Identity Theft in Cyberspace: Issues and Solutions

Judge Mohamed CHAWKI[1] and Dr. Mohamed S. ABDEL WAHAB[2]

Lex Electronica, vol.11 n°1 (Printemps / Spring 2006)
http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.htm
http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf

---

---

[1] (LL.B), (BA), (LL.M), (DU), (FRSA) is a "Junior Judge" at the Council of State (Conseil d'Etat), a Phd Researcher in cyberlaw at the School of Law, University of Lyon III, France; an expert in cybercrime at the International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme (ISPAC); a fellow of the Royal Society of Arts in the United Kingdom (FRSA) and a member of Cybercrime Institute in France. Mohamed Chawki has taught part-time on Cybercrime and Cyberlaw for the LL.M English programme at the ITI Institute. He has authored many articles in English and French journals and conference papers. He is recipient of numerous academic prizes and the Medal of Excellence. Email: mohamed_chawki@hotmail.com

[2] Assistant Professor, Faculty of Law Cairo University; Vice-Chairman, Chartered Institute of Arbitrators (Cairo Branch); Legal Counsellor and Expert, Information Technology Industry Development Agency (Egypt); Member of the United Nations Expert Group on Online Dispute Resolution; Fellow of the Centre for Information Technology and Dispute Resolution, University of Massachusetts, USA; Of Counsel, Shalakany Law Office, Egypt.
Email: mohamed_wahab@hotmail.com

"He That Filches From Me My Good Name Robs Me Of That Which Enriches Him, And Makes Me Poor Indeed"
- Shakespeare, *Othello* (3.3180-86)

INTRODUTION

Identity theft[3] occurs when someone uses or exploits the personal identifying information[4] of another person such as: name, social security number, mother's maiden name, ID number, etc…to commit fraud[5] or engage in other unlawful

[3] The term "identity" is commonly used arbitrarily and imprecisely in popular media and literature and the terms "identity theft" and "identity crime" are frequently used interchangeably. Occasional misusers are not surprising because in the contemporary context, the traditional meaning underlying those concepts have become increasingly known as information and information technology (IT). The *Oxford English Dictionary* defines "identity" as "*the set of behavioral or personal characteristics by which an individual is recognised*". The traditional use of the word "identity" spoke to one's name, familial membership and occupation. The contemporary meaning of "identity" has, however, assumed a candidly IT connotation that extends traditional meanings to include such things as one's consumer and credit histories, financial accounts, and Social security number. It is this contemporary usage of "identity" that is at issue when it comes to conceptualizing identity theft. *See* J. COLLINS, *Preventing Identity Theft Into Your Business* (New Jersey, John Wiley), [2005], p. 7.

[4] According to the American Heritage Dictionary of the English Language, information is "knowledge of specific events or situations that has been gathered or received by communication, intelligence, or news".

[5] Considerations of the topic of computer fraud raises three major questions: What is it? How extensive is it? Is it illegal? In common with most aspects of the topic, definitional problems abound. In the United Kingdom, the Audit Commission has conducted four triennial surveys of computer-related fraud based on a definition referring to: 'any fraudulent behaviour connected with computerisation by which someone intends to gain financial advantage'. Such a definition is capable of encompassing a vast range of activities some of which may have only the most tenuous connection with a computer. The Council of Europe, in its report on computer-related crime advocates the establishment of an offence consisting of: "*The input, alteration, erasure or suppression of computer data or computer programmes [sic], or other interference with the course of data processing, that influences the result of data processing thereby causing economic loss or possessor loss of property of another person, or with the intent of procuring an unlawful economic gain for himself or for another person*". However this definition is broad in scope. It would appear for example that the proposed offence would be committed by a person who wrongfully uses another party's cash dispensing card to withdraw funds from a bank account. Although there can be little doubt about the criminality of such conduct, the involvement of the computer is purely incidental. In most areas of traditional legal interests, the involvement of computer data does not cause specific legal problems. The respective legal provisions are formulated in terms of results and it is completely irrelevant if this result is achieved with the involvement of a computer or not. However, even in this area computer-specific qualifications are proposed in some countries. When examining the field of financial manipulations, the situation will be different: Many countries require that the offender take an "item of another person's property". The statutory provisions are not applicable if the perpetrator appropriates deposit money. In many legal systems, these traditional provisions also cause difficulties, as far as manipulations of cash dispensers are concerned. The statutory provisions of fraud in most legal systems demand a deception of a person. They cannot be used when a computer is "cheated". The statutory definitions of breach of trust or "*abus de confiance*" which exist in several countries – such as in Belgium, Germany, Japan, France, or Switzerland – only apply to offenders in high positions and not to punchers, operators or programmers; some provisions also have restrictions concerning the protected objects. On such a basis, many European countries looked for solutions *de lege lata* which did avoid stretching the wording of already existing provisions too much. Laws on ICTs fraud have been enacted in Australia, Austria, Denmark, Greece, Germany, Finland, Japan, the Netherlands, Sweden, Norway, Spain, and the USA. Similar reform proposals are being discussed in the United Kingdom while others are already discussing amending and tightening the existing rules. Moreover, the Swedish legislature expanded the provisions on breach of trust to technicians in qualified positions of trust.

activities.[6] Whilst numerous variations of this crime exist, an identity thief can fraudulently use personal identifying information for any of the following purposes: (a) opening new credit card accounts;[7] (b) taking over existing credit card account(s) ; (c) applying for loans; (d) renting apartments; (e) contracting with utility companies; (f) issuing fraudulent checks using another person's name and account number; (g) stealing and transfering money from existing bank accounts; (h) instituting bankruptcy proceedings; and/or (i) obtaining employment using a victim's name and details.[8]

On such account, identity theft is a serious crime that merits due consideration and adequate prevention and combating.[9] Identity theft may be committed in whole or in part by the use of information and communication technologies (ICTs), which dispenses with face-to-face physical contact and allows for distant encounters.

Historically, fraud involved face-to-face communication since physical contact was primarily the norm.[10] Even when remote communication—i.e., snail mail—could be used to set up a fraudulent transaction, it was often still necessary for the parties to meet and consummate the crime with a physical transfer of the tangible property obtained by deceit.[11]

Nevertheless, the proliferation of ICTs has exerted a profound impact upon the nature and form of crime, and has altered the mechanisms of crime commission. Nowadays, perpetrators can use fraudulent e-mails and fake websites to scam thousands of victims located around the globe, and may expend less effort in doing so than their predecessors.[12] These new forms or genera of automated or electronic crime distinguishes online virtual fraud[13] from real-world fraud in at least two important respects: (a) it is far more difficult for law enforcement officers to identify and apprehend online fraudsters; and (b) these offenders can commit crimes on a far broader scale than their real-world counterparts.[14]

---

[6] *See* J. MAY, *Preventing Identity Theft* (N.Y., Security Resources Unlimited), [2004], p. 2.

[7] Credit card fraud consists of the unauthorized use of a regularly issued or cloned credit card. *See, e.g.,* Consumer Action, Preventing Credit Card Fraud, *at:* <http://www.consumer-action.org/English/library/credit_cards/2000_PreventingCreditFraud/index.php> (last accessed Sept. 27, 2004); BBC News, Credit Card Cloning (July 12, 2004), at: <http://www.bbc.co.uk/insideout/east/series3/credit_card_cloning.shtml> (last accessed Sept. 27, 2004).

[8] This type of fraud is known either as 4-1-9 fraud or "advance fee fraud." *See, e.g.,* U.S. Secret Service, Public Awareness Advisory Regarding "4-1-9" or "Advance Fee Fraud" Schemes, *at* <http://www.secretservice.gov/alert419.shtml> (last accessed Sept. 27, 2004). The "4-1-9" reference derives from the fact that these scams often originate in, or are presented as originating in, Nigeria; "4-1-9" is the section of the Nigerian penal code that addresses fraud. In advance fee fraud scams, the target is convinced to part with substantial sums of money, which are characterized as advance fees the payment of which will result in the victim's sharing in a substantial sum of money, usually in the millions.

[9] *See* D. PARKER, *Fighting Computer Crime* (N.Y., Wiley), [1998].

[10] *See* S. BRENNER, *Cybercrime Metrics: Old Wine, New Bottles* (Virginia, Virginia Journal of Law and Technology), [2004], p. 6.

[11] *Ibid.*

[12] *Ibid.*

[13] *See, e.g.,* Federal Bureau of Investigation & National White Collar Crime Center, IFCC 2002 Internet Fraud Report 3, *at* <http://www1.ifccfbi.gov/strategy/2002_IFCCReport.pdf.> Another common type of fraud is non-delivery of merchandise and payment. *See id.* For other types of online fraud, see Internet Fraud Watch, Internet Fraud Tips, *at* <http://www.fraud.org/internet/inttip/inttip.htm> (last accessed Sept. 18, 2004).

[14] *Ibid.*

People whose identities have been stolen can spend months or years and thousands of dollars cleaning up the mess generated by the thieves' exploitation of a good name and credit record.

On a different note, being an identity theft victim can lead to a variety of problems including: (a) being hassled by creditors demanding payments on balances they do not owe[15]; (b) ending up with a ruined credit report[16]; (c) being unable to secure a job, rent an apartment, buy a car or obtain loans[17]; (d) being arrested for crimes the victim did not commit; and (e) finally the cost to law enforcement is not inexpensive, as it could cost between $ 15,000 to $ 25,000 to investigate each case.[18]

PART I: CYBERSPACE IDENTITY THEFT: STATEMENT OF PROBLEM(S)

> *I first was notified that someone had used my Social Security number for their taxes in February 2004. I also found out that this person opened a checking account, cable and utility accounts, and a cell phone account in my name. I'm still trying to clear up everything and just received my income tax refund after waiting four to five months. Trying to work and get all this cleared up is very stressful.*
>
> *A consumer's complaint to the FTC, July 9, 2004*

1- THE PROBLEM OF IDENTITY THEFT

Identity theft is a major problem and a vexing threat. It takes diverse forms and degrees ranging from simple unauthorized use of a credit card to complete takeover of a person's identity.[19] Furthermore, law enforcement officers find it difficult to

---

[15] *See* J. PETRO, *Identity Theft* (Ohio), available at : <http://www.ag.state.oh.us/online_publications/consumer_protection/id_theft_lesson.pdf#search='%EF%83%98%20Being%20hassled%20by%20creditors%20demanding%20payments%20on%20balances%20they%20do%20not%20owe.'> (visited 01/10/2005).

[16] *Id.*

[17] *Id.*

[18] Identity Theft Resource Center [2003].

[19] Most experts believe that common forms of computer related crime are significantly underreported because 'victims may not realize that they have been victimized, may not realize that the conduct involved in a crime, or may decide not to complain for reasons of embarrassment or corporate credibility'. Other reasons for the under-reporting of cybercrime are that 'Further problems arise with the mass victimization caused by offences such as virus propagation, because the number of victims are simply too large to identify and count, and because such programs can continue creating new victims long after the offenders have been caught and punished'. Finally, a factor complicating the gathering and comparison of national crime statistics will be the fact that transnational computer related crimes are, by definition committed in or have effects in at least two States risking multiple reporting or no reporting at all. Thus, much of the information we have on cybercrimes is the product of studies and surveys addressed to individuals working in information security. On such a basis the obvious problem that survey results include only the respondents of people who agreed to participate. Before basing critical decisions on survey information, it is important to find out what the response rate was; although there are no absolutes, in general we aim to trust survey results more when the response rate is high. However, response rates for telephone surveys are often less than 10%; response rates for mail and e-mail surveys can be less than 1%. It is not easy to make any case for random sampling under such circumstances, and all results from such low-response-rate surveys should be viewed as indicating the range of problems or experiences of the respondents rather than as indicators of population statistics.

identify and apprehend online Identity thiefs. This may be due to the fact that they can use technology to conceal their identities and physical location, thereby frustrating law enforcement efforts to locate them.

The traditional model of law enforcement assumes that the commission of an offence involves physical proximity between perpetrator and victim.[20] This assumption has shaped our approaches to criminal investigation and prosecution. Real-world criminal investigations focus on the crime scene as the best way to identify a perpetrator and link him to the crime. However, in automated or cybercrime[21] there may either be no crime scene or there may be many crime scenes, with shredded evidence of the crime is scattered throughout cyberspace.[22]

Accordingly, identifying an electronic crime scene can be a daunting task when the perpetrator may have routed his communications with the victim through computers in three or four countries, with obscure networks that are inaccessible to investigators. Additionally, perpetrators could make things much more difficult and complicated by using technology and encryption techniques that provide a high-level of anonymity or assuming the identity of an innocent person. Moreover, the scale of online identity theft can exceed that of real-world crime in terms of the degree of harm[23] inflicted by a single crime[24].

---

[20] *See* S. BRENNER, *op. cit.* p. 6.

[21] Donn PARKER, who has been studying computer crime since the 1960s, believes we will see the emergence of totally automated crimes, which are available for purchase. *See* Donn PARKER, *Automated Crime*, WindowSecurity.com [2002], *at* <http://secinf.net/misc/Automated_Crime_.html> (last modified Oct. 16, 2002).

[22] *Ibid.*

[23] The principle that the only justification for criminalizing conduct is to prevent harm is traceable in the writings of John Stuart Mill. In *On Liberty*, Mill declared that the sole end for which mankind are warranted, individually or collectively, in interfering with the liberty of action of any of their number is self-protection. That the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others. J. MILL ON LIBERTY 9 (1859). The position Mill takes in this passage, of course, can only be used to justify the articulation of crimes against persons and crimes against property, for only these crimes directly inflict harm upon others. In the years after the appearance of On Liberty, Mills and later scholars expanded the principle so it now reaches a wide variety of harms. *See*, e.g., E.BERNARD, *The Collapse of the Harm Principle*, 90 (J. CRIM. L. & Criminology) 109, 120-39 [1999]. *See* also J. HALL, General Principals in Criminal Law 213-22 (1960). The nature of the harm encompassed by a criminal prohibition is not relevant to the issues under consideration in this article; the issue addressed in the section immediately above is whether or not the varieties of conduct that are currently, and casually, described as cybercrime result in the infliction of socially-intolerable harms that are distinct from those addressed by the repertoire of crimes respectively found in contemporary human societies.

[24] There have been surveys of the incidence and effects of cybercrime on business. *See, e.g.,* U.S. Department of Justice – Bureau of Justice Statistics, Cybercrime Against Businesses [2004] at : <http://www.ojp.usdoj.gov/bjs/pub/pdf/cb.pdf> (last visited Sept. 27, 2004); Computer Security Institute, Ninth Annual CSI/FBI Computer Crime and Security Survey [2004] at : <http://www.gocsi.com/forms/fbi/pdf.jhtml> (last visited Sept. 27, 2004) [Hereinafter CSI/FBI Survey]; Australian CERT, 2004 Australian Computer Crime and Security Survey, at <http://www.auscert.org.au/render.html?it=2001&cid=1920> (last visited Sept. 18, 2004). These surveys generally do not differentiate between crime and cybercrime as *legal* phenomena. The question used in the Bureau of Criminal Justice Statistics' 2001 survey of cybercrime against businesses, for example, asked about the following categories of security threats: embezzlement; fraud theft of proprietary information; denial of service; vandalism or sabotage (electronic); computer virus, other intrusion or breach of computer systems, misuse of computers by employees, unlicensed use of copying of digital products developed for resale, and other.
See U.S. Department of Justice – Bureau of Justice Statistics, 2001 Computer Security Survey 1, *at* <http://www.census.gov/eos/www/css/cssprimary.pdf> (last visited Sept. 27, 2004). The same agency's survey of cybercrime cases handled by state prosecutors audited the following issues: credit card fraud, bank card fraud, computer forgery, computer sabotage, unauthorized access to computer, unauthorized copying or

For example, with respect to bank robbery in the United States, the "average amount netted from an individual [real-world] bank robbery is less than $8,000."[25] While bank robbery is of common occurrence, the scale of the harm resulting from each incident is small. Compare this with an incident that occurred in 1995 when Russian hacker Vladimir Levin and his associates transferred $12 million surreptitiously, and illegally, from Citibank customer accounts.[26]. The $12 million was transferred in increments, each of which exceeded the $8,000 average by far. Despite being ancient, the Levin incident reveals that in cyberspace single attacks, single crimes, could inflict harm of greater magnitude compared to the real world.

The Levin incident is equally a clear demonstration of potential external threat, as ICTs render physical barriers and national borders irrelevant, wealthy countries will find themselves increasingly the object of undesired attention from hackers.[27] The notorious bank robber Willie Sutton allegedly said, when asked why he robbed banks, "because that's where the money is." The same can be said for online identity theft crime, especially financially motivated crime. Individuals and entities in wealthier countries are the source of wealth, and therefore present tempting targets for online criminals. Thus, territorial-based strategies tend not to be effective against online identity theft crime because they are designed to prevent the citizens of one nation-state from preying on each other, not to prevent their preying on citizens of other nation-states.[28]

In this respect, Marc GOODMAN has succinctly stated:

> [L]aw has evolved to maintain order *within* a society. Each nation-state is concerned with fulfilling its obligations to its citizens…[N]o nation can survive if its citizens are free to prey upon each other. But what if they prey upon citizens of *another* society? What if the citizens of Nation A use cyberspace to prey upon the citizens of Nations B and C? Is this a matter that is likely to be of great concern to Nation A? There are historical precedents for this type of behavior that may shed some light on what will ensue in cyberspace. The most analogous involves high-seas piracy and intellectual piracy. Both involved instances in which societies were willing to allow (or even encourage) their citizens to steal from citizens of other societies. In both, the focus was on crimes against property the motivation was purely economic. [T]he conduct took place at the 'margins' of the law: high-seas piracy occurred outside the territorial boundaries of any nation and therefore outside the scope of any laws; eighteenth-century American intellectual property piracy [29]occurred

---

distribution of computer programs, cyberstalking, theft of intellectual property, transmitting child pornography, and identity theft. The CSI/FBI Computer Crime survey focused on these issues: virus insider abuse of net access, laptop/mobile theft, unauthorized access to information, system penetration, denial of service, theft of proprietary information, sabotage, financial fraud, telecom fraud. CSI/FBI Survey, as § II explains, these categories do not represent increments of a new type of criminal activity: cybercrime. Instead, they represent the use of computer technology to commit traditional offenses: crime. Section II considers whether the use of computer technology to commit crimes differs from traditional criminal activity in ways that justify treating it differently for purposes of legal analysis and/or tracking its incidence and effects.

[25] *See* L. LESSIG, *Code and other Laws of Cyberspace* 33 [1999] (Whereas real space requires that you reveal "your sex, your age, how you look, what language you speak, whether you can see, whether you can hear, [and] how intelligent you are," cyberspace requires only that you reveal your computer address.).

[26] *See* S. BRENNER, *op. cit.* p. 19.

[27] *Id.*

[28] *See* S. BRENNER, *op. cit.* p. 19.

[29] In 2002, Rep. Howard Berman introduced the Peer-to-Peer Piracy Prevention Act (2002), which would have

> when the legal status of intellectual property as 'property' was still evolving. Both were outlawed when they became economically disadvantageous for the host countries. One can, therefore, hypothesize that countries may be inclined to tolerate their citizens' victimizing citizens of other nations if (a) the conduct takes place at the margins of the law and (b) results in a benefit to the victimizing nation. The former gives the victimizing nation plausible deniability when confronted with its tolerance of illegal activity; the latter is an obvious motive for tolerating the activity. [30]

Unlike real-world crime, which inflicts harm of various types upon discrete victims, online identity theft can inflict both individual harm and systemic harm. Cyberspace and ICTs have become an essential part of the national critical infrastructures[31]. While identity theft harms individual victims, it is not limited to that; as the National Strategy to Secure Cyberspace rightfully noted, online identity theft can undermine or even destroy a nation's critical infrastructure. This makes it a far more pressing threat than traditional, real-world crime; in a sense, online identity theft erodes the distinction between internal and external threats.

In a world of physical and territorial barriers, societies divide threats into external and internal and allocate the responsibility for dealing with each to respective social institutions. whilst we will always need institutions to deal with traditional forms of real-world threats, nonetheless, we would certainly need a strategy to deal with threats that come from cyberspace or the virtual world. In devising that strategy, we should revist and consider the adequacy and feasibility of the classical and traditional nomenclature of internal and external threats.[32]

Finally, online identity theft does carry the seeds of a potential conflict between national legal systems due to the intrinsic transnational and cross-border implications of such crimes, and the relative variation and divergence of national and regional

---

protected copyright owners who engaged in acts of self-help to protect their works, H.R. 5211, 107th Cong. (2002), 18 U.S.C.A. § 1030; see also H. BERMAN, *The Truth About the Peer to Peer Piracy Prevention Act: Why Copyright Owner Self-help Must Be Part of the P2P Piracy Solution*, available at <http://writ.news.findlaw.com/commentary/20021001_berman.html>. During the summer of 2003, Senator Orrin Hatch proposed destroying the computers of individuals who illegally download material, pointing out that damaging someone's computer "may be the only way you can teach somebody about copyrights." Senator Takes Aim at Illegal Downloads, AP ONLINE, June 18, 2003 (on file with the Yale Journal of Law and Technology). Representative John Carter (R-TX) also suggested that jailing college students for piracy would deter other infringers. Katie Dean, Marking File Traders as Felons, WIRED NEWS, Mar. 19, 2003, at< http://www.wired.com/news/business/0,1367,58081,00.html> In 2004, Congress considered the Inducing Infringement of Copyright Act of 2004, which aimed to hold software creators liable for the infringing activities of their consumers. *See* 2003 CONG US S. 2560, introduced [June 22, 2004] X. JARDIN Induce Act Draws Support, Venom, WIRED NEWS [Aug.26,2004], at <http://www.wired.com/news/print/0,1294,64723,00.html> K . DEAN Copyright Proposal Induces Worry, WIRED NEWS [Sept.11,2004] at http://www.wired.com/ news/politics/0,1283,64870,00.html; K. DEAN, Big Anti-Induce Campaig Planned, WIRED NEWS [Sept. 14, 2004] at : <http://www.wired.com/news/politics/ 0,1283,64935,00.html> Eventually the Induce Act was shelved, ostensibly due to the outcry among technology companies. See K. DEAN, Senate Shelves Induce Review, WIRED NEWS, [Oct. 7, 2004], at <http://www.wired.com/news/politics/0,1283,65255,00.html>. Just a week later, however, former Attorney General John Ashcroft vowed to "build the strongest, most aggressive legal assault against intellectual property crime in our nation's history," *see* Katie DEAN, Ashcroft Vows Piracy Assault, WIRED NEWS, Oct. 14, 2004, at <http://www.wired.com/news/politics/ 0,1283,65331,00.html>.

[30] *See* M. GOODMAN and S. BRENNER, *The Emerging Consensus on Criminal Conduct in Cyberspace* (UCLA J. L. & TECH.), [2002], 3, 4-6.

[31] *See* S. BRENNER, *op. cit.* p. 19.

[32] *See* S. BRENNER, *op. cit.* p. 19.

policies dealing such crimes. This brings into question the effectiveness of territorial-based strategies and policies implemented in a real-world context.

Whilst efforts are underway to establish harmonized and consistent national strategies and policies to combat cybercrime, global condemnation as well as adequate universal policies may not be achieved in the near future at least until all states recognize the importance of ICTs and the need for existence of an adequate regulatory framework.

2- IMPACT AND HARM GENERATED BY IDENTITY THEFT

According to the survey released by US Sentencing Commission on February 2005[33], 9.3 million Americans have been victims and suffered harm[34] as a result by the theft of their identity in the last twelve months.[35] Moreover, in 2003, identity theft losses to businesses and financial institutions totalled nearly $52, 6 billion and consumer victims reported $5 billion in out-of- pocket expenses.[36]

Furthermore, the agency also released a commission report detailing its identity theft program since its inception. The survey found that within a period of one year, 2.28 million consumers discovered that new accounts had been opened, and other fraudulent activities such as renting an apartment or home, obtaining medical care or employment, had been committed in their name.[37]

In those cases, the victims were categorized as follows: 2.28% Existing Credit Card Account Fraud, 1.15% Existing non Credit Cards Accounts Fraud, and 0.83% New Accounts and other Frauds, with a mean fraud loss of $ 5,803 per victim. Existing Credit Card Accounts fraud is the least costly classification, while New Accounts and other Frauds with a mean loss of $ 12,646 is the most serious category.[38] Existing non Credit Card Accounts fraud, which includes existing credit and saving accounts, is the mid-range classification with a mean loss of $ 9.912.[39]

---

[33] *See* F.T.C. Survey 2004.

[34] In penal theory, harm is the focal point between criminal conduct and the punitive sanction In relation to criminal conduct, harm is essential as the relevant effect, the end sought. Without an effect or end, it is impossible to have a cause or means, and everything in penal law associated with causation and imputation would be superfluous. [H]arm is equally necessary in the elucidation of punishment. Harm, in sum, is the fulcrum between criminal conduct and the punitive sanction; and the elucidation of these interrelationships is a principal task of penal theory. *See also, e.g.,* Model Penal Code Articles 210-251(Official Draft and Revised Commentary 1980); United States Sentencing Commission, Guidelines Manual 43-304 (Nov. 2003), *at* <http://www.ussc.gov/2003guid/2003guid.pdf>. Oregon Criminal Justice Commission, Sentencing Guidelines Rules – Crime Seriousness
Scale [2003], *at* <http://arcweb.sos.state.or.us/rules/OARS_200/OAR_213/213_017.html>.

[35] The culpability calculus for these online crimes should be the same as for their real- world analogues. For example, Id-theft, like real-world theft, requires that the offender have acted with the purpose of depriving another of their property. This requirement is made for most other property crimes, such as online fraud, forgery, extortion, etc. The culpability calculus should also remain the same for the "crimes against the person" that migrate into cyberspace, as well as for crimes against the state and crimes against morality. Since human behaviour is a constant in offline and online crime, and since our experience with human misbehaviour has given us a good sense as to the appropriate levels of fault to assign to various misdeeds, we should not need to alter culpability standards, except perhaps to accommodate new crime variations. *See* S. BRENNER, *op. cit.* p. 19.

[36] An increase of 2, 3% with 2003.

[37] *See* F.T.C. Survey 2004.

[38] *Id.*

[39] *Id.*

According to the survey results, 5.2% of all identity theft victims discovered that they were victims of identity theft by spyware.[40] Another 2.51 percent reported that they were victims through online transactions. 2.2 percent reported that they were victims to online hackers and crooks. While most identity thieves use consumer personal information to make purchases,[41] 1.7% of all victims reported that their personal information was misused in non-financial ways, to obtain government documents, for example, or on tax forms.[42]

The most common non-financial misuse took place when the thief used the victim's name and identifying information in the event of apprehension by law enforcement authorities.

Family members and relatives along with friends and neighbours make up half of all identity thieves.[43] Identity theft committed by family members and relatives tend to have greater financial and non-financial implications.

Although there has been recent public concern over electronic methods of obtaining information, most thieves still obtain personal information through traditional rather than electronic channels.[44] In the cases where the methods were known, 68.2% of information was obtained offline, versus only 11.6% obtained online by electronic means.[45]

The length of time to detect is correlated with the amount of money embezzled, or in other words, time is proportionate to money. Victims who take longer to detect fraud are more likely to be victims of new accounts; the most costly type of fraud.

The slowest methods of discovering fraud are: (a) being contacted by creditors; or (b) being turned down for low or bad credit record or history.

The report detailing the FTC's identity theft program since its inception in 1998 states that complaints to the agency about identity theft have nearly doubled each year since then.[46]

---

[40] Identity theft, for example, can consist of either (i) the zero-sum phenomenon we know from the real-world, in which the thief totally deprives an owner of the possession and use of her tangible or intangible property; or (ii) of the non-zero-sum, online version in which the thief takes a copy of intangible property and leaves the owner with the "original." In both instances, the owner suffers a loss of property. However, are the losses identical? In a zero-sum theft, the owner is completely deprived of the possession and use of her property; in a non- zero-sum theft, she is deprived of a quantum of the possession and use of her property. The harm associated with this less-than-zero-sum loss depends, at least in part, on the extent to which the value of the property is a function of its exclusivity; in other words, the extent to which dominion and control of the property is limited. *See* S. BRENNER, *op. cit.* p. 34.

[41] *See* J. KANG: *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1195-99 (1998) (discussing how the private sector seeks to exploit data commercially for database marketing); Jonathan Krim, Web Firms Choose Profit over Privacy; Policies Can Hide Sale of Customer Data, WASH. POST, [July 1, 2003], at A1 (noting that many Web sites promise to protect consumer information from sale to a third party, but instead often rent the information to others). For other studies on the surreptitious collection of information in cyberspace, *see* generally R. Clarke, Information Technology and Dataveillance, available at <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html (1988)>; A. MICHAEL, *The Death of Privacy?* 52 STAN. L. REV. 1461 [2000]; M. PAUL, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609

[42] *See* F.T.C. Survey 2004.

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] Steven A. Hetcher, Commentaries on Eric Posner's Law and Social Norms: Cyberian Signals, 36 U. RICH. L. REV. 327, at 337-38 (2002), citing 15 U.S.C. §§ 45(a)(1), 41-58 (observing that the Federal Trade Commission has spearheaded a number of efforts to protect consumer privacy on the Web pursuant to its

3- FACTORS FACILITATING IDENTITY THEFT

Understanding the factors that contribute to the growth of the identity theft problem certainly helps in devising adequate and effective measures of protection and prevetion.

Generally, there are few scientific studies on identity theft victims, offenders, or incidents, though there are some studies on aspects of identity theft-related crimes such as check and credit card fraud.[47]

The most important findings with respect to victims of such crimes concern the time taken to discover the crime:

- The longer it takes to discover the theft, the greater the victim's loss and suffering.[48]
- Low-income, less-educated victims take longer to discover or report the crime, resulting in greater suffering, especially from harassment by debt collectors, utility cut-offs, and banking problems[49]

With respect to victims' characteristics, they are probably not directly related to identity theft vulnerability.[50] The average age of victims is the fourties. They most often live in a large metropolitan area, and typically do not notice the crime for over 14 months.[51] On a different note, evidence suggests that seniors are less victimized by identity theft than the rest of the population, though they can be targeted in specific financial scams that may or may not involve identity theft. From a racial perspective, African Americans may suffer more from non-credit card identity theft, especially theft of telephone and other utility services and check fraud.[52]

With respect to offenders or identity theft perpetrators, statistical data suggest that the reasons underlying their criminal behaviour are two-fold:

First, it is easy to commit because of the ready availability of personal information on the Internet, or contained in business files accessible to dishonest employees or burglars. Many people are not vigilant in protecting their personal information, and businesses are rarely held accountable for customer information accessed by those unauthorized to do so.[53] *In toto,* Opportunities

---

authority under the Federal Trade Commission Act, which mandates that the agency respond to "unfair" and "deceptive" trade practices). For a discussion of the FTC's role in protecting privacy, *see* Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV 1609(1999]; J. SOVERN, 69 FORDHAM L. REV. 1305 [2001].

[47] Credit card fraud consists of the unauthorized use of a regularly issued or cloned credit card. *See, e.g.,* Consumer Action, Preventing Credit Card Fraud, *at* <http://www.consumer-action.org/English/library/credit_cards/2000_PreventingCreditFraud/index.php> (last accessed Sept.18, 2004); BBC News, Credit Card Cloning (July 7, 2003), *at* <http://www.bbc.co.uk/insideout/east/series3/credit_card_cloning.shtml> (last accessed Sept. 18, 2004). *See* G. NEWMAN, *Identity theft* (U.S. Department of Justice, COPS), [June 2004], p. 7.

[48] Federal Trade Commission [2003a].

[49] *Id.*

[50] In fact, criminal harm differ in gravity, first, because of the differential external effect upon the victim and the community, *e.g.* a battery is obviously less serious than a death; and secondly, by reference to the degree of moral culpability of the offender, *e.g.* a death caused by a motorist's reckless driving is a less serious harm than a death caused by a deliberate murderer.

[51] Federal Trade Commission [2003a].

[52] *Id.*

[53] *Id.*

are legion. There are even websites that offer guides on how to create alternative identities, to access other people's personal identifying information, and a step-by-step guidance on becoming a hacker.

Secondly, victims do not typically discover the crime until some time after it has occurred, in some cases this could be years.[54] If a retailer has lax security, and an offender gets away with using a stolen credit card, the legitimate cardholder may not realize it until receiving the next card statement.[55]

As previously mentioned, familiarity or close connection between the victim and the offender provides opportunities for identity theft because of the availability of personal information among relatives, co-workers, and others. According to the 1999-2001 FTC complaint files close to 11 percent of the complainants knew the offender.[56] Whilst, the FTC's 2003 survey found that 86 percent of victims had no relationship with the offender, other sources claim that up to 60 percent of victims knew or had some information about the offender.[57] Thus, statistical information in this context have be approached with scepticism.

4- INFORMATION PRIVACY AND IDENTITY THEFT

Information in cyberspace is largely intangible. Thus, the architectural conditions that support the nature of ownership in real-world and physical space and which vary in their power and efficacy may not be entirely suitable for cyberspace.[58]

John Perry Barlow, a cyberspace futurologist, stated,

> "*legal concepts of property, expression, identity, movement and context do not apply to us. They are based on matter. There is no matter here.*"[59]

As Barlow suggests, the nature of both information and identity have been transformed by their intangible and evanescent character in cyberspace.[60]

Nevertheless, such view has not prevented other scholars from treating cyberspace like any other "place" and possibly applying some traditional conceptions thereto.[61]

Law confers property rights over profiles of consumer information to collectors, rather than the individual subject, it creates substantial incentives for surreptitious monitoring of consumer activity[62]. This, in turn, alters the fragile balance of privacy and property by permitting accumulation of data that is often enabled by careless consumers who unwittingly consent to such collections,[63] but who continue to

---

[54] *Id.*
[55] *Id.*
[56] Verton [2001].
[57] *Id.*
[58] *See* S. KAKYTL, *Privacy vs. Privacy*, Yale Journal of Law and Technology, [Winter 2004], p. 19.
[59] *See* J. PARLOW, *A Declaration of Independence of Cyberspace in Ibid.*
[60] *See* S. KAKYTL, *op. cit.*
[61] *See* D. HUNTER, *Cyberspace as Place and the Tragedy of the Digital Anti Commons* (Cal. Cal. L. Rev.), 439, 453-54 [2003], 91.
[62] *See* D. HUNTER, *op. cit.*
[63] For example, the Supreme Court has developed a limited, "penumbral" conception of this right flowing from a variety of constitutional sources—the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments, and a host of later decisions that outline (and often complicate) the borders of this right. See U.S. CONST. amend.I,III,IV,V,IX, XIV. *See* Planned Parenthood v. Casey, 505 U.S. 833 (1992); Cruzan v. Director, Miss. Dept. of Health, 497 U.S. 261 (1990); Bowers v. Hardwick, 478 U.S. 186 (1986); Whalen v. Roe, 429 U.S. 589 (1977); Moore v. East Cleveland, 431 U.S. 494 (1977); Roe v. Wade, 410 U.S. 113 (1973); Eisenstadt

retain expectations of informational privacy.[64] This transition towards third-party possession or ownership, in turn, has radically altered the pre-existing balance between privacy and property contemplated in real space by subordinating the protection of informational privacy to the accumulation of database property.[65] Some of these changes are attributable to an innate transformation in the value of information itself. Although information has always served as a resource, it was always "relegated to the position of supporting other resources."

Today, however, since the advent of digital technology, information has become a valuable commodity in and of itself, leading to a shift towards its commercialization.[66] Thus, the economic base of society has shifted from industry to information, marking a transition into the third millennium of information economy and digital revolution.

Vast amounts of personal information are now primed for harvest, distribution, and disclosure to third parties on the Internet, often without the individual's knowledge.[67] In cyberspace, identity thieves are looking for sensitive personal information, and there are many pieces of information that could be utilized. Some of the most common are[68]:

- **Social Security Numbers (SSN)** — These number was created to keep an accurate record of earnings and pay retirement benefits on those earnings.
- **Date of Birth (DOB)** — Date of birth, in conjunction with other pieces of information, can be used in many ways to compromise a person's identity.
- **Current and Previous Addresses and Phone Numbers —** Both can be used in cybercrime and identity theft to enable an offender to assume the identity of the victim or to obtain more information thereabout..
- **Current and Previous Employment Information —** Such information can be used to jeopardize the victim's identity.
- **Financial Account Information —** This includes checking and saving accounts, credit cards, debit cards, and financial planning information. Such information is a rich source for an identity thief to commit financial cybercrimes.
- **Mother's Maiden Name —** In many instances, the maiden name of the victim's mother may be used as the password for financial accounts and is easily available through public record information.
- **Other Personal Information —** This includes passwords, passcodes, email addresses as well as photos. Such information could be utilized to

---

v. Baird, 405 U.S. 438 (1972); Stanley v. Georgia, 394 U.S. 557 (1969); Loving v. Virginia; 388 U.S. 1 (1967); Griswold v.Connecticut, 381 U.S. 479 (1965). In addition, numerous federal and state enactments affect the enforcement of privacy rights in various ways. *See* e.g., 5 U.S.C. § 552a (2000); CAL. PENAL CODE § 630 (Deering 2003); MASS. ANN. LAWS ch. 214,§ 1B (Law. Co-op 2002); N.Y. CIV. RIGHTS LAW § 50 (McKinney 2002); R.I. GEN. LAWS § 9-1-281 (2002); WIS. STAT§ 895.5 (2002).

[64] *See* D. HUNTER, *op. cit.*

[65] *Ibid.*

[66] *Ibid.*

[67] *Ibid.*

[68] *See* J. PETRO, *op. cit.*

obtain access to other sensitive information or to facilitate total or partial identity theft.

5- INFORMATION ACCESSIBILITY AND MECHANISMS OF CYBERSPACE IDENTITY THEFT

Cyberspace[69] makes it possible for anyone to gather personal information about others.[70] Much of this information is available for a price on the Internet.[71]

In a recent case, a Californian women downloaded credit reports from the same websites used by landlords to conduct background checks on prospective tenants.[72] Some sites sent her the credit reports, after nothing more than a mouse click accompanied by a promise to use the information legally. At the time of her arrest, the women had financial data on more than three hundred people.[73]

Similarly, a curious news correspondent recently decided to explore how easy it is to get supposedly confidential financial records from such credit-checking sites. It took him only two minutes and $ 14.95 to access his spouse's credit report.[74]

On such account, it could be said that ICTs and cyberspace had facilitated the following:[75] (a) First, making public records quickly accessible to anyone who wants them, even though most of this information has always been a matter of public record, how to access it has not been common knowledge. Now anyone with a computer and Internet access can do it.[76]

(b) Secondly, allowing identity thieves to work anonymously or after assuming the identity of an innocent victim, and access information anywhere in the world.

A smart crook working on the Internet may turn a tax-free gain of as much as $ 50.000 per week. There are many ways in which information could be obtained online amongst which are: cyber-trespass, phony or sham websites and phishing and pharming, spoofing, spyware, electronic bulletin boards, information brokers, internet public records, and malicious applications such as trojan horses.

In the following pages we shall provide a brief overview of each of the above-mentioned techniques.

---

[69] In fact, the term cyberspace literally means 'navigable space' and is derived from the Greek word *kyber* (to navigate). In William Gibson's 1984 novel, the original source of the term, cyberspace refers to, a navigable, digital space of networked computers accessible from computer consoles, a visual, colourful, electronic, Cartesian datascape known as 'The Matrix' where companies and individuals interact with, and trade in, information. Since the publication of this novel, the term cyberspace has been re-appropriated, adapted and used in a variety of ways, by many different constituencies, all of which refer in some way to emerging computer-mediated communication and virtual reality technologies. Here, we refocus the definition back to the envisaged by Gibson, so that cyberspace refers to the *conceptual space* within ICTs, rather than the technology itself. *See* W. GIBSON, *Neuromancer* (New York, Grafton), [1984]; M. DODGE, *Mapping Cyberspace* (N.Y, Routeldge), [2001] p. 1.

[70] *See* ex., R. GELMAN, *Protecting Yourself Online, The Definitive Resource on Safety, Freedom and Privacy in Cyberspace* (Harpcollins Publishers), [1998].

[71] *See* ex., M. BARKARDJIEVA, *Internet Society: The Internet in Everyday Life* (Sage Publishers), [2005].

[72] *See* J. MAY, *op. cit.*

[73] *Id.*

[74] *Id.*

[75] *Id.*

[76] *Id.*

5-1 Cyber-Trespass or Hacking:[77]

Cyber-Trespass is becoming more common to commit identity theft. It can include many different ways of using a computer and network to steal information, money, or other valuables. Cyber-trespass offences include: embezzlement,[78] unlawful appropriation,[79] corporate / espionage,[80] plagiarism,[81] and DNS cache poisoning.[82]

In April 2005, the DSW shoe chain revealed that hackers had stolen data from 1.4 million credit and debit card transaction at 108 stores in the U.S.[83] The breach also included account numbers from 96,000 check transactions. Moreover, some hackers bypass and breach electronic security,[84] and password barriers[85] to gain access to a

[77] To some extent, the definition of cyber-trespass/hacking may vary depending on the context. Generally speaking, a 'hack' used to be a clever solution to a restriction. A hack was an ingenious, but temporary, fix or 'make-do' rather than an attack on a computer system. However, in 1960s malicious hacking started with compromising telephone systems and stealing telephone services or eavesdropping. It soon spread to computers and networks. When we extend this term to the individuals who practice the art of hacking, however, the definitions become murkier. The Oxford English Dictionary (1998) defines hacker as "a person who or thing that hacks or cuts roughly" or "a person whose uses computers for a hobby, esp. to gain unauthorized access to data". In his book *The Hacker Crackdown* Brice STERLING takes a rather positive view of the activity, explaining that the term *hack* 'can signify the free-wheeling intellectual exploration of the highest and deepest potential of computer systems. 'Hacking can involve the heartfelt conviction that beauty be found in computers, that the fine aesthetic in a perfect program can liberate the mind and spirit'. This is hacking as it was defined in Steven LEVY's much praised history of the pioneer computer milieu, *Hackers* published in 1994. Hacking or gaining unauthorized access to computer system, programs, or data, open a broad playing filed for inflicting damage. The *New Hackers Dictionary* offers six definitions for hacking and hacker: (a) A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to many users, who prefer to learn only the minimum necessary; (b) A person who enjoys the intellectual challenge of overcoming or circumventing limitations; (c) A person good at programming quickly; (d) An expert in a particular language; (e) A person who programs enthusiastically; (f) A malicious meddler who tries to discover sensitive information by poking around. On such a base hacking can manifest itself in many ugly forms including "cyber murders". A British hacker hacked into a Liverpool hospital in 1994 and changed the medical prescriptions for the patients. A nine-year-old patient who was 'prescribed' a highly toxic mixture survived only because a nurse decided to re-check his prescription. The hacker's motive - he wanted to know 'what kind of chaos could be caused by penetrating the hospital computer'! Others have not been so lucky. An underworld don who was only injured in a shoot out was killed by an overdose of penicillin after a hacker broke into the hospital computers and altered his prescription.

[78] This involves misappropriating money or property for the criminal's own use that has been entrusted to him by someone else.

[79] This crime differs from embezzlement in that the criminal was never entrusted with the valuables but gains access from outside the organization and transfers funds, modifies documents giving him title to property he doesn't own, or the like.

[80] In which persons outside/inside the company use the network to steal trade secrets, financial data, confidential data.. etc.

[81] This is the theft of someone else's intellectual work with the intent of passing it off as one's own.

[82] Is a form of unauthorized interception in which intruders manipulate the contents of a computer's DNS cache to redirect network transmissions to their won servers.

[83] *See* S. LEVY, *Grand Theft Identity* (N.Y., Newsweek), [September 5, 2005), pp. 41.

[84] The main goal of Internet security is to keep proprietary information confidential, to preserve its integrity, and to maintain its availability for those authorized to view that information. When information is accessed and examined by unauthorized individuals, it is no longer confidential. By connecting to the Internet organizations have made their information assets far more vulnerable to unauthorized access and breaches of confidentiality. If data are tampered with, modified, or corrupted by intruders there is a loss of information integrity. Some times this can happen inadvertently, but most often it is the intentional act of a hacker or a disgruntled employee seeking revenge. Finally, if information is deleted or becomes inaccessible to authorized users, there is a loss of availability. *See* R. SPINELLO, *Regulating Cyberspace: The Policies and Technologies of Control* (U.S.A, Spinello), [2002] p. 207.

[85] A password is a type of secret authentication word or phrase used to gain access. Passwords have been used since Roman times. Internal to the computer, passwords have to be checked constantly. So, all computers try to

company's computer server, or sometimes the server of an ISP.[86] They then steal names, addresses, credit card numbers, and other information.[87]

In one case, individuals hacked into an ISP computer server and stole the records of 10,000 customers. They then sent a message to the ISP offering to return the stolen data for $30,000. In the end, the hackers were apprehended and charged extortion – but only after considerable damage.[88]

5-2 Phoney or Sham Websites: Phishing and Pharming

Identity thieves can also set up and use sham or phoney websites to commit their crimes.

Phishing is a clear variation and manifestation of phoney communications and websites.[89] It is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.[90] Thus, phishing is essentially a method of committing credit card fraud, identity theft and/or generic theft. Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them.

In one case, a cyber-criminal decided to impersonate the FBI in order to obtain Social Security numbers and other personal information.[91] He set up a complete fake website with the FBI logo. As many citizens like to request information from the government, the presence of such a request form on the website contributed to the perception of its authenticity.[92] Visitors to the web site furnished the information

---

"cache" passwords in memory so that each time a password is needed the user does not need to be asked. If someone hacks into the memory of a computer, he can sift the memory or page files for passwords. Password crackers are utilities that try to 'guess' passwords. One way, the dictionary attack, involves trying out all the words contained in a predefined dictionary of words. Ready-made dictionaries of millions of commonly used passwords can be freely downloaded from the Internet. Another form of password cracking attack is 'brute force' attack. In this attack, all possible combinations of letters, numbers and symbols are tried out one by one till the password is found out. *See* B. STERLING, *The Hacker Crackdown* (Batman Books) pp. 50 -51.

[86] ISPs can further be broken down into two separate groups: Online Service Providers—such as America Online, Prodigy and Compuserve, who provide both Internet access as well as a system for posting and exchanging content—and Internet Access Providers, who simply provide direct access to the Internet.

[87] *See* J. MAY, *op. cit.*

[88] *Id.*

[89] The word phishing comes from the analogy that Internet scammers are using e-mail lures to fish for passwords and financial data from the sea of Internet users. The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords from unsuspecting AOL users. Since hackers have a tendency to replacing "f" with "ph" the term phishing was derived. Available at <http://www.webopedia.com/DidYouKnow/Internet/2005/phishing.asp>

[90] See Anti-Phishing Working Group, What Is Phishing? *at* <http://www.antiphishing.org/> (last accessed Sept. 18, 2004).

[91] *See* J. MAY, *op. cit.*

[92] *Id.*

requested, including their credit card numbers to pay the ten dollar application fee.[93] Surprisingly, not only such victims did not get a penny of what they paid but also expended much time and effort fixing damaged credit histories.

In another recent case, a phisher e-mail claiming to be from MSN was sent to computer users. It said: "*we regret to inform you that technical difficulties arose with our recent update. Unfortunately part of our customer data base and back up system became inactive*".[94] This authentic-looking message offered a toll free telephone number in addition to a web link and urged individuals to click on the link to the phony web site. The message then informed individuals that they needed to enter their personal information. Later on, they realized that they were victims to this phishing attack.

Similar in nature to phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. The victim's browser, however will show you are at the correct website, which makes pharming more serious and more difficult to detect. Whilst phishing attempts to scam people one at a time, pharming allows the scammers to target large groups of people at one time through domain spoofing.[95]

5-3 Spoofing

A closely interconnected and often confused term with phishing and pharming is spoofing. A "spoofer", in Internet terms, is defined generally as the "cracker" who alters, or "forges," an e-mail address, pretending to originate a message from a different source address than that which he or she truly has.[96] There are many ways an attacker may do this, and there are many types of attacks. The attacker may do this to gain access to a secured site that would accept the "hijacked" address as one of few permissible addresses, or more maliciously, the reason may be to hide the source of any type of attack.[97] "Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords)."[98]

---

[93] *Id.*
[94] *Id.*
[95] See <http://www.webopedia.com/TERM/p/pharming.html>
[96] A "cracker" is someone whose interest includes unauthorized entry and modification of computer systems. Although not the case, this term has become synonymous with the term "hacker," who is someone intensely interested in complex computer systems, but is often a systems operator or administrator who detects, repairs, and prevents the break-in and damage done by "crackers."
[97] *See* R. FARROW, *Source Address Spoofing: Forged Addressess aid Internet Attacks. Here's What to do About Them,* NetworkMagazine.com, [May 1, 2000], *at* <http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleID=8702815>. (visited, 12/08/2005).
[98] In fact, spoof attacks occur at the Protocol layer level. When the spoofer's goal is to either gain access to a secured site or to mask his or her true identity, he or she may hijack an unsuspecting victim's address by falsifying the message's routing information so that it appears to have come from the victim's account instead of his or her own. He or she may do so through the use of "sniffers." Since information intended for a specific computer must pass through any number of other computers while in transit, the data essentially becomes fair game, and sniffers may be used to essentially capture the information en route to its destination. Sniffer software can be programmed to select data intended for any or every computer. Thus, the spoofer can use the recipient's address, which is found in the header, and configure his or her own machine to emulate the recipient's machine. When information comes along the network that is intended for the true recipient, the spoofer can receive it

Furthermore, the spoofer may send an e-mail to the victims' accounts claiming to be from a system administrator, and request users to change their passwords to a specified string, threatening to suspend their account if they do not comply.[99] Similarly, they might send an e-mail claiming to be from a person in authority, and request users to send them a copy of a password file or other sensitive information.

5-4 Spyware

Spyware is computer software that can be used to gather and remove confidential information from any computer without the knowledge of the owner.[100] Everything the surfer does online, including his passwords, may be vulnerable to spyware.[101] Spyware can put anyone in great danger of becoming a victim of identity theft.

Moreover, some forms of spyware can be installed on the computer from a remote location without the identity thief ever having physical access to the victim's computer.[102] We would think that it would be difficult for the average person to find spyware, but it is not. Typically it is used by employers monitoring employees' computer use and parents who monitor their children's computer use. Spyware could also be used by a not-too-trusting spouse who wants to know what his or her spouse is doing online. Additionally, some file sharing programs also contain spyware. Sometimes this information is used merely to send advertisements for products and services that may interest the surfer.[103]

5-5 Electronic Bulletin Boards

Chat rooms and electronic bulletin boards have become breeding grounds for identity theft.[104] When criminals have obtained personal identifying information such as credit card numbers or social security numbers, they visit hacker chat rooms and post messages that they have personal information for sale.[105]

In one case, a former employee of an insurance company stole a database containing sixty thousand personnel records and sold some of the private information over the Internet.[106] He posted a message on an electronic bulletin board announcing that he had thousands of names and social security numbers for sale.[107] Further

---

instead. In this way, the spoofer is able to gain entry into those sites to which the recipient had access, and thus has the ability to now steal passwords, credit card information, and other personal information, and use that information for any number of illegitimate purposes. Additionally, the spoofer can also automatically send a packet back to the sender, which makes the sender believe that its message was properly received. The spoofer may also alter the original e-mail and then relay it on to the intended recipient, or he or she can change the message in its entirety, and send it to a different recipient or recipients altogether. If and when the recipient responds, that message will be routed back to the original sender, not to the spoofer. The spoofer, however, will need to sniff the response off the network for the attack to go unnoticed. Conversely, when the spoofing involves unsolicited bulk e-mail, the attacker will choose not to sniff the responses off the network, thereby remaining unacquainted with the effects of his or her attacks. These hostile reactions have been the cause for spammers to mask their identities initially. *See Id.*

[99] *Id.*

[100] *See*, on spywares PC Magazine (N.Y., Wiley), [2005], p. 8.

[101] *Id.*

[102] *Id.*

[103] *See* J. McNamara, *Secrets of Computer Espionage: Tactics and Countermeasures* (London, Wiley Publishing, Inc.), [1998].

[104] *See* J. MAY, *op. cit.* p. 17.

[105] *Id.*

[106] *Id.*

[107] *Id.*

investigation revealed that he had also posted the credit card number of a former supervisor.

Surprisingly, some offenders are sufficiently brazen to post their offerings on websites that are sort of fraudster eBay. At one site, it was posted by a member of the Shadow crew organisation that for $200 a person can get 300 credit cards without the security codes printed on the back of the card. If card numbers with the code are required, the cost will be 200$ for 50 cards.[108]

In April 16, 2004, a Manchester, New Hampshire man was sentenced on eight felony counts related to a website and electronic bulletin boards where he posted for sale thousands of Social Security Numbers and other personal information belonging to employees of Global Crossing, as well as threats to injure or kill.[109]

5-6 Information Brokers

Information brokers have been around for decades, however, a new breed of information broker has emerged in recent years; the kind that sells personal information to anyone requesting it electronically via the Internet.[110] Driven by greed, some information brokers are careless when they receive an order. They fail to verify the identity of the requesting party and do little, if any, probing into the intended use of the information.

In one case, an online information broker was sued by the parents of a young woman slain by an Internet stalker.[111] it was alleged that for a nominal fee the broker sold personal information that led the killer to the victim's place of employment. He then ambushed her as she got into her car after leaving work.[112]

In another very recent 2005 case, a Chicago based engineer, aged 42, was paying $40 a year to have the Trans Union credit agency monitor his credit report.[113] Unfortunately, when an identity thief somehow got the victim's information and used it to open new credit lines in stores, the stores authorized his credit with one of TransUnion's rivals, Equifax. Over a period of eight weeks, the offender charged $3,000 on credit cards and spends an additional $1,000 on telephone calls.[114] The victim, driven by the will to clear his name and records, spent hundred of dollars sending out certified letters to close accounts and, haunted by visions of overseas hucksters, even called the State Department.[115]

In another case, a 24-year old Indian man who at the time (March 2005) worked for Gurgaon-based online marketing firm named Infinity eSearch, allegedly sold information on 1,000 bank accounts to an undercover journalist working for The Sun for £ 2,750. The victim has since claimed that he was only a middleman and that he did not sell data collected by his employer.[116] Infinity eSearch has said the company does not handle any data for the banks named in the Sun report, and that the victim

---

[108] *Id.*
[109] Available at <http://www.cybercrime.gov> (visited 14/10/2005).
[110] *See* Identity Theft and Data Brokers (WTOP), available at <http://www.wtopnews.com/?sid=434596&nid=97> (visited 02/10/2005).
[111] *See* J. MAY, *op. cit.*
[112] *Id.*
[113] *See* S. LEVY, *op. cit.*
[114] *Id.*
[115] *Id.*
[116] *Id.*

did not have access to confidential data of any kind through his employment with the company, according to press reports. But the case has raised fears of an anti-outsourcing blacklash if Indian firms are seen to be careless with the data they handle.[117]

In the case of *R* v *Thompson*,[118] Thompson, a computer programmer, was employed by a bank in Kuwait. Whilst so employed, he devised a plan to defraud the bank. Details of customer's accounts were maintained on computer. A number of these accounts were dormant, i.e, no transactions had taken place over a significant period of time. Thompson devised a program which instructed the computer to transfer sums from these accounts to accounts which he had opened with bank. In an effort to minimise the risks of detection, the transfers were not to be made until Thompson had left the bank and was on a plane returning to England. On his return, Thompson opened a number of accounts with English banks and wrote to the manager of the Kuwaiti bank instructing him to arrange for the transfer of the balances from his Kuwaiti accounts.[119] This was done but subsequently his conduct was discovered and Thompson was detained by the police. Charges of obtaining property by deception were brought against him and a conviction was secured. An appeal was lodged on the question of jurisdiction. Whilst not denying any of the facts received above, Thompson argued that any offence had been committed in Kuwait and, therefore, that the English courts had no jurisdiction in the matter. This plea did not commend itself to the Court of Appeal which held that the offence was committed at the moment when the Kuwaiti manager read and acted upon Thompson's letter. At this stage, Thompson was subject to the jurisdiction of the English courts.[120]

5-7 Internet Public Records

People search and genealogy websites have come under fire and some consumers are concerned that personal information online can be used to commit identity theft. Privacy advocates have become extremely concerned about the ease with which people can obtain personal information online.

Local State and Federal governments have begun to make all public records of kinds available online. For example, birth and death records have long been available to the public through state offices, but people had to physically visit the court house. Now it can be accessed by computer.

In one recent case, Judy McDonough, a 56-year-old occupational psychologist from Shaw, England, suffered a disturbing blow: she realized someone had stolen her identity from Internet.[121] But by that time, the thief had already opened two credit cards in her name, taken out three bank loans and ordered £ 2, 3000 in debt in three years.[122] McDonough tried six times to report the crime to the local authorities, and bank officers made lacklustre efforts to help. Finally, McDonough turned to her Member of Parliament for assistance. Hitherto the thief – who McDonough suspects is a relative- has not been caught.[123]

---

[117] *Id.*
[118] *See* [1984] 1 WLR 962 at pp. 967-8, *in* C. REEDS, *op. cit.* p. 248.
[119] *Id.*
[120] *Id.*
[121] *See* S. LEVY, *op. cit.*
[122] *Id.*
[123] *Id.*

In another very recent case,[124] an American citizen tried to sell his house in California. He contacted several real estate agents to discuss with them a listing for the house. He was then informed by these agents that his house has been rented to individuals that he was not aware of or have even agreed to rent his house to. Someone was collecting the rent on his house, and upon checking with the USA county records he found out that someone has used his name and arranged to fake his signature, made a power of attorney in his name and received loans on his property, bought a business in his name and has accumulated a huge amount of financial burden in his name as well. The personal information of this victim was found and downloaded from Internet.

5-8 Malicious Applications: Trojan Horses

In this context, a Trojan horse could be defined as an application that appears to be benign, but instead performs some type of malicious activity.[125] A Trojan can be disguised as a game, an e-mail attachment, or even a Web page.[126] As soon as the victim runs or opens the camouflaged application, the Trojan installs itself on the hard drive and then runs each time Windows is started.[127]

Successful Trojan attacks are based on exploiting both human and computer security weaknesses. First and foremost, to get a Trojan onto a computer the attacker has to do some social engineering to convince the target to do something that installs and runs the Trojan.[128] He will also need to deal with any electronic defenses that are in place, such as firewall, antivirus, or anti-Trojan software.[129]

Once installed, the Trojan will carry out whatever evil deeds that its creator designed it for. This may include: uploading files; viewing the desktop in real time; retrieving cached passwords; logging keystrokes; editing the registry…etc.[130]

It is worthnoting that unlike worms, Trojans do not self-replicate. After the rouge application is installed on a system, it does not try to spread itself to other computers. If it does, then it is considered to be a virus or a worm.

6- USING STOLEN IDENTITES

Offenders use victim's personal information in diverse and numerous ways, amongst the most common examples of usage are:[131]

- They may call the credit card issuer to change the billing address on the victim's credit card account. The imposter then runs up charges on the victim's account. Because his bills are being sent to a different address, it may be some time before the victim realizes that there is a problem. In the District of Delaware, one defendant was sentenced to a thirty-three months imprisonment and $160,910.87 in restitution, and another defendant to a forty-one months imprisonment and $126,298.79 in restitution for obtaining names

[124] Privacy Rights Clearing House (UCAN), [Feb. 2005].
[125] *See* M. ERBSCHLOE, *Trojans, Worms and Spyware* (Oxford, Heinmann), [2005], p. 21.
[126] *Id.*
[127] *Id.*
[128] *See* J. McNAMARA, *op. cit.*
[129] *Id.*
[130] *Id.*
[131] *See* FTC, *Take Charge, Fighting Back Against Identity Theft* (Report),[2004].

and Social Security Numbers of high-ranking military officers from an Internet website and using them to apply on-line for credit cards and bank and corporate credit in the officers' names.[132]

- They may open new credit card accounts in the victim's name. When they use the credit cards and do not pay the bills, the delinquent accounts are reported on the victim's credit report.
- They may use it in illegal drug or human trafficking. In the District of Oregon, seven defendants have been sentenced to imprisonment for their roles in a heroin/methamphetamine trafficking organization, which included entering the United States illegally from Mexico and obtaining SSNs of other persons.[133] The SSNs were then used to obtain temporary employment and identification documents in order to facilitate the distribution of heroin and methamphetamine. In obtaining employment, the defendants used false alien registration receipt cards, in addition to the fraudulently obtained SSNs, which provided employers enough documentation to complete employment verification forms. Some of the defendants also used the fraudulently obtained SSNs to obtain earned income credits on tax returns fraudulently filed with the Internal Revenue Service.[134] Some relatives of narcotics traffickers were arrested in possession of false documents and were charged with possessing false alien registration receipt cards and with using the fraudulently obtained SSNs to obtain employment. A total of twenty-seven defendants have been convicted in the case, fifteen federally and twelve at the state level.[135]
- They may use the information to make telephone calls. In *United States v. Bosanac*, no. 99CR3387IEG the defendant was involved in a computer hacking scheme that used home computers for electronic access to several of the largest United States telephone systems and for downloading thousands

---

[132] *United States v. Lamar Christian, CR 00-3-1 (D. Del. Aug. 9, 2000); United States v. Ronald Nevison Stevens, CR 00-3-2*

[133] *See UnitedStates v. Jose Manuel Acevez Diaz*, CR 00-60038-01-HO (D.Or. Aug. 10, 2000); *UnitedStates v. Pedro Amaral Avila*, CR 00-60044-01-HO (D.Or. Nov. 7, 2000); *United States v. Jose Arevalo Sanchez*; CR 00-60040-01-HO (D.Or. Nov. 21, 2000); *UnitedStates v. Maria Mersedes Calderon*, CR 00-60046-01-HO (D.Or. May 10, 2000); *UnitedStates v. Victor Manuel Carrillo*, CR 00-60045-01-HO (D.Or. Oct. 24, 2000); *UnitedStates v. Alfonso Flores Ramirez*, CR 00-60043-01-HO (D.Or. Aug. 30, 2000); *UnitedStates v. Cleotilde Fregoso Rios*, CR 00-60035-01-HO (D.Or. Nov. 7, 2000); *United States v. Javier Hernandez Lopez*, CR 00-60038-01-HO (D.Or. Aug. 10, 2000); *United States v. Ranulfo Salgado*, CR 00-60039-01-HO (D.Or. Jan. 18, 2001); *United States v. Angel Sanchez*, CR 00-60080-01-HO (D.Or. Aug. 31, 2000); *UnitedStates v. Cresencio Sanchez*, CR 00-60143-01-HO (D.Or. Dec. 13, 2000); *UnitedStates v. Piedad Sanchez*, CR 00-60131-01-HO (D.Or. Jan. 9, 2001); *United States v. Noel Sanchez Gomez*, CR 00-60034-01-HO (D.Or. Dec. 12, 2000); *United States v. Kelly Wayne Talbot*, CR 00-60081-01-HO (D.Or. Dec. 31, 2000); *United States v. Jose Venegas Guerrero*, CR 00-60037-01-HO (D.Or. Nov. 21, 2000); *State of Oregon v. Fred Harold Davis*, Case No. 006276FE (Jackson County Dec. 13, 2000); *State of Oregon v. Pablo Macias Ponce*, Case No. 004317MI (Jackson County Sept. 13, 2000); *State of Oregon v. Raul Navarro Guiterrez*, Case No. 005257FE (Jackson County Nov. 8, 2000); *State of Oregon v. Miranda Mae Byrne*, Case No. 004363FE (Jackson County Jan. 9, 2001); *State of Oregon v. James Tracy Campbell*, Case No. 002376FE (Jackson County Oct. 18, 2000); *State of Oregon v. Ann Marie Eaton*, Case No. 002378FE (Jackson County Aug. 25, 2000); *State of Oregon v. Michael Scott Gilhousen*, Case No. 002225FE (Jackson County Nov. 7, 2000); *State of Oregon v. Robert Dean Golden*, Case No. 002726FE (Jackson County Oct. 18, 2000); *State of Oregon v. Annetta Lynn Kelley*, Case No. 002377FE (Jackson County July 24, 2000); *State of Oregon v. Gerald Jerome King*, Case No. 003594FE (Jackson County Oct. 31, 2000); *State of Oregon v. Micah John Right*, Case No. 002374FE (Jackson County Sept. 7, 2000); and *State of Oregon v. Todd Ivan Williams*, Case No. 004533FE (Jackson County Jan. 12, 2001).

[134] *Id.*

[135] *Id.*

of calling card numbers (access codes).[136] The defendant, who pleaded guilty to possession of unauthorized access devices and computer fraud, used his personal computer to access a telephone system computer and to download and transfer thousands of access codes relating to company calling card numbers. In taking these codes, the defendant used a computer program he had created to automate the downloading, and instructed his co-conspirators on how to use the program. The defendant admitted that the loss suffered by the company as a result of his criminal conduct was $955,965. He was sentenced to eighteen months' imprisonment and $10,000 in restitution.

- They may counterfeit checks or credit or debit cards, or authorize electronic transfers in another name, and drain the bank account.[137] In a recent case, a women got back from her vacation in Las Vegas to find out that her sister has been using her credit card ($584) and has committed fraudulent activities in her name. The victim did not order or receive any of the items that were charged. Moreover, when she got home, she opened all her mail and discovered that she has been denied housing because her sister had stolen her identity.
- They may file for bankruptcy under another name to avoid paying debts they have incurred or to avoid eviction.
- They may buy a car by taking out a loan in another name. In *United States v. Wahl*, No. CR00-285P [138] (W.D. Wash. sentenced Oct. 16, 2000), the defendant obtained the date of birth and Social Security number of the victim (who shared the defendant's first, last name and middle initial). He then used the victim's identifying information to apply online for credit cards with three companies and to apply online for a $15,000 automobile loan. He actually used the proceeds of the automobile loan to invest in his own business. (The defendant, after pleading guilty to identity theft, was sentenced to seven months imprisonment and nearly $27,000 in restitution).[139]
- They may get identification such as a driver's license issued with their picture, in the victim's name.
- They may give the victim's name to the police during an arrest. In such case if they do not show up at court on the hearing date, a warrant for arrest will be issued in the victim's name.

By and large, the first part or section of this research focused on the concept of Identity theft, its different forms, interests at stake, and provided an overview of the diverse mechanisms for committing identity theft.

In the following part or section, we shall focus on potential solutions to combat and prevent identity theft as well as addressing the need for establishing an effective regulatory and legislative framework to deter offenders. Furthermore, an overview of possible ICT applications that could be used to prevent or, at the least, mitigate the occurrence and impact of identity theft will be provided.

---

[136] (S.D. Cal. filed Dec. 7, 1999),
[137] *See* Privacy Rights Clearing House (UCAN), [Sep. 2004].
[138] [W.D. Wash. sentenced Oct. 16, 2000].
[139] *Ibid.*

PART II: CYBERSPACE IDENTITY THEFT PROPOSED SOLUTIONS

From logical, theoretical, and pragmatic perspectives, knowing the problem, risks associated therewith, and the ills resulting therefrom is an indispensable step towards a possible solution. Furthermore, such determination constitutes an integral part of devising effective vaccines and serums to eradicate and prevent this evil.

Having discussed the diverse aspects of the vexing problem of identity theft, we shall now address some of the potential solutions thereto. Thus, we shall first analyze and ascertain the need for adequate regulatory and legislative approaches, and conclude by exploring and scrutinizing a number of technical solutions or approaches 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, and hence reducing identity theft in cyberspace.

1- REGULATORY STRATEGIES AND LEGISLATIVE APPROACHES: A QUEST FOR GLOBAL HARMONIZATION

1.1. National and Regional Strategies: The European Approach

The adaptation of established legal norms and standards to new forms of identity theft in Europe resulted in a multitude of novel and complex legal questions.

Under this sub-section, we shall focus on two forms of anti-identity theft legislation: (i) the protection of privacy; and (ii) the protection against economic and financial crime.

1.1.1. The Protection of Privacy:

Legislative framework against infringement of privacy rights is existent in most European countries both on national and regional levels. Despite the ongoing efforts for harmonization and unification of data protection and privacy standards spurred by a number of supra-national European instruments in this context such as the 2002 EU Directive on Privacy and Electronic Communications, a pragmatic analysis of such efforts reveal that some differences are still persistent, especially regarding the procedural and institutional framework, which merit further consideration.

On such a basis, a comparative analysis of the protection of privacy results in distinguishing four main categories of privacy infringements pertinent to EU privacy legislation: (a) violation of substantive privacy rights; (b) violation of formal legal requirements; (c) violation of access rights; and (d), negligence in security measures.

Infringements of substantive privacy rights includes the following offences:

- The illegal entering, modification, and/or falsification of data with the intent to inflict harm or damage.
- The storage of incorrect data. This act in most countries is covered by the general offences of information and in some countries by additional statutes within the privacy laws.
- The illegal disclosure, dissemination, obtaining of and/or access to data, acts which are covered in most laws, however, to different degrees.
- The unlawful use of data.

However, due to the uncertainties in implementing substantive provisions, many legal systems rely to a great extent on an additional group of offences against formal legal requirements or orders of supervisory agencies. These formal provisions also vary considerably within the national legislation.

Formal offences which can be found in many European privacy legislations are: the infringement of some regulations, prohibitions, or decisions of the surveillance authorities; the refusal to give information or the release of false information to the surveillance authorities; obstructing the work of surveillance authorities; the refusal to grant access to property and the refusal to permit inspections by surveillance authorities; the obstruction of the execution of a warrant; the failure to appoint a controller of data protection in the company, as well as neglecting to record the grounds or means for the dissemination of personal data.

The third category of privacy infringement is the individual's rights of information or freedom of information. With regard to a party's right of access, in many countries such as in Luxembourg and Sweden – it is an offence to give false information, not to inform the registered party or not to reply to a request.

With respect to the fourth category, some legislators penalize for negligence of security measures by an administrative fine or a penal sanction.[140]

1.1.2. Computer Related Economic Crimes[141]

As a reaction to the acceleration and increase in computer-related economic crimes,[142]a reform for combating and preventing computer-related economic crimes has been underway since the 1980s. Due to the accelerated pace of advancement in ICTs and the emergence of new forms of computer-related financial crimes, which posed a serious threat to the development of e-commerce and progression of the global information economy, many states within the EU and all around the globe have enacted new legislations or amended existing laws to penalize and prevent illegal access to computer systems as well as computer-related crimes that undermine the stable infrastructure of cyberspace.

In this context, it is worth noting that the Council of Europe Budapest Convention on Cybercrime marks a new era of international cooperation in penal and criminal matters. Mindful of the necessity to deter actions directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such systems, networks and data, by providing for the criminalisation of such conduct, as described in the Convention, Member States of the EU as well as other signatories have sought to provide a supranational regulatory framework in order to effectively combate computer-related offences, by facilitating the detection, investigation and prosecution of such criminal offences at both the domestic and international level, and by providing arrangements for fast and reliable international co-operation.[143]

---

[140] *See* Denmark, section 27(1) no. 2 Private Registers Act. Luxembourg, section 36 of the Act Regulating the Use of Normal Data. Also see for Italy, Article 36(2) of the new Data Protection Act.

[141] In fact, the definition of the term computer in most countries often suffers from overbreadth. It includes for example handheld calculators, new kitchen stoves and electronic typewriters. These problems are avoided in a 1983 Tennessee statue which defines "computer" in terms of function as "a device that can perform substantial computation, including numerous arithmetic or logic operations, without intervention by a human operator during the processing of a job. *See* Tennessee Code An. Section 39-3-1403(2).

[142] *See* U. SIEBER, *op. cit* p. 69.

[143] See *infra* p.41

By and large, in order to combat identity theft and ensure the protection of privacy and personal data in cyberspace, effective legislative framework for combating cybercrime is an absolute necessity to dispense with new forms of financial and computer-related crimes such as hacking (cyber-trespass) and computer espionage.

1.1.1. Cyber-Trespass

Cyber-trespass has been previously addressed whilst analyzing the diverse mechanisms for identity theft in cyberspace. However, in this context our focus shall be on the necessity for devising adequate and efficient legislative policies that target cyber-trespass and consider hacking a serious criminal offence.

In those jurisdictions with developed criminal norms that target computer misuse, such as the United States, the policy has been to penalize the initial unauthorized access of a computer system.

Similarly, in some jurisdictions, penalizing computer trespass is absolute regardless of the motivation or reason for the intrusion.[144] Thus, the act of unauthorized access in itself constitutes a criminal offence regardless of the underlying reasons and even if they were legitimate or even if no harm was intended.

In response to the new cases of "hacking", many countries developed new statutes protecting a "formal sphere of secrecy" for computer data by criminalising the illegal access to or use of a third person's computer or computer data.

On such a basis, legislation covering wiretapping and unauthorised access to data processing and communication systems have therefore, been enacted in Canada, Denmark, Germany, Finland, France, the Netherlands, Norway, Spain, Sweden, Switzerland, the United Kingdom,[145] and the United States.[146]

Moreover, some of the new laws which have been proposed demonstrate various approaches, which range from provisions penalizing "mere" access to DP-systems,[147] to those punishing access only in cases where the accessed data are

---

[144] M. WASIK, *Crime and the Computer* (Oxford, Rendon Press Oxford), [1998] p. 70.

[145] It became quite clear after the decision of the House of Lords in *Gold and Schifreen* that there was no specific criminal offence in England which could be used to deal with the unauthorized use of a legitimate user's password or the use of a false password to gain access to information stored in a computer. There is no general offence of impersonation in English law and none of the traditional property offences in the Theft Act 1986 and 1978 can be made out on these facts. It had been throught by (R.A.BROWN) that an offence under the Forgery and Counterfeiting Act 1981 might be utilized in such a case, but a prosecution under this statue, while proving successful at trial, ultimately resulted in the convictions being overturned on appeal. This meant a substantial limitation on the prospects for successful prosecution of the hacker or other computer misuser, where no dishonest or malicious intent at the time of access could be proved, and where no offence consequent upon access had been committed. On this point see M. WASIK, *op. cit.* p. 71.

[146] *See* for Canada, Article 342.1 Criminal Code ; for Denmark, Section 263 (2) and (3) Penal Code, for Germany Section 202a Penal Code; for Finland, chapter 38 Section 8 of the Penal Code (as amended 1990); for France, Article 462-2 Criminal Code, amended in 1988; for Greece, Article 370 C (2) Criminal Code, as amended in 1988; for the Netherlands, Article 138a (1), (2) Criminal Code, amended 1992; for Norway, Section 145 Penal Code, amended 1987; for Spain, Article 256 Criminal Code 1995; for Sweden, Section 21 Data Protection Act; for the UK, Sections 1, 2 Computer Misuse Act 1990; for Switzerland, Article 143bis Criminal Code; for the USA, the Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510-2521, 2701-2710, 3117, 3121-3126), the Computer Fraud and Abuse Act of 1984 and 1986 (codified at 18 U.S.C. §§ 1029, 1030) as well as different state laws.

[147] See for example, Australia, Denmark, England, Greece and the majority of states of the United States of America.

protected by security measures,[148] where the perpetrator has harmful intentions,[149] where information is obtained, modified or damaged,[150] or where a minimum damage is caused.[151] Other countries, [152] combine one or more of these approaches with a "basic" hacking offence and the creation of qualified forms of access (in a more serious "ulterior" offence) carrying more severe sanctions.

1.1.2. Computer Espionage

Ranking amongst the most serious forms of cybercrime that pertain to national security, the act of computer espionage raises the following question: to what extent pure acquisition of incorporeal information can or should be covered national legislations?

Many European countries, such as Belgium, Italy, are reluctant to apply the traditional provisions on theft and embezzlement to the unauthorised "appropriation" of secret information, because these legislations generally require that corporeal property is taken away with the intention of permanently depriving the victim of it.[153]

In Japan, according to Articles 235, 252 and 253 of the Penal Code, the definition of the intention of unlawful appropriation has been broadened to include the intent to use property only temporarily. Nevertheless, Japanese law still requires the taking of tangible property and cannot be applied if data are accessed via telecommunication facilities. Whatever might be the case, enacting national laws or amending existing laws to efficiently deal with computer-related crimes such as hacking and espionage is a fundamental prerequisite to securing the confidentiality and secrecy of electronic data and personal information, and assists in the progressive development of cyberspace as a secure medium for trading and communicating.

By and large, having addressed the European approach to providing a safe harbour regulatory and legislative framework for combating identity theft and cybercrime, it is necessary to shed some light on the American approach to such problems.

1.2. Prosecuting Identity Theft under Federal Criminal Laws: American Approach

There are a number of federal laws applicable to identity theft, some of which may be used for prosecution of identity theft offences, and some of which exist to assist victims in repairing their credit history.

The primary identity theft statute is 18 U.S.C. § 1028(a)(7) and was enacted on October 30, 1998, as part of the Identity Theft and Assumption Deterrence Act (Identity Theft Act). The Identity Theft Act was needed because 18 U.S.C. § 1028 previously addressed only the fraudulent creation, use, or transfer of identification ***documents***, and not the theft or criminal use of the underlying personal ***information*****.**

The Identity Theft Act added Section §1028(a)(7) which penalizes fraud in connection with the unlawful theft and misuse of personal identifying information, regardless of whether the information appears or is used in documents.

---

[148] See for example, Germany, the Netherlands, and Norway.
[149] See for example, Canada, France, Israel, New Zealand, and Scotland.
[150] Some states of the USA.
[151] Spain.
[152] See for example, Finland, the Netherlands, the United Kingdom.
[153] *See* for example, the Penal Code of Belgium section 461, and the Italian Penal Code sections 624 and 646.

Section 1028(a)(7) provides that it is unlawful for anyone who:

"Knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law..."

The Identity Theft Act amended the penalty provisions of §1028(b) by extending its coverage to offenses under the new §1028(a)(7) and applying more stringent penalties for identity thefts involving property of value.

Section 1028(b)(1)(D) provides for a term of imprisonment of not more than fifteen years when an individual commits an offence that involves the transfer or use of one or more means of identification if, as a result of the offence, anything of value aggregating $1,000 or more during any one year period is obtained. Otherwise, §1028(b)(2)(B) provides for imprisonment of not more than three years.

Furthermore, the Identity Theft Act added §1028(f) which provides that attempts or conspiracies to violate §1028 are subject to the same penalties as those prescribed for substantive offences under §1028.

Moreover, the Identity Theft Act amended § 1028(b)(3) to provide that if the offence is committed to facilitate a drug trafficking crime, or in connection with a crime of violence, or is committed by a person previously convicted of identity theft, the individual is subject to a term of imprisonment of not more than twenty years.

Additionally, the Identity Theft Act added § 1028(b)(5) which provides for the forfeiture of any personal property used or intended to be used to commit the offence.

Section §1028(d)(3) defines "means of identification", as used in §1028(a)(7), to include "*any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual*." It covers several specific examples, such as name, social security number, date of birth, government issued driver's license and other numbers; unique biometric data, such as fingerprints, voice print, retina or iris image, or other physical representation; unique electronic identification number; and telecommunication identifying information or access device.

Section§1028(d)(1) modifies the definition of "document-making implement" to include computers and software specifically configured or primarily used for making identity documents.

The Identity Theft Act is intended to cover a variety of individual identification information that may be developed in the future and utilized to commit identity theft crimes. The Identity Theft Act also directed the United States Sentencing Commission to review and amend the Sentencing Guidelines to provide appropriate penalties for each offence under Section §1028.

The Sentencing Commission responded to this directive by adding U.S.S.G. §2F1.1 (b) (5) which provides the following: "*(5) If the offense involved – (A) the possession or use of any device-making equipment; (i) the unauthorized transfer or use of any means of identification unlawfully to produce or obtain any other means of identification; or (ii) the possession of [five] or more means of identification that*

unlawfully were produced from another means of identification or obtained by the use of another means of identification, increase by 2 levels. If the resulting offense level is less than level 12, increase to level 12".

These new guidelines take into consideration the fact that identity theft is a serious offence, whether or not certain monetary thresholds are met. For most fraud offenses, the loss would have to be more than $70,000.00 for the resulting offence level to be level 12.

In providing for a base offence level of 12 for identity theft, the Sentencing Commission acknowledged that the economic harm from identity theft is difficult to quantify, and that whatever the identifiable loss, offenders should be held accountable.

Identity theft offences will usually merit a two-level increase because they often involve more than minimal planning or a scheme to defraud more than one victim. (U.S.S.G. § 2F1.1(b)(2)).

Identity theft offences may also provide for two to four-level upward organizational role adjustments when multiple defendants are involved. (U.S.S.G. § 3B1.1)

As previously mentioned, identity theft is often committed to facilitate other crimes, although it is frequently the primary goal of the offender. Schemes to commit identity theft may involve a number of other statutes including identification fraud (18 U.S.C. §1028(a)(1) - (6)), credit card fraud (18 U.S.C. §1029), computer fraud (18 U.S.C.§ 1030), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. §1343), financial institution fraud (18 U.S.C. §1344), mail theft (18 U.S.C. § 1708), and immigration document fraud (18 U.S.C. § 1546).

For example, computer fraud may be facilitated by the theft of identity information when stolen identity is used to fraudulently obtain credit on the Internet. Computer fraud may also be the primary vehicle to obtain identity information when the offender obtains unauthorized access to another computer or web site to obtain such information. These acts might result in the offender being charged with both identity theft under 18 U.S.C. §1028(a)(7) and computer fraud under 18 U.S.C. § 1030(a)(4).

Regarding computer fraud, it should be note that U.S.S.G. § 2F1.1(c)(1) provides a minimum guideline sentence, notwithstanding any other adjustment, of a six month term of imprisonment if a defendant is convicted of computer fraud under 18 U.S.C. § 1030(a)(4).

It is worth noting in this context that identity theft schemes may involve other statutes. For example, this includes the case of an offender who fraudulently obtains identity information by posing as an employer in correspondence with a credit bureau. This offender might appropriately be charged with both identity theft under 18 U.S.C. §1028(a)(7) and mail fraud under 18 U.S.C. §1341.

Moreover, an offender who steals mail thereby obtaining identity information might appropriately be charged with identity theft under 18 U.S.C. § 1028(a)(7) and mail theft under 18 U.S.C. §1708.

Furthermore, the offender who fraudulently poses as a telemarketer thereby obtaining identity information might appropriately be charged with both identity theft under 18 U.S.C. § 1028(a)(7) and wire fraud under 18 U.S.C. § 1343.

1.3. International Strategies: The Council of Europe Convention on Cybercrime

Cyberspace is a primarily a borderless society**.** Thus, there is a persisting need to establish global norms and standards that govern conduct and behaviour in this virtual world. On such account, national or regional policies, despite their necessity, may not be the best option available. This calls for universal or global regulatory framework that takes into account the inherent transnational and sweeping impact of cybercrime in general and identity theft in particular.

Despite the intrinsic difficulty in harmonizing or unifying criminal and penal policies, being a manifestation of sovereign power and authority, the stakes of cyberspace have instigated states to tread upon this erratic and wobbly territory marking a new epoch of cooperation in criminal and public law matters.

Incontrovertibly, the above-mentioned Council of Europe Convention on Cybercrime is a huge step towards realizing the long lost hope for cooperation in the field of criminal law and cybercrime.[154]

The primary purpose of the Convention[155] is to harmonize domestic substantive criminal law offences and investigation procedures.[156]

The Convention drafters' principal concerns were two-fold:[157] first, they wanted to ensure that the definitions were flexible enough to adapt to new crimes and methods of committing existing crimes as they evolve.[158] Secondly, the drafters wanted the Convention to remain sensitive to the legal regimes of nation-states.[159]

These concerns were especially challenging in the human rights area because states have different moral and cultural values.[160] For example, European nations have a much higher degree of privacy protection than the United States.[161] The United States, on the other hand, has stronger speech protection than other states.[162]

---

[154] See *Supra.*

[155] On November 23, 2001, in Budapest, Hungary, the United States and 29 other countries signed the Council of Europe Cybercrime Convention, the first multilateral instrument drafted to address the problems posed by the spread of criminal activity on computer networks. The Cybercrime Convention will require parties to establish laws against cybercrime, to ensure that their law enforcement officials have the necessary procedural authorities to investigate and prosecute cybercrime offenses effectively, and to provide international cooperation to other parties in the fight against computer-related crime. *See* Council of Europe, Convention on Cybercrime (ETS No. 185),
available at <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> (last visited Sept. 21, 2004).

[156] *See* Preamble (recognizing the need to ensure a proper balance between human rights and law enforcements needs); (articulating the need to balance human rights with individual privacy in defining crimes and implementing investigative procedures); U.S. Senate Committee on Commerce, Hearing on Security Risks in Electronic Commerce, in FDHC Political Transcripts (July 16, 2001) (statement of U.S. Senator Ron Wyden (D-OR) Chairman) (discussing the Convention and stating, "we're trying to balance security versus liberty"). Available at:
<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

[157] *See* Explanatory Memorandum, available at <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

[158] *Id.*

[159] *Id.*

[160] *Id.*

[161] *See* S. HOPKINS, *Cybercrime Convention: A Positive Beginning to a Long Road Ahead* (Journal of High Technology Law), [2004], p. 105.

[162] *See* Draft Hate Speech Protocol to the Convention [Sept. 5, 2002], available at: <http://assembly.coe.int//Documents/WorkingDocs/doc02/EDOC9538.htm>.

To further its purpose, the Convention also empowers parties to restrict or eliminate criminalization of certain offences, and limit investigation procedures by reservation. The Convention's drafters have, thus, attempted to strike an equitable balance between crime definitions, the investigation needs for law enforcement, and individual rights.[163]

The Convention is broken up into four main segments, with each segment consisting of several Articles.

The first segment or section outlines the substantive criminal law aspects which all ratifying countries should implement to prevent the listed offences.[164]

The second section delineates the procedural and investigation requirements and standards to which individual countries must adhere.

The third section sets out guidelines for international cooperation that most commonly involve joint investigations of the criminal offences listed under section one.[165]

Finally, the fourth section contains the provisions pertaining to the signing of the Convention, territorial application of the Convention declarations, amendments, withdrawals, and the ever-important, federalism clause.[166]

Amongst the most important crimes covered by the Convention, whose criminalization exerts a profound impact on preventing and combating identity theft are:

> (a) "***illegal access***" or access to a computer system without right.[167] "Access" deals with entering into any part of the computer system, such as hardware components and stored data but it "does not include" the mere sending of an e-mail message to a file system. The corresponding US provision is found in the Computer Fraud and Abuse Act of 1986 ("CFAA") ;[168]
>
> (b) "***illegal interception***" where Article (3) of the Convention criminalizes the interception, without right, of non-public transmissions of computer data, whether by telephone, fax, email, or file transfer.[169] This provision is aimed at protecting the right to privacy of data communications.[170] One element of this offence is that interception occurs through "technical means" which is the surveillance of telecommunications through the use of electronic eavesdropping or tapping devices.[171] However, it should be noted that this provision does not

---

[163] *Id.*

[164] Many of the crimes committed against individuals and businesses are legislated against in the European Convention on Cybercrime, and include identity theft, child pornography, and fraud.

[165] Convention, *op. cit.*

[166] *Id.*

[167] See Article 2 of the Convention. Examples of unauthorised intrusions are hacking, cracking, or computer trespassing. Intrusions such as these allow identity thieves to gain access to confidential data, such as passwords and social security numbers.

[168] The act makes it unlawful to either knowingly access a computer without authorization or to exceed authorization and obtain protected or restricted data. (18 U.S.C § 30 (2000))

[169] It should be noted in this context that the non-public nature relates only to the transmission and not the transferred data transferred.

[170] Explanatory Report, *op. cit.*

[171] *Id.*

exhaustively define what forms of interception are lawful and which are not, leaving this a matter of national policy;

(c) "***data and system interference***", where Articles (4) and (5) criminalize the intentional damaging, deletion, deterioration, alteration, suppression of computer data without right, or serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data; and

(d) "***misuse of devices***", where Article (6) establishes, as separate and independent offences, the intentional commission of illegal acts regarding certain devices that are utilized for the commission of the listed offences under the Convention.[172] This Article not only covers tangible transfers but also the creation or compilation of hyperlinks facilitating hacker access to these devices.

However, in this context, a vexing issue arises with respect to "dual-use devices" or multi-purpose devices that could have more than one function. In such cases, the drafters intended the latter Article to relate to devices that are objectively "designed, or adapted, ***primarily*** for the purpose of committing an offence. Furthermore, this provision requires both a general intent and a specific intent that the device is used for the purpose of committing any of the offences listed under the Convention.

Having addressed a number of regulatory and legislative policies and efforts needed to combat cybercrime and identity theft, we shall move on to shed some light on a number of technical precautions and techniques that would certainly minimize the risk of identity theft, and act as preventive measures to cybercrime.

2- TECHNICAL APPROACHES

ICTs are a double-edged sword that, despite being used to commit online identity theft, could act as risk minimizing or mitigating factors to enhance privacy and secure the confidentiality and secrecy of personal identifying information.

2.1. Minimizing Recurrences: Precautionary Guidelines[173]

(i) People are encouraged to request and use password-protected credit cards, and bank and phone accounts. To avoid using easily available information like their mother's maiden name, their birth date, the last four digits of their SSN, their phone number, or a series of consecutive numbers.

(ii) People must refrain from giving out their personal information on the phone, through emails, or over the Internet unless they have initiated the communication or are sure they know who they are dealing with. Identity thieves are clever, and have posed as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their SSN, mother's maiden name, account numbers, and other identifying information. Before consumers share any personal information, they must confirm that they are dealing with a legitimate organization.

[172] In many cases, black markets are set up to facilitate the sale or trade of "hacker tools," or tools used by identity thieves in the commission of cybercime.
[173] See the FTC 2004 Report.

(iii) People should be careful when storing their financial records, birth date, and bank account numbers on their computer, and should ensure that virus protection software should be updated regularly,[174] and patches for the operating system and other software programs should be installed to protect against intrusions and infections that can lead to the compromise of their computer files or passwords. Ideally, virus protection software should be set to automatically update each week.

(iv) People are recommended to use firewall programs, especially if they use a high-speed Internet connection like cable, DSL that leaves their computer connected to the Internet 24 hours a day. The firewall program will allow them to stop uninvited and unauthorized access to their computer.

(v) It is advisable not to open files sent from an unknown source or a stranger, or click on hyperlinks or download programs from untrustworthy sources. People should be careful about using file-sharing programs. Opening a file could expose their system to a computer virus or a program known as "spyware", which could capture their passwords or any other information as they type it.[175]

(vi) Consumers and businesses are encouraged to use a secure browser and encryption software when entering into online transactions or sending their personal information to trusted sites. Examples of the encryption technologies used to ensure the security and confidentiality of email and web-based communications are Secure Multipurpose Internet Mail Exchange Protocol (S/MIME) and Pretty Good Privacy (PGP) for e-mails and Secure Sockets Layer technology (SSL) and Secure Hypertext Transfer Protocol (S-HTTP) for web-based communications. Both S/MIME and PGP are powerful cryptographic products that guarantee both privacy and authentication. Even if the information is intercepted, it remains completely unreadable. As regards SSL and S-HTTP, whilst the former creates a secure connection between a client and a server and has the added feature of being able to encrypt all data passed between the client and the server, including data at the Internet Protocol (IP) level, the latter only encrypts HTTP-level messages and is designed to transmit individual messages securely. Thus, both could be seen as complementary rather than competing technologies.

---

[174] The term *computer virus* was formally defined by Fred COHEN in 1984, while he was performing academic experiments on a Digital Equipment Corporation VAX computer system. Fred Cohen is best known as the inventor of computer viruses and virus defence techniques. A computer virus is a specific type of malicious code that replicates itself and inserts copies or new versions of itself in other programmes, when it is executed with the infected program. It replaces an instruction in the target program with an instruction to transfer control to the virus which is stored in the memory. Whenever the program transfer instruction is executed, it dutifully transfers control to the virus program, which then executes the replaced instructions and performs its work of inserting itself in other programs. There are presently more than 10,000 identified viruses affect the PC and Apple operating systems. In addition, a few viruses affect other operating systems such as UNIX. There are, however, no known viruses that attack the large-scale mainframe computer operating systems. There are, however, no known viruses that attack the large-scale mainframe computer operating systems. This probably because the virus makers have easy access to the desk top and laptop computing environments, and because of the proliferation and casual exchange of software for these environments. On this point see experiments with computer virus. Available at <http://all.net/books/virus/part5.html> (visited 03/10/2005).

[175] *See* P2P File Sharing, available at <http://www.ftc.gov/bcp/conline/pubs/alerts/sharealrt.htm> (visited 03/10/2005), also see Spyware, available at <http://www.ftc.gov/bcp/conline/pubs/alerts/spywarealrt.htm> (visited 03/10/2005).

(vii) Before disposing of a computer, people must delete all stored personal information and format their hard drive. Nevertheless, deleting files or reformatting the hard drive may not be enough because the files could still be retrieved from the computer's hard drive. Thus, a "wipe" utility program could be used to overwrite the entire hard drive.

(viii) Accounts' passwords should not be disclosed to anyone, as accounts can be hijacked, and people can find unexpected charges on their bills and statements.

(ix) Finally, beware of phishing, spoofing, spam attempts by being diligent, prudent, and sceptical about suspicious communications.

2.2. Utilizing State-of-the-Art Technologies:

As previously mentioned, the sharp and rough edges of technology should be mitigated and ICTs should be harnessed to combat the ills of modern technology. ICT applications are in a constant state of flux and advancement in the field is progressing at an accelerated pace that is difficult to trace. On such a basis, it is always advisable to upgrade and implement top-notch latest technologies to safeguard privacy and personal identifying information against identity theft and cybercrime.

The current state of affairs reveal that top high-tech technologies utilized for security purposes include: biometric applications, tokens, padded cells, cryptography and digital signature technologies etc…

2.2.1 Biometric Security Solutions

Biometrics,[176] is the study of measurable biological characteristics. In computer security, biometrics refers to authentication[177] techniques that rely on measurable physical characteristics that can be automatically checked. There are several types of biometric identification schemes:[178]

- **face**: the analysis of facial characteristics

[176] The term *biometics* is derived from the Greek words bio (*life*) and metric (*(to measure*). Among the first known examples of practised biometrics was a form of member printing used in China in the fourteenth century, as reported by the Portuguese historian Joao de Barros. The Chinese merchants were stamping children's palm and footprints on paper with ink to distinguish the babies from one another. In the 1890s an anthropologist and police desk clerk in Paris named Alphonse Bertillon sought to fix the problem of identified convicted criminals and turned biometrics into a distinct field of study. He developed a method of multiple body measurements that was named after him (the Bertillonage technique – measuring body length. *See* J. CHIRILLO, *Implementing Biometric Security* (N.Y., Wiley), [2003], p.1; For a brief study on how Finger-Scan technology works, see S. NANAVATI, *Biometrics: Identity Verification in a Networked World* (N.Y., John Wiley), [2002], p. 48.

[177] Authentication is the process whereby an entity verifies that the claimed identity of another entity is its true identity. For applications involving computers and telecommunications, this is done for the purpose of performing trusted communications between them. We distinguish between *machine-by-machine authentication* (or simply, *machine authentication*) and *human-by-machine authentication* (or simply, *human authentication*). *See* L. GORMAN, *op. cit.* p. 3.

[178] Authenticator types can be combined to reap benefits in security or convenience or both. This is commonly called, *multi-factor authentication*. A common multi-factor authenticator is an ATM card, which combines a token with a secret (PIN). If a user has difficulty remembering the secret, a token may be combined with a biometric. The photo-ID is the traditional 2-factor ID plus biometric. Rarely is a secret combined with a biometric ID, since the objective is usually to get rid of the task of memorizing the secret. There has not been much application for 3-factor authentication.

- **fingerprint**: the analysis of an individual's unique fingerprints
- **hand geometry**: the analysis of the shape of the hand and the length of the fingers
- **retina**: the analysis of the capillary vessels located at the back of the eye
- **iris**: the analysis of the colored ring that surrounds the eye's pupil
- **signature**: the analysis of the way a person signs his name.
- **vein**: the analysis of pattern of veins in the back if the hand and the wrist
- **voice**: the analysis of the tone, pitch, cadence and frequency of a person's voice.

Though the field is not yet entirely developed, many scholars and scientists believe that biometrics will play a critical role in the future of security and especially in electronic commerce.[179]

Biometric can provide a greater degree of security than traditional authentication methods, meaning that resources are accessible only to authorise users and are kept protected from unauthorised access.[180]

Because biometrics are difficult if not impossible to forget, they can offer much greater convenience than systems based on remembering multiple passwords, or on keeping possession of an authentication token.[181]

For computer applications in which a user must access multiple resources, biometrics can greatly simplify the authentication process – the biometric replaces multiple passwords, in theory reducing the burden on both the user and the system administrator.

Applications such as point-of-sale transactions have also begun to see the use of biometrics to authorise purchases from prefunded accounts, eliminating the need for cards.[182] Moreover, biometric authentication allows for association of higher levels of rights and privileges with a successful authentication. Highly sensitive information can more readily be made available on biometrically protected network than on one protected by passwords.[183]

---

[179] The Hong Kong government began to issue identity cards several years ago and has been successful with its program. It is a "smart" card with an embedded silicon chip that performs data storage and computational functions.
See, Rina CHUNG, *Hong Kong's* 'Smart' Identity Card: Data Privacy Issues and Implications for a Post-September 11th America (4 ASIAN-PAC. L. & POL'Y J.), 519, 531 [2003].

[180] *See* S. NANAVATI, *op. cit.* p. 4.

[181] The password has been the standard for computer network access for decades. If the system employs some secure challenge-response password transmission protocol [20, 21] and limits the number of failed authentication attempts (as most systems should), it will be resistant to most attacks. Since passwords can be lent, this choice does not offer non- repudiation. Nor does it offer compromise detection. Password maintenance is straight forward, however it may be costly when passwords are forgotten, especially if system policy mandates good, non-dictionary passwords and frequent changes. A commonly quoted cost for each instance of password reset is $30-$50. The problem with a password-only system is that people either forget their password, incurring maintenance costs, or they choose a memorable password, which might also be guessable and that weakens the security of the system. A password plus token combination is the more secure choice for authenticating network access. The penalty is an increased system cost for the token, reader, and system software. There is a convenience cost for the user as well because she still has to remember a password for the token and also has to remember to carry the token. *See* L. GORMAN, *op. cit.* p. 19.

[182] *See* S. NANAVATI, *op. cit.* p. 4.

[183] *Id.*

Finally, the potential application of biometric technology for the prevention of identity theft is infinite. Any situation that allows for an interaction between man and machine is capable of incorporating biometrics. The benefits of biometrics will make the use of technology, and consequently, its acceptance, inevitable.[184]

Despite the real and actual benefits of biometric applications to both business and consumers in relation to identity theft, public acceptance of biometrics is not necessarily inevitable. It will only ensue if the privacy and trust concerns associated with technology are effectively addressed.

Whether biometrics are privacy's friend or foe, it is entirely dependent upon how the systems are designed and how the information is managed. While the biometric industry has made some positive initial steps, without private sector data protection legislation, companies are still free to use biometric data without restriction.[185] It must be recognized that the use of biometrics needs to conform to the standards and expectations of a privacy-minded society. The responsibility to ensure that this new technology does not knowingly or unknowingly compromise consumer privacy lies not only with businesses, but also with consumers[186]. Businesses must acknowledge and accept their obligation to protect their customers' privacy. Prior to introducing any biometric system, the impact that such an application may have on consumer privacy should be fully assessed. To appropriately and effectively balance the use of biometric information for legitimate business purposes with the consumer's right to privacy; companies should adopt and implement the fair information practices and requirements discussed in this article. Voluntary adoption of such practices is essential if there is to be meaningful privacy protection of consumers' biometric data in the private sector.[187]

---

[184] *See* J. VACCA, *Biometric Security Solutions* (London, Prentice Hall), [2002].

[185] *Id.*

[186] Legislations against infringements of privacy have been adopted in most European countries with data protection laws of more or less general character. An analysis of these acts shows that different international actions have already achieved a considerable uniformity in the general administrative and civil law regulations of the national privacy laws. In spite of this tendency, some differences in these regulations can be remarked. These differences concern the legislative rationale, the scope of application, the procedural requirements for starting the processing of personal data, the substantive requirements for processing personal data, and finally the respective control institutions. On such a basis a comparative analysis to the protection privacy will distinguish four main categories of criminal privacy infringements, which can in particular be found in the European privacy laws: infringements of substantive privacy rights (a), infringements against formal legal requirements (b), infringements of access rights (c), and neglect of security measures (d). The category of "crimes against privacy" is constituted by infringements of substantive privacy rights and includes the following offences: The illegal entering, modification, and/or falsification of data with the intent to cause damage ; The storage of incorrect data. This act in most countries is covered by the general offences of information and in some countries by additional statutes within the privacy laws ; The illegal disclosure, dissemination, obtainment of and/or access to data, acts which are covered in most laws, however, to different extents; The unlawful use of data. However, as a result of the uncertainties of the substantive provisions, many legal systems rely to a great extent on an additional group of offences against formal legal requirements or orders of supervisory agencies. The formal offences against supervisory agencies and regulations which are, furthermore, included in most privacy laws contain in general more precise descriptions of the prohibited acts than the substantive offences. These formal provisions also vary considerably within the national legislation. The differences among the formal offences are not only based on differences in administrative law concerning the existence, nature, and powers of supervisory agencies, and the respective duties of the data processors. They are mainly evoked by different answers to the fundamental question whether "formal" offences should be regarded as criminal or not. This leads to the fact that some countries, such as France, punish formal offences against supervisory agencies and regulations with severe criminal sanctions, while others, such as Germany, regard such acts as "*Ordnungswidrigkeiten*", or "petty offences", only punishable by fines.

[187] *See* J. VACCA, *Biometric Security Solutions* (London, Prentice Hall), [2002].

Consumers need to advocate for their own privacy rights. They can make a difference by only doing business with companies that follow fair information practices; and, that make use of the privacy-enhancing aspects of biometrics in the design of their information management systems and ID theft protection techniques. Consumer preferences will be key in defining the appropriate uses and protection of biometrics. Consumers have the power -- they need to use it wisely[188].

2.2.2 Honey Pot Decoys and Padded Cells

The anonymity of the Internet that allows identity thieves to hide conceal their true identity so effectively can be a double-edged sword used against them.[189]

In his book *The Cuckoo's Egg*, Cliff Stoll describes how he effectively used decoy data files with exotic names to lure prey to his hacker-attacked computer. This type of enticement is generally referred to as a "honey pot" or "padded cell". The technique involves setting up a dummy server on the network and assigning an intriguing name, then loading a security information program into it along with a few nonsense data files, a copy of an important application program, and a pager service.[190] Because there should be no reason for anybody to use the server when the pager calls to indicate unauthorized use, you can begin a trace to identify the source of intrusion.

In many cases, the hits will be accidental, but if you identify one real intruder among one hundred false alarms, the honey pot may be well worth its modest cost. Law enforcement agencies are using this technique with increasing effectiveness to catch identity thieves online.[191]

However, there is a drawback to this technique, as network users will discover the honey pot, and its effectiveness will be diminished. Alternatively, they may use it for spoofing you with false attacks. You may wish to inform your trusted, legitimate users about the subterfuge with the intent of catching intruders, or you may wish to run a honey pot for a short period of time, then replace it with a new one with a different identity.

2.2.3 Tokens

No matter how secure a password system is, a clever identity thief can beat it. That is why many system owners now require use of tokens along with passwords. A token is a hardware or software device carried by, or in possession of, a computer user.[192]

The token contain an electronically recorded and encrypted password. Alternatively, it may have an on-board processor that can store and retrieve such a password when needed.[193] A token may be a plastic "smart card" similar to a credit card, or a program stored on a diskette; mobile computers or pocket calculators may also be tokens if they generate passwords.

There are two categories of tokens:[194]

- Passive or Stored Value, e.g., bank card;

---

[188] *Id.*
[189] *See* J. WALLACE, *Nameless in Cyberspace: Anonymity on the Internet* (Cato Institute), [1999].
[190] *See* D. PARKER, *op. cit.* p. 397.
[191] *Id.*
[192] *See* ex., L. GORMAN, *Securing Business's Front Door; Password, Token and Biometric Authentication*
[193] *See* D. PARKER, *op. cit.* p. 388.
[194] *See* L. GORMAN, *op. cit.*

- Active, e.g., one-time password generator.

The passive storage device is usually a magnetic stripe or smart card in which a static code word is stored. The active device usually contains a processor that computes a one-time password, either by time-synchronization or challenge-response. Some active tokens can also perform cryptographic calculations to encrypt and decrypt.[195] A smart card can participate in challenge-response protocols from the authenticating server by virtue of a cryptographic processor on the card.

Active tokens are higher end "secure" smart cards having a cryptographic processor.However, if they only store passwords or code words, but cannot perform processing functions, they are passive devices.

The primary advantage of tokens is their security. As they can store or generate a code word much longer than that which a human can remember, they are much less easily attacked.[196] A token that yields a 12-digit codeword has 10 possible different code words. This is called its *key space* and it is advantageous that the key space be as large as possible to minimize or dispense with successful attacks.

However most users are not usually so diligent in their password selection and average password key space is around 10. Therefore, in the average case a token is more secure than a password as measured by key space.

Another advantage of a token is that it provides compromise detection. Unlike a password which if stolen the legitimate user might have no idea, if a token is stolen, its owner has evidence of this fact by its absence.[197]

A final advantage is that it prevents denial of service attacks. Whereas an attacker with knowledge of a user's login can make a number (usually three) of login attempts with incorrect passwords until the system freezes that account, the attacker cannot achieve this if a token were required.

On a different note, there exist three main drawbacks to security tokens:[198]

- The user must remember to physically possess it to authenticate.
- Most security tokens require the user to memorize a PIN, so this effectively adds the memorization drawback as for passwords.
- Most tokens require a port or reader to convey information to the machine, for instance a smart card reader, USB port, etc. These may not be widely available or available across different access modes such as computers and telephones.

2.2.4. Cryptography

Although encryption is probably best known for protecting information from identity thieves, this application is probably overrated in business because of the colourful history of espionage, military and diplomatic concerns.[199]

Cryptography has a variety of purposes and requires different kinds of key

[195] *Id.*
[196] *Id.*
[197] *Id.*
[198] *Id.*
[199] *See*, ex., N. FERQUSON, *Practical Cryptography* (N.Y., John Wiley), [2003], p. 8.

management for its three applications in communications, storage, and digital signatures.[200]

In communications, communicators use cryptography to protect information in transit when it is particularly vulnerable (i.e., going through the cyberspace) because the senders and receivers typically do not have control over the communication route.[201] This application requires short-term protection by encrypting the information before it is sent, and decrypting it upon arrival. Sender's systems may generate keys or receive keys from the intended receiver for short-term use.

The challenge is for the sender's and receiver's systems to securely exchange and coordinate use of the keys, ensuring that no unauthorised party could change the senders key or has possession of the decryption key required to decrypt the information.[202]

In storage, possessors of information require several different methods to store information securely. Storing encrypted information requires the secure storage, backup, and retrieval of keys and cryptographic mechanisms – presumably in ways that are subject to better protection than the stored plaintext information.[203]

This presents a potential adversary with a twofold challenge: obtaining the keys and mechanisms and obtaining the ciphertext. The authorised decryptors must be able to securely retrieve the keys and mechanisms, possibly after long periods of time. Obviously, key and mechanism security is crucial to effective use of cryptography. The strength of the cryptography algorithm is of little importance at or above a prudent level.[204]

Much of literature on cryptography emphasizes the need for key management, but often omits mention of the important preservation of the mechanisms as well. Without the mechanisms, or at least possession of the algorithms used, it is virtually impossible to retrieve the plaintext, even if you do possess the keys.

In digital signatures, in order for digital signatures to be effectively a functional equivalent to handwritten signatures, cryptography is used to ensure the authenticity and integrity of signatures, documents, and transactions.[205] The cryptographic application accomplishes this by including a checksum or hash total of the entire message in the signature before it is encrypted. A new business function, called *certificate authorities* or *trusted third parties*, is emerging to create and provide authentic digital signatures for people to use in electronic communications and transactions.[206]

3. Digital Signatures with PKI Technology

Digital signatures may be considered more complex than biometrics.[207] in this

[200] *See* D. PARKER, *op. cit.* p. 374.
[201] *Id.*
[202] *Id.*
[203] *Id.*
[204] *See* D. PARKER, *op. cit.* p. 375.
[205] *Id.*
[206] *Id.*
[207] In the 1990s, most states in the United States adopted some form of the Uniform Electronic Transactions Act, which mandates broad recognition of electronic signatures. In order to achieve more uniformity in the laws of the states, the United States. federal government enacted "E- Sign" in 2000, which preempted all existing state law

context, it should be stated in the outset that digital signatures are quite distinct, from a technical stance, from electronic signatures which may be considered an electronic reverberation of handwritten signatures.[208]

In its true essence, a digital signature uses encryption and alogarithm based on certain technologies such as Public Key Infrastructure, or "PKI." The first step in utilizing this technology is to create a public-private key pair; the private key will be kept in confidence by the sender, but the public key will be available online. The second step is for the sender to digitally "sign" the message by creating a unique digest (hashing) of the message and encrypting it.[209]

The third step is to attach the digital signature to the message and to send both to the recipient.

The fourth step is for the recipient to decrypt the digital signature by using the sender's public key. If decryption is possible, the recipient knows the message is authentic, *i.e.*, that it came from the purported sender.[210]

Finally, the recipient will create a second message digest of the communication and compare it to the decrypted message digest; if they match, the recipient knows the message has not been altered. Thus, PKI technology verifies and authenticates the source of a message and its contents.[211]

4. Future Trends

Time plays a critical role in advancement and progression, and in the field of information technology there is always room for improvement and progress at an accelerated rate, especially with respect to authentication, cryptography, and privacy enhancing systems. However, the challenge, in effect, lies in striking the right balance between simplicity and convenience on one hand, and maximum security on the other hand.

Amongst the current pilot and ongoing projects for the provision of a higher level of security that minizes the risk of identity theft and cybercrime are:[212]

- ***Graphical passwords*** which claim to be more memorable to users. The *Déjà vu* project at the University of California at Berkeley, [213] displays an array of abstract images to users and focuses on the ones memorized. Similarly, the *HumanAut* project at Carnegie Mellon University requires the user to choose the pictures he/she has memorized from a sequence of

---

unless it was the original form of the Uniform Electronic Transactions Act. Unfortunately, United States jurisdictions now have a "patchwork quilt" of dissimilar law regarding digital signatures. The United States is technologically-neutral. The United Kingdom enacted the Electronic Communications Act in 2000. The Act recognized the validity of electronic signatures and affirmed their admissibility as evidence in court. Furthermore, the United Kingdom's Electronic Signatures Regulations went into force in 2002. The purpose of the regulations was to implement certain provisions of the European Union's E-Signatures Directive. However, the United Kingdom remained technologically-neutral

[208] *See* S. BLYTHE, Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce with Enhanced Security (11 RICH. J.L. & TECH), [2, 2005].

[209] *Ibid.*

[210] *Ibid.*

[211] *Ibid.*

[212] *Id.*

[213] *See* R. DHAMIJA, *Dja Vu* (University of California), available at: <http://www.ece.cmu.edu/~adrian/projects/usenix2000/> (visited 04/10/2005).

images.
Furthermore, the *Draw-a-Secret* project at Bell Labs, AT&T Labs, and NYU requires the user to draw a line in the same shape and sequence within an invisible grid pattern.[214]

- ***Enhanced tokens*** include multi-function smart cards that store multiple passwords on a single token and can perform other tasks, such as employee identification (employee identity card) or cafeteria debit. For wireless convenience, new security tokens will contain a Radio Frequency Identification tags (RFID) or Bluetooth chip, both for wireless detection in the proximity of a reader.[215] PDAs will also be enhanced with hardware and software to securely store passwords and other secure or private information.
- ***New and Multi-modal biometrics*** attempt to address some of the shortcomings of current biometric solutions. Multi-modal biometrics combine different biometric modalities to strengthen security, reduce false rejections, and provide alternatives to the user. New biometrics include gait recognition, infrared capture of blood vessel patterns, and implantable chips.[216]

5. Culture-Oriented Strategy: Public Awareness and Training on Security Issues

It should be stated in the outset that the best security policies in the world will be ineffective and worthless if users are not aware of them, able to use them, or if the policies are inconveniently restrictive. Policies that are unenforceable, or those which users are not willing to enforce are futile; their existence undermines the credibility of the system as a whole.

Moreover, transparency is a key factor of success. This entails full transparency on the efficiency of such policies, their scope, any restrictions or exceptions should be clear and explicit..

By and large, a culture of awareness, training, and transparency with respect to security issues and applications should be developed between all stakeholders to minimize the risks associated with cyber-communications.

CONCLUSION

This article aimed to explore and critically analyze the risk of identity theft in cyberspace. In the outset it should be noted that there is an direct relationship between the development and evolution of ICTs and Internet-related applications, and the intensification of identity theft risks and applications.

Technology is truly a double-edged sword that has transformed the classical and traditional forms of criminal behaviour. The proliferation of ICTs and progressive development in digital transactions and communications has created new opportunities and opened up new windows for the illicit exploitation and utilization of

[214] *See* L. GORMAN, *op. cit.* p. 20.
[215] An RFID tag is a small object that can be attached to or incorporated into a product, animal, or person. RFID tags contain silicon chips and antennas to enable them to receive and respond to radio-frequency queries from an RFID transceiver. Passive tags require no internal power source, whereas active tags require a power source.
[216] See Biometrics Consortium <www.biometrics.org> (visited 05/10/2005).

ICTs, which has resulted in the emergence of new forms of criminal behaviour and cybercrime. On such a basis, cyberspace identity theft ranks amongst the most important and virulent forms of cybercrime; not only due to its adverse impact on the development of cyberspace and e-commerce but also due to the diversity of means and methods that could be utilized in committing this crime as well as the inherent risk of using identity theft as a leeway and instrument to commit other crimes using the stolen identities of victims. Furthermore, identity theft could have a devastating impact on the financial security and credit scoring of victims.

Being aware of the potential and actual risks associated with this serious exploitation of ICTs, the authors have, throughout this article, attempted to provide a comprehensive overview of the fundamental issues and potential solutions pertinent to this form of criminal behaviour.

On such account, the article has been divided into two main parts: the first addressed the threat of identity theft by analyzing the threats associated, harms caused, factors contributing to the occurrence of the crime, the sort of information that could be stolen and attractive for identity theft offenders, the diverse mechanisms and methods utilized by offenders in committing this abhorrent crime (such as hacking, spoofing, phishing and pharming, spyware and malicious applications etc…), and the potential use of stolen information and personal data.

The second part of the article focused on the potential solutions to identity theft in cyberspace and devised a three-fold scheme based on the necessity for: (a) establishing adequate and efficient regulatory, strategic and legislative policies that protect online privacy and penalize cyber-criminal activities on national, regional, and global levels; (b) adopting technology-based solutions that enhance information security and protect online privacy. The need for adopting state-of-the-art technology to provide adequate information security was emphasized with respect to biometric security applications, tokens, honey pot decoys, cryptography and digital signatures, and graphical passwords; (c) developing cultural awareness and devising training programmes that raise public awareness and prudent practices in online activities.

By and large, the current article, by tackling the problem of identity theft in cyberspace, presents a modest contribution to the field of cybercrime and information security.