481, 287-304 (2001); Laura J. Nicholson, Tom F. Shebar and Meredith R. Weinberg, *Computer Crimes*, 37 Am. Crim. L. Rev. 207, 220-231 (2000); Michael Hatcher and Jay McDannell and Stacy Ostfeld, *Computer Crimes*, 36 Am. Crim. L. Rev. 397, 411-418 (1999); and Sheri A. Dillon, Douglas E. Groene and Todd Hayward, *Computer Crimes*, 35 Am. Crim. L. Rev. 503, 513-519 (1998).

[138] The objectives of harmonization and consistent laws that are enforceable anywhere in the world are equally applicable here at the national plane. See below Part 3 on the "Objectives of Multilateralism".

[139] See Nate Anderson, *"World's Worst Internet Law" ratified by Senate* (arstechnica.com, 4 August 2006), available at: http://arstechnica.com/news.ars/post/20060804-7421.html. As noted, civil libertarians have criticized the move, warning of the potential problems associated with the apparent dispensation of the dual criminality requirement in some cases for law enforcement. See also, Dan Kaplan, *Senate Ratification of Cybercrime Treaty Praised* (SC Magazine, 4 August 2006), available at: http://www.scmagazine.com/uk/news/article/576037/senate-ratification-cybercrime-treaty-praised/; and Anon., *Senate Ratifies Convention on Cybercrime* (Tech Law Journal, 3 August 2006), available at: http://www.techlawjournal.com/topstories/2006/20060803b.asp.

[140] Also, how this translates into its laws and how it will relate to existing federal and state laws will require closer examination.

[141] The U.K. Government was involved in the creation of two treaties on the prevention of cybercrime, under the CoE and the EU, both of which originated in Europe and both of which calls for international coordination to tackle abuses of computer systems. They are the Cybercrime Convention of 2001 and the E.U. Council Framework Decision on Attacks Against Information Systems (OJ L 069, 16 March 2005), which was proposed on 19 April 2002, adopted on 24 February 2005 and required to be transposed into national law by 16 March 2007 by member states.

fact that European countries are a closely interconnected community of nations historically, geographically and economically.[142]

The United Kingdom computer crimes legislation is the Computer Misuse Act of 1990 (CMA).[143] The government is currently proposing amendments to the CMA to update it with more expansive provisions and stiffer penalties.[144] The amendments have been sent to the House of Lords for consideration as part of the Police and Justice Bill.[145] The only overlapping provision under the CMA with cyber crime offences is section 2 which makes it an offence to gain unauthorized access to any program or data held in any computer with the intention of committing or facilitating the commission of further offences that satisfy a set of criteria.[146]

Unlike the Cybercrime Convention that provides for both computer crime and cyber crime under one instrument, the United Kingdom itself has a distinctive dual track approach by enacting the CMA for computer crimes while leaving computer-enabled commission of more traditional offences to be dealt with under existing criminal legislation. Amendments to specific legislations and provisions have also been made to cover possible lacunas as a result of developments brought on by the advent of the electronic age. The application of

[142] In contrast, the United States is not strongly influenced by the rule of law of Europe. Even if the United States government adopts some of the propositions set out by the European community, it is not bound to the same extent that other European countries are bound.
[143] The United Kingdom CMA is available at: http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm. For an overview, see generally, Martin Wasik, *The Computer Misuse Act*, 1990 Crim. L. Rev. 767. This CMA became the model and formed the template for many similar Acts in other Commonwealth jurisdictions including Singapore and Malaysia.
[144] Although the United Kingdom pioneered computer crime legislation, it has since been overtaken in terms of its relevance by other countries such as Singapore, which has seen many changes to it since it has been originally enacted, in particular, taking into account new problems relating to the uses of the computer for communications and as the gateway to the Internet. See, Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How To Kill Zombies*, 24 Cardozo Arts & Ent LJ 23, 36 (2006).
[145] See, Jeremy Kirk, *Analysts Wary of U.K. Cybercrime Law Revamp: Tougher Penalties, But Can the Law Stay Up to Date?* (IDG News Service, 7 June 2006), available at: http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Cybercrime_Hacking&articleId=9000999&taxonomyId=82 and http://www.networkworld.com/news/2006/060706-analysts-eye-revamp-uk-cybercrime.html?prl. An earlier proposal for revision, the Computer Misuse Act 1990 (Amendment) Bill, 2004-2005, H.C. Bill [102], sponsored by the chair of the All Party Parliamentary Internet Group (APIG), fell through when Parliament was prorogued in April 2005.
[146] Under subsection 2: "[O]ffences for which the sentence is fixed by law; or for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years…" Cf. section 4 of the Singapore CMA.

traditional criminal concepts to non-traditional acts and actors, instruments, information and products arising from new technology require amendments, in particular relating to definition, interpretation and scope. The United Kingdom government has done this for some of its legislation such as those pertaining to fraud and theft, pornography and intellectual property offences.

With regards to amendments to fraud and theft legislation, which is relevant to our case study, section 2 of the CMA is a useful net to catch offences that are perpetrated through electronic means. Also, an offence of "obtaining a money transfer by deception"[147] was created under the Theft Act of 1968, which required that property "belonging to another"[148] must be obtained for fraud because it did not cover, for instance, an accounts-related fraud case where the data recorded in a set of accounts was altered, since it did not constitute the obtaining of *property* "belonging to another".[149] This appears to cover most phishing and related offences, since in all likelihood there will be some form of money transfer involved. However, the transfer of other financial or other assets such as something that is only of sentimental value, in particular those in digital form may not fall under either "money transfer" or "property".[150]

In the meantime, in a new development, the Fraud Act was been enacted and passed by the Parliament, which is of direct relevance to the act of phishing and other such fraudulent

[147] Money can be transferred to a third party for the purchase of goods or it can be transferred to the offender's own account.
[148] Under the Act, "[a] person is guilty of theft, if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it". Section 4 defines "property" as "include[ing] all *personalty*, i.e. land itself cannot be stolen but anything severed from the land (with the exception of wild flowers) can be stolen, as can intangible property such as a chose in action."
[149] See section 1 of the Theft (Amendment) Act of 1996, available at: http://www.opsi.gov.uk/acts/acts1996/1996062.htm. There are now five offences, namely: Obtaining services by deception under section 1; evasion of liability by deception under section 2; obtaining property by deception under section 15; obtaining a money transfer by deception under sections 15A and 15B; and obtaining a pecuniary advantage by deception under section 16. It is also an offence to make off without paying. This does not require a deception.
[150] The Act also does not cover the use of improperly obtained passwords and identifiable information *per se* or its use to access data or information. It appears that that is left to other laws including the CMA and laws relating to trade secrets, confidential information, privacy and data protection.

acts.[151] It was introduced into the House of Lords on 25 May 2005 with the aim of modernizing the definitions of fraud, which have not been changed to take into consideration technological advances since 1968.[152] The law will ensure that criminals utilizing technology to commit offences will not escape prosecution due to a loophole in the law based on outdated and narrow definitions. For example, under the current narrowly defined offences of deception in the Theft Acts, criminals operating online often escape prosecution, as their crime does not technically fall within the definition of the offence.

The Act creates a general offence of fraud which can be committed in one of three ways: Firstly, false representation which this offence would also be committed by someone who engages in "phishing": i.e. where a person disseminates an email to large groups of people falsely representing that the email has been sent by a legitimate financial institution. The email prompts the reader to provide information such as credit card and bank account numbers so that the "phisher" can gain access to others' personal financial information." [153] secondly, failure to disclose information, and thirdly, abuse of position. Other new offences relating to obtaining services dishonestly,[154] and possessing, making and supplying articles for use in fraud have also been created under the Bill.[155] The wording of the Act has been specifically drafted to include online fraud and other offences involving the use of

[151] Bill 166 Sess. 2005-2006, available at the U.K. Parliament web site at: http://www.publications.parliament.uk/pa/cm200506/cmbills/166/06166.i-i.html or http://www.publications.parliament.uk/pa/cm200506/cmbills/166/2006166.pdf. For the latest updates, see: http://www.publications.parliament.uk/pa/pabills/200506/fraud.htm. See further, the House of Lords Explanatory Notes on the Fraud Bill, available at: http://www.publications.parliament.uk/pa/ld200506/ldbills/007/en/06007x--.htm; and the House of Commons Explanatory Notes on the Fraud Bill, available at: http://www.parliament.the-stationery-office.co.uk/pa/cm200506/cmbills/166/en/06166x--.htm.

[152] The Government's Response to the views expressed in earlier consultations was published on the U.K. Home Office web site on 24 November 2004, available at: http://www.homeoffice.gov.uk/documents/cons-fraud-law-reform).

[153] See the House of Lords Explanatory Notes on the Fraud Bill at para. 14; and the House of Commons Explanatory Notes on the Fraud Bill at para. 16.

[154] E.g. fraudulent credit card transactions on the Internet.

[155] See, Susan Barty and Phillip Carnell, *Fraud Bill Offers Protection from IT Fraud* (dCode.co.uk, 11 July 2005), available at: http://www.dcode.co.uk/site/home/20050711fraud.html; or Susan Barty and Phillip Carnell, *United Kingdom: New Protection Against Technology Abuse Under Government's Fraud Bill* (Mondaq, 5 July 2005), available at:http://www.mondaq.com/article.asp?articleid=33546&lastestnews=1.

technology. It is to be noted that fraud by false representation is committed irrespective of whether the intended victim is deceived. Hence, it has a pre-emptive effect similar to that which is offered in the United States Anti-Phishing Bill, and punishes an offender without requiring a victim to materialize in the first place. If and when it is passed, it will overtake many of the offences under the Thefts Act.[156]

Since the new Fraud Act come into force in early 2007, the aims to close a number of loopholes in preceding anti-fraud legislation, which the Government said was unsuited to modern fraud. The Act seeks to simplify the criminal law by creating a general offence of fraud, which may be committed in three different ways[157]. The Attorney General, Lord Goldsmith commented:

"*This reform is needed to enable prosecutors to get to grips with the increasing abuse of new technology, particularly in relation to fake credit cards scams and personal identity theft, which cost millions of pounds every year*"[158].

In the similar vein, the Home Office official said, "The introduction of a general fraud offence will improve the criminal law in a number of respects. It will simplify the law, making it clearer to juries and the general public as well as making the prosecution process more effective by providing a clear definition of fraud. Our aim is to encompass all forms of fraudulent conduct, with a law that is flexible enough to deal with developing technology, allowing us to bring more offenders to justice"[159]. Earlier, in its consultation paper the Home Office rejected calls for a specific offence to cover phishing, maintaining that this, "is an offence, or an attempted offence, of fraud under the current law" and that it

[156] Meanwhile, the United Kingdom recently folded its national computer crime unit, the National Hi-Tech Crime Unit, into a new agency known as the Serious Organized Crime Agency (SOCA); while the Crown Prosecution Service (CPS) is sending its legal officers for special training on computer-related crimes in order to educate them on the technical aspects of such offences and to keep them abreast of developments so as to update their skills and knowledge in this area.

[157] Ref Abu Bakar Munir, "Would the Phishers get Hooked"

[158] *See* finextra.com, "UK Government Cracks Down on Phishers", available at http://www.finextra.com/fullstory.asp?id=13735

[159] *See* ZDNet.co.uk, "Government Moves to Tackle Phishing", available at http://www.zdnet.co.uk/misc/print/0,000000169,39201079-39001093c,00.htm

would be caught by the proposed new offence created by the Bill. Section 1 of the Bill sets out a new general offence of fraud, the maximum penalty for which will be ten years' imprisonment and a fine. There will be three different ways of committing the new offence and these are set out in Sections 2, 3 and 4 of the Act. They are fraud: (1) by false representation (Section 2); (2) by failing to disclose information (Section 3); and (3) by abuse of position (Section 4).

Section 2 covers phishing. Under this section, it will be an offence for a person to commit fraud by making a false representation dishonestly. Section 2(2) defines a representation as being "false" if it is untrue or misleading and the person making it knows that it is, or might be, so.

"Representation" is defined in Section 2(3) as any representation as to fact or law, including a representation as to a person's state of mind. The representation may be expressed or implied.

Section 2 is drafted broadly so as to encompass fraudulent Internet and other activities such as phishing. The Act requires that the representation must be made dishonestly and it must be made with the intention of making a gain or causing loss or risk of loss to another, regardless of whether the gain or loss actually takes place. The prosecution will not have to show that actual gain or loss took place. There is no limitation on the way in which the words must be expressed and that it could therefore be written, spoken or posted on a website. The explanatory notes states," This offence would also be committed by someone who engages in phishing…."

Section 6 of the Fraud Act can be used against phishers as well. This clause seeks to make it an offence, punishable by up to five years' imprisonment and a fine, for a person to have in his possession or under his control any article for use in the course of or in connection

with any fraud. Under this clause, it is an offence for phishers to have in his possession or under his control any software or trojan to be used to intercept communication between parties to glean information which he should not have access. This is relevant in relation to pharming and man-in the- middle-attack. As stated in the explanatory notes, the intention of section 6 is to cover a situation where the defendant had the article for the purpose of or with the intention that it be used in the course of or in connection with the offence, and that a general intention to commit fraud will suffice.

Another provision of the new law which is applicable to phishing is section 11. It is designed to make it an offence, punishable by up to five years imprisonment and a fine, for a person, by dishonest act, to obtain services for him or another person, for which payment is required, with intent to avoid paying the full amount required. For a prosecution to succeed it will have to be proved that the person knew when he obtained the services that payment was required or that it might be. Deception is not required under this new offence. The explanatory notes comments that the new offence will be committed only where the dishonest act was done with the intention of avoiding the expected payment for the services concerned. The explanatory notes states:

The offence is not inchoate; it requires the actual obtaining of the service. For example, data or software may be made available on the Internet to a certain category of person who has paid for access rights to that service. A person dishonestly using false credit card details or other false personal information to obtain the service would be committing an offence under this clause.

5.2.3 The Singapore Model[160]

Unlike the United States and the approach taken by the CoE for the Cybercrime Convention, which combined computer crimes and cyber crimes in a single instrument, the Singapore legislature focused its efforts on producing a computer crime specific legislation, while attempting to leave cyber crime to be dealt with under its existing statutes through augmentation by amendment. Thus, it follows the United Kingdom model and approach to the problem. This stems from the perception that since the actual criminal acts relate to traditional offences, the inclusion of definitions and references to electronic modes of communication and commission of offences will be sufficient. However, as it will be shown in the case of phishing and similar offences of fraud involving identity theft, this approach is clearly inadequate as to its coverage under current legislation. It is also not able to satisfactorily meet public policy objectives such as crime deterrence, prevention and punishment.

Like the United Kingdom, only computer crime is dealt with under the Computer Misuse Act (Cap. 50A) (CMA).[161] Cyber crime remains to be dealt with under the provisions of the Penal Code (Cap. 224) and the provisions of a host of other legislations,[162] which as stated

[160] Gregor Urbas, "An Overview of Cybercrime Legislation and Cases in Singapore"Asian Law Institute Working Paper Series No 001, Dec 2008

[161] In summary, the CMA adopts four approaches to fight computer crimes: First, creating of new computer crimes for new problems that arise which require regulation; second, providing appropriate penalties as punishment and for deterrent effect, often increasing penalties, particularly in relation to the seriousness of the offence, such as the increased penalties where "damage" occurs (sentencing guidelines and policy further complement this approach); third, giving enhanced and specific powers of investigation to law enforcement agencies and creating specialised agencies with trained professionals and experts to deal with what are specialty crimes; and fourth, acknowledging the trans-national nature of such offences and its effects by giving extra-territorial effect to the offences under the Act and making it also an offence to abet and even to attempt the commission of such offences. The CMA further enhances computer security, by broadening the powers of the police to investigate such misdeeds and by giving it extra-territorial effect. In relation to law enforcement, on top of broader police powers, the Singapore government has also established specialized technology units to handle computer crime investigations. These are the Computer Crimes Branch of the Criminal Investigation Department (CID), the Computer Forensics Branch of the Singapore Police Force (SPF), and the Singapore Computer Emergency Response Team (SingCERT) of the IDA. They were considered necessary to cope with the technological aspects of such cases and the increasing sophistication of computer programs and functions as well as of computer users. Finally, it is worth noting that section 4 of the CMA refers to offences involving "property", "fraud" and "dishonesty" (all of which appear mostly in the cheating provisions) or which causes bodily harm (offences against the person). However, the prerequisite of a punishable 2-year jail term appears arbitrary.

[162] E.g. the Miscellaneous Offences (Public Order and Nuisance) Act (Cap.184).

are inadequate to deal with the problem in terms of both applicability and the effects of the punishment.[163]

The problem with relying on a legislation that was drafted before the electronic age, and that has not been amended, is that certain words and their interpretation do not apply to the electronic form of transacting or to such an environment. Under the current version of the Penal Code, the offence of cheating should apply to acts of phishing with the purpose of using stolen information for unlawful economic gain. A person cheats "by deceiving any person, [and] fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property."[164] The victim could be the person whose information is stolen, provided that such information can constitute "property" (which shall be an issue to be considered in relation to other property offences), or it could be the person or organization which is deceived or intentionally induced into transacting with the offender on the basis of that information (which can include banking and financial institutions, companies and business, and other forms of organization).

The definition of "property" here is a crucial one in order for there to be an actionable offence of cheating in relation to the theft of the users or customers' (the primary target) identity and other personal data and information such as passwords and identifiable codes

[163] This statement relates to the general criminal offence provisions under the Penal Code (Cap. 224) alone. There may be other provisions in specific legislation providing against fraud and fraudulent transactions pursuant to the use of stolen information that can cover phishing and related activities.
[164] Section 415 of the Penal Code (Cap. 224).

per se.[165] In order for the scammer to face criminal prosecution in such a case, irrespective of any subsequent transaction on other forms of property occurring through the use of the identity or information, it must be accepted that personal data and information can constitute property. There is no general interpretation of "property" under the Interpretation Act (Cap 1). However, there is a definition of "immovable property" under section 2 of the Interpretation Act which "includes land, benefits to arise out of land and things attached to the earth or permanently fastened to anything attached to the earth", and of "movable property" which means "property of every description except immovable property". What "property of every description" means and whether it extends to personal data and information, and in particular, digital and electronic information, in the context of the Penal Code and other criminal provisions is still unclear. A purposive interpretation may still yield criminal recourse against perpetrators of phishing and similar offences.[166] Certainly, it would appear that it is easier to prove cheating if a subsequent transaction on financial or tangible assets takes place through the use of such personal data or information, as can be seen in sections 421 to 424 which deals with fraudulent deeds and dispositions of property. However, they still relate to a different set of transactions.[167] The offence of cheating also does not have the effect of pre-empting further offences from occurring such as by allowing for the prosecution of theft of data or information *per se*.

Unlike the cheating provisions, which can possibly still cover phishing and related scams, some other potential criminal offences are rendered inapplicable due to the limited scope of the "property" that forms the subject matter of the offence and one of its essential elements.

[165] Additionally, the spoofing of the target organization's (the secondary target) web site can constitute copyright and trademark infringement under intellectual property laws.

[166] Clarity in the law such as in the language of the criminal provisions themselves as well as explanatory notes and modern illustrations will be most useful to remove any ambiguities.

[167] Forgery is another offence that can be applicable to cyber-fraud cases. It is a criminal offence to commit forgery for the purpose of Section 464 states that: "Whoever makes any false document or part of a document with intent to cause damage or injury to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery."

The preamble to section 2 of the Interpretation Act states that the definitions contained within it are only applicable to the extent that they are not inconsistent with the construction due to the subject or context in which they appear or unless it is otherwise expressly provided. Section 22 of the Penal Code provides that "movable property" is intended to include "corporeal property of every description, except land and things attached to the earth, or permanently fastened to anything which is attached to the earth." The ordinary meaning of "corporeal" is that which relates to, or has the characteristic of a material or tangible form. Personal information such as identity numbers and financial information do not appear to fall under this definition; neither will digital materials and property. Hence, it is unlikely that the offence of theft or criminal misappropriation of property, for example, will be useful in relation to cyberspace transactions as these offences refer to "movable property" only.

We have seen in the context of the United States and the United Kingdom law, there are two levels to the problems relating to phishing and its progeny: Fraud and identity theft. The solution to fraud, whether or not it leads to the theft of other forms of property comes in the form of general criminal legislation, such as provisions under a Criminal Code; specific legislation, such as a Theft and/or Fraud Act, or both. Identity theft can also constitute a criminal offence if it is provided as such under legislation as the United States have done.[168] Privacy and data protection laws as well as computer crime legislation also play a part if applicable to the fact situation. In Singapore's case, the basis for a fraud or theft action of intangible property such as digital assets and personal information is archaic

[168] E.g. the United States' Internet False Identification Prevention Act of 2000 and the Fraudulent Online Identity Sanctions Act of 2004 (proposed amendment to the Trademark Act of 1946).

and in need of reform, and there are no privacy or data protection laws against identity theft and personal data.[169]

There are also problems relating other subject matters of penal provisions to their digital analogues such as "book, paper, writing, valuable security or account"[170] and "document"[171].

On the other hand, it is to be noted that despite its deficiencies in cyber crime law making, the Singapore CMA has been constantly amended. However, the United Kingdom CMA is in the process of amendment. In particular, it incorporates denial of services attacks as a computer crime. It contains amendments to the CMA in Miscellaneous Part 5. It is likely to be accepted into law by the end of 2006. If it becomes law it will amend section 1(3) of the CMA by increasing the penalties for unauthorised access to computer material; section 3 of the CMA, by broadening the offence of unauthorised acts with intent to impair operation of computer to "any unauthorised act in relation to a computer", which will widen the scope of the CMA to include denial of service attacks.[172]

5.3 Technical Measures

Phishing is a problem that exploits a weakness in the current state of technology and, in a manner of speaking, "uses it against us." It makes sense, then, that an effective solution to

[169] It is also an offence to cheat by personating under section 416 of the Penal Code (Cap. 224), punishable under section 419. However, it has to involve the impersonation of a "person", whether real or imaginary, and does not extend to artificial entities or automatic agents. In Singapore, there is self-regulation in the private sector for some form of data protection but no general legal recourse, civil or criminal, for the taking of personal identifiable information *per se*.

[170] See section 477A, which is a forgery offence that may be applicable, for example, to the case of the defrauding employee.

[171] Which is defined under section 29 of the Penal Code as: "[A]ny matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, as evidence of that matter." Explanation 1 further states that: "It is immaterial by what means, or upon what substance, the letters, figures or marks are formed, or whether the evidence is intended for, or may be used in, a court of justice, or not." Explanation 2 further states that: "Whatever is expressed by means of letters, figures or marks, as explained by mercantile or other usage, shall be deemed to be expressed by such letters, figures or marks within the meaning of this section, although the same may not be actually expressed." However, this does not shed much light on whether electronic or digital forms of information or record are included in the definition. The Interpretation Act does not have a definition of "document".

[172]. See, the Computer Misuse Act 1990 (Amendment) Bill. Bill 102 Sess. 2004-2005. See also, the U.K. Parliament web site at: http://www.publications.parliament.uk/pa/cm200405/cmbills/102/2005102.htm. See, The Police and Justice Bill. Bill 119 Sess. 2005-06. See also, the U.K. Parliament web site at: http://www.publications.parliament.uk/pa/cm200506/cmbills/119/2006119.htm. The Bill is now at the House of Lords Committee (see: http://www.lga.gov.uk/Legislative.asp?lsection=59&ccat=1156). See also, Bill Thompson, *How to Legislate Against Hackers* (BBC News, 13 March 2006), available at: http://news.bbc.co.uk/1/hi/technology/4799338.stm.

this problem should focus on repairing this weakness. One commentator described the technological weakness in this way:

"When the Internet was used mainly to communicate and access information, the lack of security didn't much matter. Now that it's used for online transactions and critical information, the absence of security is truly a big problem. It's as if consumers and businesses that rely on the Internet have wandered into a dangerous neighborhood of cheats, pickpockets and thieves, and don't even know it."[173]

The U.S House of Representatives has offered this useful suggestion: "[t]here is no silver bullet to end spyware or phishing but greater consumer awareness and use of available technological countermeasures clearly hold the greatest promise for curbing these abusive practices."[174]

United States Congress's first recommendation is to increase "consumer awareness." To be sure, "common sense and a healthy level of suspicion go a long way toward not becoming a victim of phishing." Nevertheless, consumer awareness alone is not sufficient to solve the phishing problem. While it might be convenient to assume that only the gullible or Internet novices fall victim to phishing scams, the current state of technology and the phishers' ability to exploit it is such that even the most jaded and "web savvy" consumers can fall victim to a phishing scam.[175] Consumer awareness must be coupled with technological improvements.

---

[173] *House of Representatives Government Reform Committee, Technology, Information Policy, Intergovernmental Relations and the Census Committee Hearing*, 108th Cong. 35-36 (2004), [hereinafter House Committee Hearing] (Testimony of Bill Conner, Chairman, President and CEO of Entrust, Inc. stating that "[j]ust as the Internet has supercharged commercial transactions, it has also supercharged cybercrime.") *available at* 2004 WL 2137978.

[174] H.R. Rep No. 108-698, at 5

[175] For an in-depth look at many of the possible ways that current phishers are defrauding consumers, *see* Gunter Ollman, Next Generation Security Software, Ltd., The Phishing Guide: Understanding & Preventing Phishing Attacks (Sep. 2004) *available at* http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf (last visited Oct. 19, 2004) [hereinafter NGSS Whitepaper].

A number of Internet-industry groups and technology companies have come out with specific recommendations for changes and improvements in the current Internet technology that they feel would reduce or even eliminate the phishing problem. These groups include the APWG, the Financial Services Technology Consortium, Next Generation Security Software Ltd., Yahoo! Inc. and Microsoft Corporation.

Judging from the number of different sources, there seems to be no shortage of recommendations for how to make the Internet and email more secure. The real questions seem to be (1) which recommendations should be implemented, (2) how should they be done, and (3) when? It is the lack of consensus on these details that has prevented us from already having the recommended upgrades. Despite the current disagreement, the rising tide of phishing scams is prodding the various groups to work together to implement changes to alleviate the problem.[176]

Leading the charge in calling for technology changes to combat phishing has been the APWG. In December 2003, the group proposed four possible technological solutions aimed at preventing phishing scams.[177] These recommendations are:

1. Strong Website Authentication.
2. Mail Server Authentication.
3. Digitally Signed Email with Desktop Verification.
4. Digitally Signed Email with Gateway Verification.

The first recommendation, i.e strong website authentication, "would require all users of legitimate e-commerce and e-banking sites to strongly authenticate themselves to the site

[176] Thomas Claburn, *E-Mail-Authentication Problems Spawn New Apps*, InformationWeek, Sept.21, 2004, *available at* http://www.informationweek.com/story/showArticle.jhtml?articleID=47900731.
[177] The Anti-Phishing Working Group, *Proposed Solutions to Address the Threat of Email Spoofing Scams*, Dec. 12, 2003

using a physical token such as a smart card." In essence, this means that anyone wanting to bank or make purchases online from such websites would first need to swipe a card in a device connected to their computer before being allowed to do so. The APWG notes that this approach is feasible only "for e-commerce and e-banking applications that do not have a large number of users, and where the risk of a phisher gaining access to a user's account are high."[178]

The second recommendation, i.e mail server authentication, would require all email to pass through a gateway server for source verification. The APWG notes that the benefits of this approach include the ease with which it can be configured and the increased ability for legitimate business email to be identified. Potential drawbacks, however, include the facts that both sender and recipient gateways are required and that it does not accommodate e-mail forwarding[179].

The third recommendation, i.e digitally signed email with desktop verification, would have companies that feel they are vulnerable to phishing attacks attach a digital signature to all their outbound email. The digital signature would then be verified for authenticity by the email client used by the recipient. In evaluating the pros and cons of using digital signatures, the APWG notes that this approach would make it impossible to forge the "From:" address without detection. However, it would still be possible for a phisher to obtain a valid digital certificate for a domain that is deceptively similar to that of a target company (e.g. the phisher could use "ebay.custservices.com," which is an entirely different domain from "ebay.com"). Concerning the use of the recipients' email client to verify the

[178] Ibid
[179] Ibid

validity of the digital certificates, the main drawback is that not all email clients currently support the secure email standard that would be employed.

The fourth recommendation, digitally signed email with gateway verification, is almost identical to the third recommendation; however, "instead of relying on the end user's email client to verify the signature on the email, a gateway server at the mail relay level would verify the signatures before they were even received by the receiver's email server." While this approach solves the problem of some recipients' use of email clients that do not support the digital certificate standard, it does not address the problem noted above regarding a phisher's possible use of a deceptively similar domain name.[180]

After providing a detailed and critical discussion of each recommendation the APWG concludes their analysis with the opinion that "a combination of signed email with desktop verification, and either gateway verification or mail server IP verification would solve all aspects of the phishing problem for both consumers and business users." Whether or not that prediction would eventually prove accurate, technological changes of the type recommended by the APWG are generally agreed to be a much needed step in the right direction to address the rising phishing problem.[181]

5.4 Conclusion

As we have seen, phishing and its progeny, require a different solution through legislative bait which the study had been made in the US, UK and Singapore law model. In order to fight such crimes effectively, a strong and robust international regime is needed; and one that is as far as possible harmonized.

[180] Ibid
[181] Financial Services Technology Consortium, *Project Proposal: FSTC Counter-Phishing Initiative*, 2004,p.5

In order for there to be an effective global system to deal with the problem of computer-related crimes, there must be all-around and appropriate approach using a combination of both legally coercive and non-legal measures especially technical software via the Anti-Phishing Working Group (APWG) proposal. The four possible technological solutions including authentication and verification aimed at preventing phishing scams. The international legal framework should consist of approach to the problem with specific treaties for each subject area that is susceptible to universally consistent treatment and model laws in areas that do not, so as to promote as similar and consistent a set of laws as possible for each category of crime. In that way, the overall effect is optimized.