UiO : Faculty of Law
University of Oslo

Identity theft through the lens of US and Greek criminal law systems.

Should the Greek legislator follow in American footsteps?

Candidate number: 9005

Submission deadline: 15 May 2016

Number of words: 16,153

Table of contents

1 Introduction

Due to the rapid and constant growth of the technology, great many new things have been introduced into our everyday lives. People started communicating via the Internet and numerous online applications were deliberately developed for this purpose. In addition to the communication, a great variety of other everyday activities entered the digital era. It is common nowadays to do online purchases of products from merchants' webpages, to transfer money electronically using the online banking tools provided by banks and to be informed about new offers of our favourite brands via emails. These are definitely some new and advanced ways to interact financially nowadays. Yet, in order to take advantage of these new opportunities, we have to render ourselves recognizable and unique users among other individuals who use the same services. This means that we need to create a new electronic identity, different from the identity we had so far in the 'real world'. This new type of identity consists of usernames, passwords, PINs, email addresses and other similar information, rendering the aforementioned identity creation feasible in a digital environment.

Naturally, the growth of the technological field and more specifically the Internet, had both beneficial and detrimental effects to its communicants. Along with the new ways to interact and participate in the electronic markets came the various offensive acts against the communicants. The extensive growth and use of the Internet gave rise to many different kinds of criminal activities, facilitated by it, the so-called, cybercrimes. Unlike the traditional crimes, cybercrimes are offences involving electronic devices, in one way or another and the Internet in their commission. One of these new crimes is also the cybercrime of identity theft, which has as its target the digital identity of the victim.

The importance of the specific cybercrime appears to be great, given that on the Internet, no one can tell for sure, whether someone is the one who claims to be or whether someone else is impersonating the person in question. The only way to clarify who someone really is on the Internet is their digital identity elements which supposedly only one person has access to. However, the identity thieves have as their target these identity elements, which once under their control, can be used to several illegitimate purposes (e.g. fraud, harassment, defamation etc.).

This paper will focus on the identity theft and more specifically on the legal framework regulating it in two different countries, the United States of America (hereinafter USA) and Greece. These coun-

tries were not chosen randomly but they were selected for their fundamentally different approach in terms of legislation and mainly in terms of their citizens' exposure to the aforementioned new technological era. USA is arguably the country that has been affected the most by the rapid technological growth and the Internet, whereas Greece, even though a European country, has only recently been exposed to its beneficial and detrimental impact.

It is, therefore, very interesting to analyse how the American legislator coped with identity theft and its various facets in the analogue and the digital world, in contrast with how the Greek legal system currently handles incidents of identity theft and what changes should be introduced in order to encompass adequately this specific offence. The current legal challenges regarding identity theft are numerous and this is something that every country's legislator definitely has to take under consideration.

1.1 Methodology

This paper will approach the existing legislative regime regarding identity theft in the US as well as in Greece. The latter has been chosen because of the rather inadequate legal framework against identity theft it has but also because of the genuine interest of the author about its legislation, since Greece is his country of origin. The US, on the other hand, has been chosen because it is arguably one of the most and for the longest period of time exposed countries to the rapid technological growth occurring in our days, which makes it a suitable example for the comparison intended by the author. The respective provisions encompassing the offence of identity theft will be presented and clarified, but first a brief presentation of some of the most common cybercrimes and especially the specific cybercrime of identity theft will take place. Further, the scope of the instruments and some interesting legislative approaches in both legal frameworks will be examined. The US legal framework in point will be explored, both at federal level, since one of the distinguishing features of the cybercrimes is their trans-border character, as well as legal provisions of selected states. Furthermore, there will be a brief comparison of the two different legal regimes which will be followed by recommendations from the author, as to what direction possible future amendments in the Greek legislation against identity theft, should head into.

2 The cybercrime of identity theft

2.1 Cybercrimes

The great growth of the communication technology nowadays, particularly the Internet, over the last decades brought our everyday lives to a new orbit in almost every aspect. Communication with other people who are located in different places of the world has now exceeded the old fashioned cable connection limitations by the new wireless technology facilitated mostly through the Internet. The old traditional methods of communication, such as letters, telegraphs and even telephones, appear to be outdated in the modern era, as a personal computer or even a smartphone is everything one needs in order to communicate, even with people on the far side of the globe. Documents, photographs, videos and music have now taken an intangible form, which only translates into megabytes and gigabytes, making the not too old fashioned mediums for multimedia files, such as vinyl discs, floppy discs, CDs and DVDs, seem obsolete and useful only as collectibles. Entertainment has also got a whole new meaning with online platforms hosting every kind of entertainment material uploaded and ready to access with a single click. Even education and new ideas now have a new ally in the technology, which contributes into their sharing to potentially a great amount of receivers, literally within a split-second.

Of course, as there is nothing in this world, or almost nothing, having only a beneficial character, the Internet could not be the exception. Whereas most of the Internet users are using it for legitimate purposes, there is also a group of people who saw the hidden opportunity lurking within it to serve their illegitimate objectives. Given that those who abuse the benefits that the Internet provides are numerous, we have to confine ourselves to discussing only about those who abuse the Internet in a criminal way. But first, in this paper, the author will make a brief presentation of the reasons why the Internet appears to be the perfect action field for a big variety of criminal activities along with a brief presentation of the various Internet based offences, in order to focus later on to the identity theft cybercrime, which is the main criminal offence this paper will be focusing on in the following chapters.

2.1.1 Cybercrime nowadays

As we all know, the Internet is now being used by a great number of people. Currently, around 45% of the world's total population uses it,[1] which on its own gives an enormous acting field to numerous aspiring criminals, who can harm their numerous potential victims in little time and without being restricted by the geographical distance barrier between them. With the use of the Internet the world has become a neighbourhood where no distance is further away than a simple click and borders have been eliminated. In addition, the availability of technology to a continuously growing number of people, particularly through small personal devices and the portability and transferability of them, have introduced a new scenery where cyber criminals are facilitated by the same technological developments to commit various offences against their victims. Furthermore, another factor that helped this great growth of cybercrime is of course the anonymity that the Internet can provide for its users. In addition to the aforementioned reasons for the blooming of cybercrime, it has to be added that it is notoriously difficult to enforce laws on the web. In such vast criminal activity field, it is all but impossible for the competent authorities to enforce the law and preserve the peace of the legal order.[2]

The terms used, in academic literature, to describe the Internet related offences are numerous. One could say that there are as many terms as the various offences that exist and are yet known. Terms as 'computer crime', 'high-tech crime', 'net crime', 'information-age crime', 'IT crime', 'internet crime' and 'cybercrime' are all seen in the various literature describing offences which are committed either online or with the usage of an Internet connection or a computer or even having the computer or the computer networks as the target of the criminal activity.[3] In this paper the term 'cybercrime' will be used, since it appears as the most frequently used in the literature, the most recognizable and the most generic term that describes more spherically those offences.[4]

Furthermore, in order to shape a better image of what is eventually a cybercrime, the US Department of Justice has developed a three-stage classification method of the crimes related to the Internet and the new technological means which is noteworthy. To begin with, there are the par excel-

---

[1] Internet World Stats, "Internet Usage Statistics: The Internet Big Picture - World Internet Users and 2015 Population Stats."

[2] Clough, *Principles of Cybercrime*, 5–8.

[3] Ibid., 9.

[4] Christensson, "Cybercrime Definition."

lence computer crimes, in which the computers or the computer networks are the targets of the criminal activity (i.e. DoS[5], hacking and malicious software attacks). The second category in this three-stage classification consists of the offences that already exist but now are committed with the use of a computer and/or a computer network (i.e. fraud, criminal copyright infringement, child pornography). These are the computer-facilitated crimes. Finally, the third category of these computer related offences, is the one in which the use of the computer is only an incidental factor of the offence and can only be used as a means of acquiring useful evidence of the commission of the offence and they can be named as computer-supported crimes. Similar or the same method for the classification of the computer related crimes have also been used in Australia, Canada, the UK and internationally.[6] However, this paper will be focused on identity theft committed in ways within the first two categories of the abovementioned classification method, namely the par excellence computer crimes and the computer-facilitated crimes, since these are genuinely the computer related offences having the computer and the networks as key factors of their commission.

2.1.2 Brief presentation of common cybercrimes

As mentioned above, the number of the already known cybercrimes is great and their variety seems even greater. However, this subchapter will discuss briefly some of the most often committed cybercrimes of the first two categories of the three-stage classification introduced by the US Department of Justice[7], along with a brief presentation of their specifics and the *modus operandi*, which makes them stand out. However this chapter will not discuss anything related to the third category of the aforementioned classification due to the incidental role the computer and the computer networks play in these offences.

2.1.2.1 Par excellence computer crimes

[5] Christensson, "Denial of Service Definition," n. "A denial of service (DoS) attack is an effort to make one or more computer systems unavailable. It is typically targeted at web servers, but it can also be used on mail servers, name servers, and any other type of computer system."

[6] Clough, *Principles of Cybercrime*, 10.

[7] Ibid.

The first category of cybercrimes is the one consisting of cybercrimes that have the computer or the computer network as their target (par excellence computer crimes). This means that the offenders in such cybercrimes are trying to harm a computer system, a computer network, a collection of data or even the sole functionality of a computer. The reasons to commit a cybercrime against one or several of the aforementioned targets vary as much as the variation of the cybercrimes existing for this purpose. Espionage, sabotage, hacktivism, cyber-bullying, cyber-terrorism, the pursuit of political purposes or even the demonstration of the hacking skills of the perpetrator, may be some of the motives or the pursued objectives behind the said criminal activities, rendering them a special and unique category of cybercrimes, which are not aiming to secure financial gains to their perpetrators, but they are rather being committed for fame or even moral satisfaction. The ways to accomplish these aims appear to be uncountable. Hence, I will only present some of the most common and usual ways that such activity is conducted by discussing the relevant cybercrimes.

One of the most common cybercrimes of the first category, according to the frequency they occur, is the Denial of Service cybercrime (also known as DoS). The perpetrator of this type of cybercrime uses his hacking skills in order to render one or more computer systems unavailable. DoS attacks can be initiated by a single computer and the targets of these attacks are usually web servers. In most of the cases though, the perpetrator creates and uses a botnet[8] consisting of many computers, which has previously been compromised and infected with malicious software (malware)[9], in order to initiate an attack, since most firewalls can counteract against one single attacking computer only. Briefly, the essence of DoS attacks is that the attacker attempts to send a stream of requests to a specific server at the same time causing it to break down, since it cannot eventually respond to all the simultaneous requests, hence making it unable to respond to the requests of its legitimate users as well.[10]

Malware attacks, in general, belong to the first category, with other cybercrimes targeting the computer systems. Malicious software such as viruses, Trojan horses, worms and spyware are also harmful for the victims' computer systems since they intrude in those systems deleting valuable files or stealing valuable information without the user of the attacked computer ever finding it out.

[8] Christensson, "Botnet Definition."

[9] Christensson, "Malware Definition."

[10] Christensson, "Denial of Service Definition."

Yet, malware attacks can also be used for the commission of the cybercrimes included in the second category of the three-stage classification, as it will be presented below.[11]

2.1.2.2 Computer-facilitated crimes

Most of the known cybercrimes are not limited to the first category, namely to which they have as target a computer system and/or a network. Great amount of concern has been given into cyber facets of already known real-life crimes that are now being committed by the use of a computer or through a computer network. One could argue that this kind of cybercrimes is the same as the traditional crimes, with the only with the difference that there is a computer involved in their commission, most of the times connected to the Internet. The counter argument might be the sole fact, that the use of current technological means in order to commit the same crime is changing the *modus operandi* of it and it renders it a totally different crime.[12] Both perspectives can be further elaborated but the outcome of such an elaboration is still likely to be uncertain. However, in this paper, it will be assumed that the traditional crimes committed by the use of a computer or any other technological means, are actually new crimes, in the sense that it is a traditional crime with a unique cyber *modus operandi*.

The number of these traditional crimes, that nowadays have got a cyber-character, is enormous. Technology has entered our lives for good and that is illustrated in the criminal side of our everyday realities as well. Almost every single traditional crime can now be committed through a computer or by the use of a computer, with the exception of some crimes that require strictly physical connection between the perpetrator and the victim or their property, such as rape, homicide, robbery. However, even in such cases the main crime can also be organized via technological means, hence giving them a cyber-character to a certain extent. An example of this kind of cybercrimes is the 'flash robs'. In this particular cybercrime, a team of offenders is organized and synchronized via social media platforms, in order to assemble a criminal team that commits robberies at the same time and place, making any defensive reaction by the victims almost impossible. In this cybercrime, the technology is not playing that crucial role in the actual commission of the crime, but is nevertheless

[11] Christensson, "Malware Definition."

[12] Clough, *Principles of Cybercrime*, 10.

the key factor to ensure that the robbery attack will be multitudinous and synchronized. In addition, the existence of the technology changes the harshness and the commission speed of the offence which gives clearly another character to the crime thus rendering it a cybercrime.[13]

Other traditional crimes have also taken a new cyber character, which renders those as cybercrimes. Criminal copyright infringement, for example, has become one of the most common cybercrimes committed on a daily basis. Peer-to-peer[14] technology has created a very broad action field for copyright infringers who can easily upload and send a link of the copyright protected material to numerous receivers infringing by this action the rights of the lawful owners of the respective material. Moreover, another quite common cybercrime is cyber-stalking which constitutes basically the computer-facilitated version of the traditional stalking crime. The only difference is that in cyber-stalking, due to the nature of the means that are being used for its commission (i.e. social media platforms), the victim appears to be completely unaware of the existence of the stalker and this makes it extremely difficult for the victims to find out, since the offender is using his computer to stalk his victim, and hence avoiding to make himself detected, while technology and the anonymity it provides act as two very powerful allies by the cyber-stalker's side.

A new trend in the cyber-criminal activity worldwide has also become the crime of cyber-bullying. Everybody was aware of the traditional bullying, that usually occurred in narrow and confined environments, such as school or work, but nowadays, due to the rapid and widespread entrance of technology into our lives, bullying became digital and exceeded previous occurrences.[15] Cyber-bullying is present not only in the confined, close to the victim, environments, as it used to be, but also online, where it causes even greater damages to the victim, such as psychological traumas, depression and occasionally it leads the victim to consider or even commit suicide.[16] However, cyber-bullying technically occurs between young individuals, whereas if adults are involved then we talk about cyber-harassment or cyber-stalking. In any case, legislators have only recently made serious efforts to regulate cyber-bullying as a crime.[17]

---

[13] Vaughan, "Teenage Flash Mob Robberies on the Rise."

[14] Christensson, "P2P Definition."

[15] Kowalski, Limber, and Agatston, *Cyber Bullying*, chap. 3.

[16] NoBullying.com, "Is Cyberbullying a Crime? Hopefully Soon!"

[17] Christensson, "Cyberbullying Definition."

Yet, the offence that has reached new heights, due to the recent technological growth, is fraud. With the new technological means and the gradual digitalization of our lives, a great field for fraud commission has opened. In the past, the traditional fraud could be committed only by the use of false documents or deceitful behaviour from the perpetrator towards the victim aiming mainly in financial gains. Back then, the risk for the perpetrator that the victim would understand the fraud, caused a high risk of revelation. Nowadays, though, the anonymity, the ease and the variety of the means available to commit fraud for financial gain in the online setting, gave new potential to the aspiring fraudsters. One of the most common ways in perpetrating fraud via a computer nowadays is by committing identity theft. This occurs when the perpetrator steals the personal identifying information of the victim (e.g. name, address, ID number, banking account number, username or password) in order to use them as if it is his and take control over his victim's assets by committing fraud. Though, this is only a superficial notion of the identity theft cybercrime, and this paper will discuss this specific cybercrime thoroughly further below.

2.2 Identity theft then and now

2.2.1 Personal identifying information – Identity

In order to understand what identity theft really is, first of all we have to clarify what an identity is. In other words, what exactly is the nature of the 'stolen goods' when identity theft occurs? Of course, everyone has a view as to what kind of information is included in the definition of identity, but here we will present the elements of someone's identity that can be 'stolen' and used by the perpetrator of the identity theft cybercrime.

A person's identity can consist of numerous different characteristics or information related to an individual. Elements of the identity of an individual can be those that he acquired by birth, like the colour of his hair, eyes, skin, the way he walks along, with some more sophisticated elements, such as the fingerprints, the shape of his skull, his eyes' iris or the formation of his denture. All these are also known as biometrics or biometric information of an individual and they are tightly connected to the sole existence of a person. However, because of the extremely personal character and the in-

timacy of those elements to their owner, it is rather difficult for them to be stolen and used by another person.

An individual's identity, however, does not consist only of elements that he acquires by birth. A lot of the identity elements are given to each citizen by others (i.e. parents, state). These are also information highly attached to a person and they are part of his identity. Some of them are one's name and surname, the date of birth, the father's name, the mother's maiden name, the social security number or the passport number. These are all information that are connected to a person and they render a person unique among the other members of a society.

Moreover, there is personal identifying information that a person creates by its own will. For instance, when a person decides to become a costumer of a specific bank, he receives an account number from the bank and a credit card which needs a PIN number to function. When he creates an email account, he also creates an identifying email address and a password. When he creates a social media account, he creates his online identity, which one could label as 'soft identity'. All these numbers, passwords and usernames are also elements of a person's identity, and form part of the total amount of personal identification information created by a person himself.[18]

As an example of what is personal identification information according to the legislation, the author randomly selected, as one of the most complete and adequate among other pieces of legislation on this matter, the respective subparagraph of the term definition paragraph as given by the Florida state statute 817.568 in paragraph 1(f). The aforementioned subparagraph states the following:

" "Personal identification information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any: 1. Name, postal or electronic mail address, telephone number, social security number, date of birth, mother's maiden name, official state-issued or United States-issued driver license or identification number, alien registration number, government passport number, employer or taxpayer identification number, Medicaid or food assistance account number, bank account number, credit or debit card number, or personal identification number or code assigned to the holder of a debit card by the issuer to permit authorized electronic use of such card; 2. Unique biometric data, such as fin-

[18] Gomes, *Electronic Identity*, chap. 1.4.1.

gerprint, voice print, retina or iris image, or other unique physical representation; 3.Unique electronic identification number, address, or routing code; 4. Medical records; 5. Telecommunication identifying information or access device; or 6. Other number or information that can be used to access a person's financial resources."[19]

In summation, the identity of an individual includes three different types of information. There are the characteristics one receives by his birth (biometrics), the identifying information others give to a person and the identifying information one creates on his own for himself in order to make himself identifiable amongst a number of other users of a service or members of a group. Subsequently, one could assume that the bigger the distance between the individual and the information the easier it is for someone to 'steal' it.

2.2.2 What is identity theft?

Each time we talk about identity theft, it is almost inevitable not to think of the actual theft crime. One could think that the perpetrator of identity theft is actually stealing the personal identifying information of another person as if he was stealing one's wallet. In that sense the term 'identity theft' seems quite problematic for several reasons.

Firstly, the term 'theft' is not being used in its literal sense, as the person's identity is not stolen. Aspects of the victim's identity are being appropriated by the offender, usually in order to commit a further offence (e.g. fraud). In addition, the term 'identity theft' is generally used when an existing identity is appropriated, but when the offender creates a false identity or even alters an existing one, then he becomes able again to commit a crime that requires the prior use of a false identity. Finally, in academic literature, it is debated what exactly is 'true' identity theft. Some of the commentators view the use of credit card information as a simple fraud while they consider that true identity theft occurs in those occasions where there is a more concerted effort for the appropriation of a person's identity.[20]

---

[19] *Criminal Use of Personal Identification Information*, para. 1(f).

[20] Clough, *Principles of Cybercrime*, 209.

Subsequently, in order to set a benchmark regarding identity theft, we must establish that the crime of identity theft is being committed when someone gains unlawful access to the personal identifying information of a person without the latter knowing it. The types of information the identity thief is usually aiming to obtain access to are mainly the social security number, name, address, date of birth, mother's maiden name, employment information, credit information and other vital victim information. By gaining access to such information, the perpetrator gets in a controlling position over the victim's identity, which allows him to commit numerous forms of fraud, such as taking over the victim's financial accounts.[21]

According to the US Department of Justice the definition of identity theft is the following: *"Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain"*.[22] However, identity theft can also be committed for other reasons, irrelevant to economic gain, such as defamation of the real owner of the personal information or even in order to hide the actual personal information of the perpetrator. The ordering of pornographic materials using the identity of another person, for example, could be done for the aforementioned non-economic reasons.[23]

The perpetrator of identity theft will manage to gain access to the personal identification information of his victim and once he succeeds, it is up to him how he will use the information to achieve his own illegal purposes. Identity theft is mainly used in order to commit various forms of fraud. The crime of identity theft took its name only in mid '90s, whereas the phenomenon had previously been labelled differently. Some of the names the identity theft crime got in the past were 'credit card fraud', 'true name fraud', 'identity fraud' and even 'Crime of the '80s'.[24] Later in this paper, the author will attempt to shed light on the impact that recent technological growth has had on this crime, hence transforming it from a regular crime to a cybercrime.

---

[21] Biegelman, *Identity Theft Handbook*, 2.

[22] US Department of Justice, "Identity Theft."

[23] Easttom and Taylor, *Computer Crime, Investigation, and the Law*, pt. 1, chap.1.

[24] Biegelman, *Identity Theft Handbook*, 3.

However, before we continue to more recent examples of identity theft incidents, it is interesting to briefly mention the story of the first identity theft victim, whose name was Hilda Schrader Whitcher. The victim was an employee of a wallet manufacturer that, in 1938, decided to advertise in its new products the innovative new slot which could fit the social security cards recently distributed to the working Americans (1936), by using the actual social security card of its employee. Even though the card used for this marketing campaign was only half the size of the real one and it had the word "specimen" written on it in red letters, it contained, however, the real social security number and other personal information of its owner. That led to a massive abuse of the victim's personal information, reaching 5,700 people using it in 1943. Eventually, the victim was given a new social security number but even in 1977, her previous one was being used by 12 people. According to the Social Security Administration, over 40,000 people had used Hilda Schrader Whitcher's social security number over the years. However, it is still uncertain how many people used it for fraudulent purposes.[25]

2.2.3 Types of Identity Theft

Since our personal identifying information is organized in various tangible and intangible forms of documents, the identity theft crime can correspondingly be committed in numerous ways. We are not anymore just human beings, who happen to live in small societies where everyone knows everyone. Nowadays, we are more an aggregation of different information, such as names, addresses, personal numbers, usernames and passwords, rather than just human beings. Each one who lives in an organized society is given a specific personal identifying information from the state in which he lives, right after his birth and creates more during his life. That is what makes this amount of personal information important to its owner and for everyone who interact with him, as it basically proves of one's existence.

2.2.3.1 Identity theft in the offline world

[25] Ibid., 14.

The types of identity theft vary, depending on the piece of information one is trying to obtain by the commission of this crime and the way he is trying to achieve that. In the analogue world, before the invasion of the new technologies in our lives, the identity theft crime was being committed through various methods. One of the classic examples of identity theft in the offline world is the so-called, dumpster diving or trashing.[26] Arguably, that method is the least technologically-demanding way to commit identity theft, and the term used for it is very descriptive, as to how the crime is committed. Identity thieves simply dive into the garbage of individuals or businesses, looking for valuable information, such as medical files, mortgage applications and various financial documents. Even though the dumpster diving identity theft has become known to the public and to the businesses, forcing them to shred the documents that contain such information, this kind of identity thefts still thrives.[27]

Another rather obsolete identity theft version is the so-called, 'white plastic fraud'. The name 'white plastic fraud' was given to the method after the procedure followed for the commission of this fraud. The criminals just embossed with stolen information, such as the name of the owner, his account name and expiration date, in simple pieces of white plastic in the size of a credit card. These phony cards required a conspiracy between the fraudster and a merchant to take place in order for the unlawful transaction to be successful. The merchant was imprinting a credit card sales draft with the counterfeit credit card, or sometimes a white piece of plastic, and depositing it into the business account. After that, the merchant had only to split the illegal earnings with the fraudster. Even though the counterfeit and altered cards scheme was a problem back in '80s, things have changed due to the advances in technology.[28] However, more sophisticated variations of this crime are still being committed in the recent years.

When we talk about identity theft, we think of career criminals and organized crime. Yet, several incidents of identity theft have occurred against banks or businesses that handle personal information, committed by their own employees. The so-called 'insiders' are taking advantage of their accessing ability or any security gaps in computers, networks and database systems, which they are aware of, in order to gain access to sensitive information and give it to the fraudsters after being

[26] Wall, *Cybercrime: The Transformation of Crime in the Information Age*, 4:73.

[27] Biegelman, *Identity Theft Handbook*, 30.

[28] Ibid., 29.

bribed.[29] In some cases, where the victim is an individual and not a company, the perpetrator may also be a friend or even a member of his family.[30]

2.2.3.2 Identity theft in the online world

The three examples of identity theft versions given above were only indicative of this kind of offence in the offline world. The list is endless, including many other offline identity theft offences, such as mail/telephone order fraud, mail theft, government benefits and documents fraud, account takeover fraud and many more. All these offences occurred on the grounds of a prior unlawful acquisition of the victim's personal identifying information by the perpetrator.[31] However this paper will focus on identity theft as a cybercrime, occurring in the online world by the utilization of a computer or a computer network. In that sense it seems necessary to present the online facets of the identity theft cybercrime by presenting a few examples of identity theft cybercrimes.

Technology has equipped aspiring identity thieves with a plethora of modern and sophisticated tools, suitable for committing identity theft in a more contemporary way. The ease that computers, networks and especially the Internet offer to the potential offenders has dramatically changed the ways identity theft is being committed nowadays.

Arguably the most common form of identity theft cybercrimes, originated in the early '90s,[32] is the so-called 'phishing' cybercrime which is committed mainly via emails.[33] Namely, bogus emails, which appear to be legitimate as coming from banks, credit cards companies or online retailers, are being distributed massively to numerous recipients, asking them to follow an attached link to the email, in order to sort out a security issue or refresh the information of the victim's account. Once the victim follows the given link, a fake web page of the supposed distributor of the bogus e-mail comes up and asks for personal information in order to verify the information for the ostensibly breached account. The spoofed web page, which is usually facilitated in a server with low or no

[29] Ibid., 32.

[30] Kitten, "ID Theft: Insider Access Is No. 1 Threat."

[31] Biegelman, *Identity Theft Handbook*, chap. 3.

[32] Jakobsson and Myers, *Phishing and Countermeasures*, 2.

[33] Yar, *Cybercrime and Society*, 87.

security scheme at all, looks, in most of the cases, extremely, similar to the real web page of the specific sender and can easily mislead people making them believe that they are actually on the legitimate web page of their bank or credit card company. When the victim submits the required information, the victim reveals his personal identifying information to the identity thief, allowing him to use it in order to commit every kind of fraud, rather than securing or refreshing his account[34] However, due to the fact that incidents of phishing tend to attract more public attention, the aspiring identity thieves came up with other more sophisticated and harder to detect techniques to achieve their goals. 'Smishing' is one of these new techniques to commit identity theft. The perpetrator guides his victim via SMS (short message service) to an imposter web page for various reasons. If the victim follows the instructions given in the SMS, he gets subjected to a similar pattern of deception as in the phishing schemes.[35] In this case, the more intimate character of the SMS sometimes leads the victim to follow the instructions given more readily than usual when the fraudsters utilize emails for their deception.

Another, even newer and more sophisticated phishing technique has been applied by the identity thieves recently. It is called 'spearfishing' and works exactly like phishing, with the sole difference that the bogus emails are not being sent to numerous of recipients, but rather to specific organizations or individuals in a more personalized manner. Accordingly, the perpetrators are addressing the bogus emails directly to their victims, which most of the times are 'big fish', by using their actual names, organizations and telephone numbers, making those emails more convincing and credible.[36]

In addition to the phishing identity theft technique, another rather infamous technique which identity thieves employ in order to gain access to personal identifying information of their victims online is the so-called 'pharming'. Although, the purpose of that scheme is the same as phishing, the *modus operandi* is quite different. Accordingly, pharming corrupts the local domain name server (DNS)[37] of the victim and redirects his request for a legitimate web site to a phony one. This method is more aggressive than phishing since it requires no positive action by the victim. The victim's

---

[34] Biegelman, *Identity Theft Handbook,* 35.

[35] Ibid., 37.

[36] Ibid., 38.

[37] Christensson, "DNS Definition," n. "DNS translates domain names into IP addresses, allowing you to access an Internet location by its domain name."

request for a specific web page is redirected to a phony one, which looks real and when personal information is given to that phony site, the personal information ends up directly in the identity thief's hands.[38] The particular identity theft technique is also known as 'DNS poisoning' or 'cache poisoning', because pharming uses malicious code embedded in the e-mail to 'poison the domain name server.[39]

Another quite common and modern identity theft facet is identity theft via social media. In this case, once the perpetrator gains access to the victim's social media account, he uses it in order to defraud the victim's "digital friends", impersonating his victim. Subsequently, due to the fact that nowadays social media have become more personalized, the 'friends' of the victim's profile are unable to realize that the real owner no longer manages his personal social media account, which makes them believe that whatever is posted by the victim's account is true. Maybe the most known incident of identity theft via social media and more specifically Facebook, was the one that occurred against a person, named Bryan Rutberg, on January 21, 2009. Briefly, Bryan's Facebook account was compromised by an identity thief who, after gaining access of Bryan's Facebook account, managed to change the access codes and posted a status saying; "BRYAN IS IN URGENT NEED OF HELP!!". Consequently, some of the online (Facebook) friends and mainly the real-life friends of the victim, worried about their friend's health and physical integrity and tried to contact him and ask him what happened. They were actually talking to the identity thief who, pretending to be Bryan, was asking them for financial help, claiming that he was abroad and went broke after being robbed. Unfortunately, some of Bryan's friends responded to Bryan's Facebook account cry for help and wired some money to the offender via Western Union in London. Back in 2009, Facebook appeared rather unprepared to deal immediately with such incidents. Due to the perpetrator deleting Bryan's wife from his friends list so that she could not inform at least their mutual friends about the scam through her account, Bryan's digital life was literally out of his control and his friends were victimized.[40] Worth mentioning that in this type of identity theft offences, the perpetrator is usually a person of the victim's close environment[41] and the motives are not always economic, as defamation and harassment can be the purpose.

---

[38] Biegelman, *Identity Theft Handbook*, 35.

[39] Wall, *Cybercrime: The Transformation of Crime in the Information Age*, 4:77.

[40] Timm, Perez, and Ely, *Seven Deadliest Social Network Attacks*, chap. 5.

[41] Biegelman, *Identity Theft Handbook*, chap. 3.

Although the aforementioned online identity theft facets are amongst the most common, there are many more methods. Namely, in the digital field, some of the most usual ways the cybercrime of identity theft is being committed are; the 'Nigerian 4-1-9 fraud', various hacking and electronic intrusions, vishing and social engineering techniques.[42]

2.2.4 Independent crime or facet of fraud

As outlined in the previous chapter, identity thefts mainly occur in the offline and the online world as a preparatory act of the crime of fraud or deception. However, the offence consists of two separate acts, namely, the theft of the personal information and an offence following the theft of personal information (i.e. fraud). So the question arises whether the theft of the personal identifying information of the victim has to be confronted as an independent criminal act or if it has to be viewed as a part of the following crime. Both perspectives have their partisans.

On the one hand, there is the identity theft as an independent crime which has to be punished regardless of whether a fraud or another crime has been committed after its commission. In this case the perpetrator is rendered guilty for acquiring personal identifying information of another individual without having any permission or any lawful grounds whatsoever for doing that. However, in this case, there is always the risk of over-criminalizing conducts, and more specifically, acquisition of personal information, even when this acquisition is taking place for legitimate purposes. Of course, the owner's consent is always on point when it comes to personal information.

On the other hand, one could argue that identity theft can only be committed when another crime follows the acquisition of the personal information. Then the theft of the personal information is only auxiliary and preparatory to the commission of the main crime, such as fraud or deception, and is being punished accordingly. In this case, the acquisition of the victim's personal identifying information by the perpetrator appears to be a key aspect of the crime since without that information, it would be difficult or impossible for the perpetrator to achieve his illegitimate goals.

---

[42] Ibid.

Moreover, when we talk about identity theft, most of the people, and especially the law enforcement authorities, tend to focus on whether or not the usage of the personal information of another person causes an economic damage to the victim. It is important, though, to clarify whether the sole act of 'stealing' someone's identity is an equally serious crime under the law, given that for the victim whose personal information has been stolen, the sole act of theft is rather important. Certainly, identity theft as such is illegal in various jurisdictions, but the real question is, whether there has to be a following offence and/or economic damage against the victim in order to prosecute the offender successfully before the criminal courts.[43]

In order to clarify this controversy, more light is about to be shed in the following chapters on these two approaches from the legislation's viewpoint. Namely, this paper will discuss how the phenomena of identity theft are confronted by the US legal regime along with the Greek one, regarding its independent or preparatory nature of that crime. In addition, it will also be discussed whether an economic perspective should be given to the crime of identity theft, in order for it to be prosecuted in both legislations, or if merely the fact that someone's identity has been stolen reason enough to prosecute the offender.

[43] Easttom and Taylor, *Computer Crime, Investigation, and the Law*, chap. 1.

3 Identity theft in the United States

In the United States of America, the crime of identity theft seems to be an issue which the federal and the local state legislators became well aware of a long time ago. In an attempt to achieve a spherical understanding of the crime of identity theft under American law, a brief presentation of the federal and some indicative state identity theft legislations will be scrutinized in this chapter. These examples are worth examining due to their language, the scope of the possible identity theft variations they encompass and the severity and importance that the legislators impose to each facet of the specific crime along with other interesting aspects.

3.1 US Federal Law on identity theft

On October 30th 1998, the US Federal government passed the Identity Theft and Assumption Deterrence Act of 1998 amendment of chapter 47 of title 18, United States Code, relating to identity fraud, and for other purposes. By this Act the legislator, among other amendments, added also the 7th paragraph stating *"whoever […] knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law […] shall be punished as provided in subsection (b) of this section."*[44] The punishment for the specific federal offence is *"a fine under this title or imprisonment for not more than 15 years, or both, if the offence is […] an offence under paragraph (7) of such subsection that involves the transfer, possession, or use of 1 or more means of identification if, as a result of the offence, any individual committing the offence obtains anything of value aggregating $1,000 or more during any 1-year period;"*[45]

Accordingly, as we can see the US Federal Law, with the aforementioned amending Act, included the cases of identity theft within the federal legislation, encompassing the identity fraud, such as the production and use of counterfeit identification documents. This, if anything, gave a formal validity to the offence of identity theft. Even though there has been a federal recognition by this Act of the

[44] *Identity Theft and Assumption Deterrence Act of 1998*, sec. 3(a)(7).

[45] Ibid., sec. 3(b)(1)(D).

specific crime, this is valued in economic terms, putting aside the identity theft offence in which there is no financial gain for the perpetrator. However, the cases where the crime of identity theft occurs for reasons other than the economic gain are not that few.

Furthermore, in order to address the gradual growth of the threat of identity theft, in the year 2008, the Identity Theft Enforcement and Restitution Act was added in the legislative quiver, as an extension of the 1984 Computer Fraud and Abuse Act. This act stands out because it expands and broadens the identity theft laws to organizations also, contrary to the previous legislation, which rendered the status of identity theft victim only to natural persons. Under this act, legal persons, such as organizations, can be viewed as victims of identity theft and fraud.[46]

3.2 State provisions on identity theft

In addition to the US Federal law, there are also various state and local legal provisions regulating the crime of identity theft and its variations, even though most of the identity theft incidents usually do not occur within the territory of the same state. However, only a selective presentation of some of those provisions will be conducted in this paper, aiming to outline the different elements of the specific offence that the legislator distinguished and decided to point out through their legislation.

Our first example will be the state of Alabama, where the legislator exalts the identity theft crime from a misdemeanor to a class C felony, recognizing in this way the general affection this crime has to the society. Another fact worth mentioning about the Alabama Consumer Identity Protection Act is that it clearly defines what constitutes an identity theft crime by separating the ways in which the identity theft crime can be committed.[47] Namely, the respective provision states that*: "A person commits the crime of identity theft if, without the authorization, consent, or permission of the victim, and with the intent to defraud for his or her own benefit or the benefit of a third person, he or she does any of the following: 1) Obtains, records, or accesses identifying information that would assist in accessing financial resources, obtaining identification documents, or obtaining benefits of the victim, 2) Obtains goods or services through the use of identifying information of the victim, 3) Ob-*

[46] Easttom and Taylor, *Computer Crime, Investigation, and the Law*, pt. 1, chap. 3.

[47] Ibid., pt. 1, chap. 4.

tains identification documents in the victim's name."[48] Interestingly, the legislator excludes perpetrators who obtain another person's identity in order to misrepresent their age for the sole purpose of obtaining goods denied to minors (i.e. alcoholic beverages, tobacco).[49]

Another example of legislation on identity theft is statute 817.568[50] of the state of Florida. This statute stands out for three reasons. First, it lays down that even if someone possesses personal identification information of another person, without the consent of that person, and has the intention to use it for fraudulent purposes, then the former commits a felony of second degree, regardless whether they use this information for their own financial benefit. This is rather important; bearing in mind that the identity theft crime is often associated with non-economic related crimes, such as defamation of the victim. Yet, this statute also addresses identity theft for financial gain, based on the scope of the offence, in terms of money and victim. The second interesting fact about this Florida act regarding identity theft is that additional penalties may be imposed when the perpetrator wilfully and without consent or specific authorization of the victim possesses, uses, or attempts to use the victim's personal identification information for the purpose of harassing him. So the furtherance of the harassment, by the use of personal identification information of the victim, weights more than the simple harassment in terms of criminal demerit.

Finally, the third interesting provision of this statute is that it specifies additional penalties for the perpetrator of identity theft who gleans personal identification information from public records. The legislator in this last provision seems to have understood thoroughly the fact that by the continuously growing use of the Internet by the public authorities, it has become easier for identity thieves to steal the personal information they need from online public databases. This is the reason why the statute poses additional penalties for those who misuse public records in order to commit the crime of identity theft.[51] Regarding the last provision though, one could argue that it over-protects the specific information and that one could be prosecuted for obtaining information for legitimate purposes.

---

[48] *Alabama Consumer Identity Protection Act*, sec. 13A–8–192.

[49] Easttom and Taylor, *Computer Crime, Investigation, and the Law*, pt. 1, chap 4.

[50] *Criminal Use of Personal Identification Information*, sec. 817.568.

[51] Easttom and Taylor, *Computer Crime, Investigation, and the Law*, pt. 1, chap. 4.

In the state of Idaho the legislators followed a different approach to the crime of identity theft. Namely, they enumerated in different statutes each potential aspect of identity theft and made each of them separately a crime in and of itself. For example, statute 18-3126 addresses the unlawful acquisition by a person of another person's personal identifying information without authorization, with the intention of obtaining credit, money, goods or services by the use of that information. Statute 18-3126A addresses the fraudulent acquisition of personal information of a person by someone who is pretending to be a member of the armed forces of the US or of another state authority. This statute deals with the crime of impersonating someone possessing state authority with the sole purpose of committing identity theft. Finally, the statute 18-3127 also criminalizes the acceptance of goods purchased through fraud. This dispersal of the legislation makes the identity theft laws of the state of Idaho rather time consuming for one to study and comprehend thoroughly, but the interesting fact about this identity theft legal framework is that it offers a plethora of possible ways for the law enforcement agencies and the prosecution authorities to cope with the variations of identity theft.[52]

In the New York legislation, identity theft is addressed in the penal code 190.77 - 190.84. In the first part of these provisions, a scaling of the identity theft crime, according to its severity and the financial damage, takes place, ranging from class A misdemeanor to class D felony. This indicates that the New York legislator took particular care when legislating, trying to identify the varying degrees of severity of this particular offence. However, the most significant thing about New York's identity theft law is that in the penal code 190.81 to 190.83, it lists three levels of crimes for possession of personal identifying information without authorization and also lists the different information that is treated as personal identifying information according to the specific piece of legislation. Namely, the law states: *"A person is guilty of unlawful possession of personal identification information in the third degree when he or she knowingly possesses a person's financial services account number or code, savings account number or code, checking account number or code, brokerage account number or code, credit card account number or code, debit card number or code, automated teller machine number or code, personal identification number, mother's maiden name, computer system password, electronic signature or unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person knowing such information is intended to*

[52] Ibid.

be used in furtherance of the commission of a crime defined in this chapter."[53] This is also important because it criminalizes the sole possession of information that can be used by someone in order to commit fraud. This means that even if there is no proof that someone committed any kind of fraud using another person's information, he can be charged for the sole possession of that information.[54]

The Maryland statute[55] for identity theft would not be mentioned in this chapter if it did not include some interesting details in its wording. First of all, in the respective provision, the legislator sets as the crime of identity theft the sole act of helping someone else to obtain personal identifying information. This helps, as in the New York statute, the law enforcement authorities to proceed with prosecutions, even before any economic damage has been caused. However, the most interesting, and at the same time controversial, fact about this statute is arguably the notion of specific electronic devices that can be used in order to gather information from credit cards, such as the re-encoders and the skimming devices. The controversy arises because of the fact that the specific law does not exclude the use of those devices for legitimate purposes, leaving that to the reasonable interpretation of the law by reasonable people. Although a prosecution against a developer of a card-scanning software has not yet taken place, according to the letter of the law it is, however, possible.[56] Additionally, the mention of specific technicological means that can be used for the commitment of identity theft can render the specific provision obsolete once those devices stop being used, due to the rapid evolution of the technology and their replacement by new more advanced devices. Nonetheless, this provision is, for the time being, rather unique and more sophisticated than other similar provisions in the US.

In this chapter, it became clear that the US legislators are not only aware of the offence of identity theft but that they have also placed particular importance on some critical and at the same time interesting additions to their provisions, in order to encompass the whole spectrum of this offence in particular. One could argue that these additions sometimes over-criminalize specific behaviours or that can be easily overtaken by the technology, due to their limited technological neutrality. Never-

---

[53] *NY Penal Code*, Title K, sec. 190.81.

[54] Easttom and Taylor, *Computer Crime, Investigation, and the Law*, pt. 1, chap. 4.

[55] *Md. CRIMINAL LAW Code Ann. § 8 - 301.*

[56] Easttom and Taylor, *Computer Crime, Investigation, and the Law*, pt. 1, chap. 4.

theless, in the US federal laws, along with the specific state laws, identity theft is being scrutinized through the potentially various aspects of the crime. For instance, the section revealed that the mere unauthorized possession of the victim's personal identifying information by one person can be prosecuted; that identity theft is not always attached to an ensuing fraud, but that it can be seen as an independent and specific crime; and that even the possession of specific electronic devices that are suitable for the commission of identity theft can call for criminal liability. Of course, some of the provisions mentioned can give rise to several questions and a lot of controversy. Notwithstanding that fact, the answers to these questions and the possible solutions to these controversies are going to be examined in the fifth chapter of this paper, where a comparison of the US and the Greek identity theft legal framework will be provided.

4 Identity theft in the Greek legal system

Unlike the United States of America, the whole information and communication technology field is rather new for Greece and its citizens. This is easily understandable, considering some interesting statistical figures. Namely, according to the Observatory for the Greek Information Society, the percentage of households having broadband internet access in 2009 was only 16%, a number which, in 2004, was only 0,09%.[57] However, things have changed drastically during the last six years and Greece has rapidly entered the so-called information age. According to the webpage Internet World Stats, approximately six million out of the total eleven million people who reside in Greece are Internet users, which roughly translates into 59,7% penetration of the Internet into the Greek society in December 2014.[58] That means that Greek citizens are now exposed to both the beneficial and the detrimental effects of the Internet, more than ever. The term 'detrimental' could, of course, reasonably be interpreted so that it covers the various forms of cybercrimes. Worth mentioning that the respective Internet penetration rate in the US though, observed in the same year (2014), which reached the percentage of 87% of the total population. This means that approximately 277 million Internet users exist in USA.[59] Of course the numbers are meaningless by themselves, but nevertheless they are indicators of the whole situation and it is important to have a generic idea about them.

One could argue that the greater the number of the people interacting with and being affected by something, the greater the need for regulatory actions. In other words, regulating the Internet in Greece and more specifically its criminal dimension, would more likely have been considered as a waste of time and valuable resources back in the year 2004 when, unlike the rest of the Western world, only the 0,09% of Greek households had access to broadband internet connections. The question that arises after taking under consideration this rapid growth of that percentage during the last ten years though, is whether the Greek legal system has adapted to the changes in the digital field or if it is still lagging far behind the new challenges, especially in terms of identity theft cybercrime. Before the answer to this question is pursued, there will be an indicative presentation of the Greek legal provisions that already exist and are being applied by the courts, when identity theft is the case.

---

[57] Vlachos et al., "The Landscape of Cybercrime in Greece," 114.

[58] "European Union - Data for the Member States of the European Union - GREECE."

[59] "United States of America - Internet Usage and Broadband Usage Report."

4.1 Provisions in the Greek Penal Code

The main legal instrument regulating the various criminal offences in Greece is the Greek Penal Code of 1985 [hereinafter P.C.]. Since then, numerous amendments have been made to its contents, by other special criminal laws, in a try to synchronize it and make it more suitable for the new challenges that arose through the years. Despite the amendments equipping the Greek P.C. with useful tools against the new technological era crimes, it still lacks of provisions dealing directly with specific cybercrimes, such as identity theft, as will be discussed in further details below. There are, of course, provisions regulating some of the most serious and infamous cybercrimes, such as child pornography or criminal copyright infringements.

Having said that, we are about to go through the most significant provisions of the Greek P.C. relating to countering identity theft in Greece. Worth mentioning though that according to the webpage of the Hellenic Police, which is the national police service of Greece, the Greek legal framework lacks specific provisions encompassing specific cybercrimes and especially identity theft. Even the Convention on Cybercrime of 2001[60]has not been implemented in the Greek legislature yet, despite having been signed on behalf of the Hellenic State. Consequently, Greek law enforcement authorities, in cases concerning cybercrimes, are forced to collaborate with the respective authorities of other European countries, the Council of Europe and other international organizations in order to confront these cybercrime cases. [61]

There are, however, some articles in the Greek P.C. that can be relied on in cases of identity theft. The most used provision of the Greek P.C., in cases of identity theft, is the one encompassing the "fraud committed with a computer". This article can be used merely when the act of identity theft is more of a preparatory to a fraud offence. More specifically article 386A P.C.[62] stipulates that everyone who intentionally and unlawfully attempts to enrich oneself or another, by causing damage to another through affecting computer data either by incorrectly executing a computer program or by

[60] *Convention on Cybercrime*.

[61] "Electronic Crime," n. Available only in Greek language.

[62] *The Greek Penal Code* art. 386A.

using wrong or incomplete data, or by causing damage to the data in any other way, shall be punished with imprisonment of at least three months, and if the damage caused is notably severe, with imprisonment for at least two years. In the third paragraph of article 386 P.C., where the punishments for the offence of fraud with a computer crime are mentioned, it is also mentioned that if a) the perpetrator commits frauds habitually or by profession and if b) the circumstances under which the crime has been committed indicate that the perpetrator is notably dangerous, the punishment is imprisonment of up to ten years. As we can see, there is no notion of the specific ways through which one can commit fraud, but the provision is rather general and requires the use of a computer to be present in order for the fraud to be considered as committed with a computer. For example, a theft from a bank Automated Teller Machine [ATM] can only be prosecuted in accordance with the wording of the aforementioned article of the P.C., whilst the act of skimming the victims PIN code will be rendered a preparatory act of the same crime and will get absorbed by the final act of theft. This means that if someone solely extracts PIN codes from ATMs with a skimming method, without, however, proceeding to thefts, he cannot be held liable of fraud committed with a computer.[63] However, the generic character of this provision gives law enforcement authorities the ease to prosecute any fraud having a computer as means, partially or fully, of its commitment, but it does not clarify the specific ways in which this computer fraud can be committed. In addition, the economic perspective of the specific crime is obvious, while the threatened punishment for the perpetrator is classified and varies according to the economic damage that the crime has caused to the victim. So in cases where no financial damage has been caused or attempted, the perpetrator cannot be accused for anything. However, as was mentioned earlier in this paper, identity theft can be committed, irrespective of financial gain purposes, such as defamation, rendering this provision incapable of confronting this specific crime.

Another frequently used provision of the Greek P.C., which illustrates some elements of identity theft, is the provision in article 370C P.C., following article 370 P.C.. Article 370C P.C. regards the protection of postal privacy. Article 370P.C. can be applied by the prosecutors against identity thieves who actually steal letters or information enclosed in letters belonging to another person. The provision mandates a fine or imprisonment up to one year if the victim files a complaint, but it cannot be used for an electronic identity theft, where technological means have been used to accomplish the purpose, such as phishing. Even though the scope of this article appears to cover electronic

[63] Board of appeals of Thessaloniki 28/2010 (Thessaloniki Board of appeals 2009).

postal privacy breaches, this breach has to be detected by the victim and followed by a respective complaint, which rarely happens in practice. Yet, in article 370C para. 2 P.C.[64],, the Greek legislator widens the protection of the postal privacy and renders as guilty anyone who obtains access to data that have been stored in a computer, an external memory of a computer or are being transferred through telecommunication systems, if the access was unlawful, and especially if the unlawful access occurred by the breaking of restrictions or security measures that the lawful owner (of the data) had previously instated. The perpetrator of the aforementioned offence shall be punished with imprisonment of up to three months or with a fine of at least 29 euros. It is important to note that the aforementioned offence cannot be prosecuted *ex officio*, but only after a complaint of the victim is filed as well. Additionally, this article can be useful in terms of identity theft, only if the data that the perpetrator is accessing unlawfully contain personal identification information but only if the victim finds out about this unlawful access, which rarely happens in most cases of identity theft. Another interesting aspect of this provision is that it addresses only the active unlawful access by the perpetrator and does not encompass the cases where the victim, after being deceived by the perpetrator, gives his personal data to the latter.

Although there is no criminal provision for one who commits identity theft, there is a provision which poses imprisonment of up to three months to the state employee who is responsible for issuing and drafting public documents, if he, while issuing or drafting those documents, omits to certify the identity of the person who is mentioned in the document as the law requires.[65] This provision prevents the Greek state from becoming liable for accommodating the commission of identity theft, at least in the public sector administrating authorities. This provision, however, applies in cases where someone impersonates another in front of the public authority employee, whilst we cannot be certain if this provision can be applied in an online setting, due to the lack of any online procedures available to the public within the Greek public sector.

The last provision of the Greek P.C. that can potentially be applied against the perpetrator of identity theft is the one encompassing cases of forgery. In article 216 P.C. the legislator regulates forgery offence by laying down that everyone who drafts fake or falsified documents, in order to mislead someone by its use about a fact which may have legal consequences, shall be punished with impris-

[64] *The Greek Penal Code* art. 370C, par. 2.

[65] Ibid. art. 243.

onment for at least three months, while the use of this document by him is to be considered an aggravating factor. The same punishment also applies to everyone who wilfully uses a fake or false document. If the perpetrator of the aforementioned offences intended to enrich oneself or another causing financial damage to another or intended to harm another shall be punished with imprisonment of up to ten years.[66]It goes without saying that under this provision, the identity thief who drafts a fake document or falsified a document using the personal identifying information of another will be prosecuted for the aforementioned acts, but not for the use of someone else's personal identifying information. In this case, we can distinguish three stages of the offence ranging from the actual identity theft, where the perpetrator steals the personal identifying information of another person, but in order to be prosecuted with article 216 P.C. he must use this information to draft a fake document or falsify documents and ultimately utilize it for his or someone else's benefit. Consequently, this article cannot encompass the crime of identity theft as such, but only the following use of the information in question.

4.2 Identity theft in other Greek legal instruments

Apart from the Greek penal code, there are other statutes that can apply to a varying degree, when identity theft occurs in terms of criminal liability. However, as this paper is about to present further on, the coverage against identity theft which these special legal instruments offer to the Greek judicial authorities is also restrained in terms of applicability. This is mainly due to the fact that these special laws do not regulate identity theft exclusively, but rather only some aspects of identity theft, corresponding to the general field that these laws were enacted to regulate.

The first example of a special law, that within its scope regulates identity theft to a certain degree, is Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data.[67] This law is an implementation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data

[66] Ibid. art. 216.

[67] *Law 2472/97.*

and on the free movement of such data,[68] as it was enacted by the Greek parliament in 1997. Given that the whole body of the specific law is regarding the protection of personal data, the focus of this paper will merely be on the penal sanctions that it stipulates in article 22 para. 4. which states the following: *"Anyone who unlawfully interferes in any way whatsoever with a personal data file or takes notice of such data or extracts, alters, affects in a harmful manner, destroys, processes, transfers, discloses, makes accessible to unauthorized persons or permits such persons to take notice of such data or anyone who exploits such data in any way whatsoever, will be punished by imprisonment and a fine and, regarding sensitive data, by imprisonment for a period of at least one (1) year and a fine amounting between one million Drachmas (GRD 1,000,000)[69] and ten million Drachmas (GRD 10,000,000), unless otherwise subject to more serious sanctions."*[70] Moreover, pursuant to para. 6 of the same article, the Greek legislator particularizes the penal sanctions against the perpetrator who aims to gain an unlawful benefit or harm another person by stating that: *"If the perpetrator of the acts referred to in paragraphs 1-5 of this article purported to gain unlawful benefit on his/her behalf or on behalf of another person or to cause harm to a third party, then s/he shall be punished with confinement in a penitentiary for a period of up to ten (10) years and a fine amounting between two million Drachmas (GRD 2,000,000) and ten million Drachmas (GRD 10,000,000)."*[71] The aforementioned paragraph encompasses the aggravated type of the offence described in the fourth paragraph of the same article, which is quite interesting. Namely, as we saw earlier in the subchapter above on the Greek penal code, there is no provision similar to the one in article 22 para. 4 of law 2472/97, which makes the latter the only provision in the Greek criminal legislation that renders the unlawful interference in any way whatsoever with a personal data file along with other actions against those data as a punishable crime. Accordingly, this is the sole legal tool for the Greek judicial system to confront offline and online incidents of identity theft. Moreover, another interesting fact about this law is that it renders guilty everyone who commits the offence of paragraph 4 of article 22, even if these actions were as a result of negligence, by stating the following in para. 8: *"If the acts referred to in paragraphs 1-5 of this Article were committed as a*

---

[68] Counsil of Europe, *Directive 95/46/EC of the European Parliament and the Counsil of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*.

[69] Ibid., n. Even though the official Greek currency is euro since 2001, the specific law is still mentioning the indicative fines in Greek Drachmas (GRD). For the ease of the reader it is useful to mention that the exchange rate between euro and Greek drachma is approximately 1€ = 341 GRDs .

[70] *Law 2472/97* art. 22, par. 4.

[71] Ibid. art. 22, par. 6.

result of negligence, then imprisonment for a period of at least three (3) months and a fine shall be imposed."[72] Nevertheless, this highlights how important the protection of the personal data is before the legislator's eyes, so even if someone unwillingly interferes with it, he or she may be held criminally liable under the said provision.

However, the aforementioned law regulates offences against personal data files, as is laid down in the first sentence of article 22 para. 4 of Law 2472/97. Therefore, it becomes quite interesting to analyze what exactly the legislator means by personal data file. As stated in article 2 (e) of Law 2472/97, *"personal data file shall mean any structured set of personal data which are accessible on the basis of specific criteria"*. In that sense, in order for a victim to be protected under the scope of the specific law, its personal data has to be structured as a set of information. So the question that inevitably arises is whether a victim of phishing, who hands his own personal data to the perpetrator, deceived by the latter's prior acts (deceiving email), can be protected. The answer is uncertain, given that in practice, the Greek courts can find someone who unlawfully interferes with personal data files guilty. But there is an absence of case law regarding the criminal evaluation of the actual identity thief who decisively gains access to these data in the first place. This means that in order to reveal the perpetrator of an identity theft, he must attempt to use this personal data in order for it to become clear that he unlawfully possesses the respective data. This renders the specific provision rather unfit to embrace the sole act of identity theft if it is not followed by another offence or if it is against personal data that are not structured as a set, as the law requires.

The last statute that will be presented in this chapter, as statute relevant to identity theft within the Greek legal framework, is Law 3471/2006 on the Protection of Personal Data and Privacy in the Electronic Communications Sector and Amendment of Law 2472/1997. This law is by and large an incorporation of Directive 2002/58/EC of the European Parliament and Council of the 12th July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector.[73] The approach of the paper to this statute will be the same as with the one used for Law 2472/97, namely we will focus on the statute's penal sanctions. But first, it is vital to take a closer look at the protection scope of the aforesaid statute.

---

[72] Ibid. art. 22, par. 8.

[73] Counsil of Europe, *Directive on Privacy and Electronic Communications*.

The aforementioned statute appears even more specialized than the one we examined earlier. Accordingly, Law 3471/2006 has as its object *"the protection of the fundamental human rights and privacy in particular, and the establishment of the conditions for the processing of personal data and the reservation of communication confidentiality in the electronic communication sector."*[74] This means that the applicability of this law is restrained to cases that involve the electronic communication sector somehow. In addition, the definition of personal data breach is of interest, defined as under the law as *"the security breach that leads to accidental or unlawful destruction, loss, distortion, unauthorized dissemination or unauthorized access of personal data that were transferred, stored or were subject to processing in any other manner in connection with the provision of a publicly available electronic communications service"*[75].

More specifically, and regarding the penal sanctions stipulated by this law, the focus shall be on article 15 paras. 1, 3 & 4. The second paragraph of article 15 is deliberately left out of this discussion, because it regulates the penal sanctions to be imposed against 'Controllers or representatives', who do not comply with the acts of the Personal Data Protection Authority and this has nothing to do with identity theft. Consequently, the main offence described in article 15 lies in the first paragraph and states: *"Anyone who unlawfully interferes in any way whatsoever with a personal data file of a subscriber or user, or takes notice of such data or extracts, alters, affects in a harmful manner, destroys, processes, transfers, discloses, makes accessible to unauthorised persons or permits such persons to take notice of such data or anyone who exploits such data in any way whatsoever, will be punished by imprisonment for a period of at least one (1) year and a fine amounting between ten thousand euro (10,000€) and one hundred thousand euro (100,000€), unless otherwise subject to more serious sanctions."* As we can see, pursuant to the first paragraph of article 15, the perpetrator of the unlawful acts cannot simply be any person, but rather someone who already has access to the personal data in question. Subsequently, in cases of identity theft, if the stolen personal data is the personal data protected under the scope of this law, the perpetrator can only be a person who already has access to this information, namely someone who is an employee of the controller of this data. In this case we are facing a very specific kind of identity thief, mentioned in subchapter 2.2.3.1 of this paper as "the insider", whilst the specific law cannot be applied against someone who obtained access to this kind of information using hacking methods for example.

---

[74] *Law 3471/06* art. 1.

[75] Ibid. art. 2, par. 11.

Moreover, in paragraphs 3 and 4 of the specific article, the offensive acts of paragraph 1 are confronted according to whether they have been purported to gain unlawful benefit for the perpetrator or a third person, or if they have been committed by negligence. In the first case, the law mandates imprisonment of up to ten years and fine from 12.000€ up to 150.000€. In addition, if the offence endangers the operation of the democratic constitution or national security, the punishment is confinement[76] and a fine ranging from 50.000€ up to 350.000€.[77] On the other hand, the commitment of the para. 1 offence by negligence is also punishable with imprisonment of up to eighteen months and a maximum fine of 10.000€.[78] Nevertheless these two last paragraphs of article 15 of Law 3471/06 illustrate the utmost importance that the processing of personal data by a 'controller' have for the Greek legislator.

As was attempted to shed light on in this chapter, the legal framework in Greece against identity theft is rather general and lacks of specialization, especially when it comes to identity theft. There are, of course, several provisions that can be applied in certain cases of identity theft, but there is no provision which specifically can encompass identity theft. In most of the cases, the penal procedure does not begin at the point when identity theft occurs, but rather after it has been committed and the 'stolen goods' (personal identifying information) are being utilized by the perpetrator in order to achieve an upper purpose (i.e. obtain benefit) through another criminal action (i.e. fraud). This is very important, bearing in mind the wording of the first article in the Greek P.C. which is titled "No punishment without law" and explicitly states: *"Punishment is not imposed except for those acts for which the law had expressly stipulated one before their commission"*.[79] This means that the Greek courts cannot impose any punishment to the perpetrator of a mere identity theft, unless one tried to employ the 'stolen goods' in the commitment of another crime, which is punishable by the Greek criminal law. In addition, an identity theft committed for a purpose other than economic gain, such as defamation or harassment, cannot be prosecuted through the existing Greek legislation on point, if not followed by another offence of economic nature.

---

[76] *The Greek Penal Code*, n. "confinement", according to article 53, par. 3 of the Greek P.C., is the imprisonment from 5 to 20 years imposed to felonies.

[77] *Law 3471/06* art. 15, par. 3.

[78] Ibid. art.15, par. 4.

[79] *The Greek Penal Code* art. 1.

Having established this, this paper will continue with a comparison of the two legal regimes presented, in terms of identity theft. Namely, the identity theft legal framework in the USA and the identity theft provisions of the Greek legal system.

5 Comparison and recommendations

5.1 Comparison

In the third chapter of this paper some indicative provisions regulating identity theft in the US legal framework were discussed, both at federal and state level. What was clearly revealed is that American legislation specifically regulates identity theft, both in terms of definition and of enumeration of the existing varieties of the offence. More specifically, through the Identity Theft and Assumption Deterrence Act of 1998 amendment of chapter 47 of title 18, United States Code, it becomes easy to conclude that the American legislator is well aware of the existence of this specific offence and that it realizes the need to encompass this offence by a specific Act. However, this development has not taken place in the Greek legal framework (chapter 4), where the rather outdated P.C. lacks any definition of the term and in particular provisions against identity theft. The respective special statutes are rather specialized to specific fields and not fully suited to handle specifically the crime of identity theft. Besides the lack of an explicit legal provision regulating identity theft in the Greek legislation, there are also other minor and major differences between the two regimes presented in the previous two chapters, which this chapter will point out and discuss.

To begin with, from the presentation in the third chapter of this paper, it is rather clear that under US legislation, the identity theft offence is clearly defined. This is very important, because it creates a clear benchmark for further discussion on the term. In the US federal provision, along with other state statutes, such as the ones from the states of Alabama and New York, it is explicitly stated what is exactly meant by the term ‘identity theft’. The provision for identity theft in the statute of New York, in addition to the definition, explicitly lists which information can be considered as personal information. Consequently, in order for the Greek legislation to become as efficient as possible, it is of great importance for the Greek legislator to lay down a similar definition for that offence in particular, stating a complete definition of the identity theft offence. Yet, it seems that the Greek legislator does currently not attribute great importance to the act of identity theft as a stand-alone crime, before it leads to another, more severe offence, such as fraud. On the other hand, encompassing identity theft in the language of a criminal provision would ease the criminal characterization of the acts prior to the fraud and it would be a solid protecting net against identity thefts which aim to

achieve other purposes than economic damage against their victims, such as identity thefts for defamation or harassment.

Moreover, it is noteworthy that some US states regulate the aforementioned non-economic types of identity theft. In addition to the identity theft committed by the perpetrator for economic benefit, some US state provisions have regulated the commission of identity theft for other purposes. This is very significant, as was discussed in the previous chapters of this paper, when the perpetrator of identity theft unlawfully acquires the personal identifying information of their victims, not solely for economic purposes. Once the identity thief possesses the personal data of another person, he can use this data in various ways to harm the victim. Accordingly, it is essential that the sole unlawful possession of personal data of another person is to constitute as an offence. However, in the Greek P.C. there is no such provision in order to protect the victim of identity theft directly. The provision of article 22 para. 4 of Law 2472/97 is specialized as to protecting personal data files, rather than personal data as such. This means that in order for a person to be protected within the scope of Law 2472/97, the perpetrators have to gain access to a structured set of data and, consequently, the targeted identity theft against a single person cannot be incriminated under this provision. In that sense, the need for the Greek P.C. to have a provision that encompasses identity theft is generated, without basing its scope to the type of personal data and the means where they are stored.

Similar wide-scope provisions against identity theft exist, as was mentioned in previous chapters, in the state statutes of Florida and New York, where the mere possession of personal information of another person without their consent is illegal. So, for example, if one gains access and possesses someone else's personal data without the latter's consent according to Florida's legislation, this act accompanied with the intention of using this data for the commission of another offence is enough for prosecution. In New York though, the mere possession of another person's personal information is illegal, without the need for the unlawful acquirer to have any intention for the commitment of any consequent offence. That seems as a fair way to confront identity theft given that, especially in terms of online identity theft, it is usual for the perpetrator to gather the personal information of numerous of victims within a short period of time, which makes this behaviour worth punishing due to the vast range of the affected individuals. For instance, obtaining personal information of another person deliberately to continue with fraud is an utterly different phenomenon to when using phishing methods or malicious software succeeds in the obtaining of personal identifying information of many individuals. In the second case, the perpetrator has to be punished solely because he offended

many individuals by stealing their personal information. This is something that the US legislation efficiently has predicted in many cases, unlike the Greek legislation. Thus, a penal provision in the Greek legislation targeting this goal would solve many problems in cases where the perpetrator unlawfully acquires personal information of many victims through separate actions (i.e. separate phishing emails) and proceeds by selling these information to a buyer in another country. In this case, a provision outlawing the mere acquisition and possession of personal information of another person, regardless of whether a follow up offence is committed, would protect more efficiently the interests of the victims. However, it could reasonably be argued that the criminalization of the mere acquisition of someone else's personal information could be considered as an over-criminalization of the specific act and an over-protection of the data owner's interests. Then it is left to the legislator's understanding as to which is the perfect analogy for the provision.

Having said that, it is worth recognizing a recent Greek case[80] in which the perpetrator got arrested for unlawfully possessing personal identifying information of nine million Greek citizens. This case is currently still in its preliminary stage. In the given case, the only way that he can be found guilty is if the prosecution proves that this personal information that he possesses belongs to a personal data file so that he can be prosecuted for breaching the provision of para. 4 of article 22 of Law 2742/97. If, however, this great amount of personal data has been gathered, one file at a time, from separate individuals with a method, such as phishing, and if there will be no proof of a follow-up offence being committed, the unlawful acquirer of personal data belonging to nine million unique Greek citizens will fall in a legal vacuum that exists and the judicial system will not be able to convict him. Even though this great amount of personal information has to be some kind of personal data file, due to the great number of it, in a case where this information is the product of many single personal attacks via phishing emails, it will be very interesting to see how the prosecutions authorities and the courts will handle cases of this type, without a criminal provision encompassing identity theft.

One of the most peculiar provisions we saw in the third chapter was the one from the criminal law code of the state of Maryland[81], which criminalized more or less the use of specific electronic devices. Under this statute, the use of electronic devices that can be used in order to extract infor-

[80] Steadman, "Hacker Arrested for Allegedly Stealing ID Info of Most of Greece."

[81] *Md. CRIMINAL LAW Code Ann. § 8 - 301.*

mation for credit cards, such as re-encoders and skimming machines, is greatly restricted. However, legitimate use of those devices are not excluded from the scope of the penal law. This broad restriction is rather strange and unique in terms of criminal law for the following reasons. Firstly, these devices can be used for legitimate purposes also and by that use they can lead to the obtaining of useful practical information countering identity theft. Consequently, the sterile criminalization of those devices can possibly harm the total confrontation of the specific offence. Instead, a more useful approach could possibly be when a clear case of identity theft is accompanied with the possession of those devices, leading to an aggregated form of the offence. In addition, these 'illegal' devices, are likely to become obsolete due to the leaping technological advances of our days, rendering the mere provision, and its explicit reference to a specific technology, obsolete. It would be preferable for the provision to be more technologically neutral. Therefore, it would be wiser for the Greek legislator, in an attempt to address identity theft in the Greek penal legislation, to avoid the criminalization of specific devices for the two aforementioned reasons and in order to protect the integrity and reliability of the Greek legislation. Such criminalization of specific devices by the Greek legislator would not only be against the principle of technological neutrality, but it would lead to the adoption of half measures against identity theft. Instead, the drafting of respective legislation from scratch appears more suitable.

5.2 Recommendations

Having compared and highlighted these interesting aspects of the US legislation, in terms of identity theft, along with the arguably weak respective Greek counterpart, it becomes imperative to suggest few reforms on point. Although this paper was meant to be rather neutral without any strong recommendations, the inadequacy of the Greek legal framework in the cybercrime[82] and, more specifically, the identity theft field, calls for, at least, the suggestion of what the next step should be for the Greek legislators in terms of identity theft.

It is indubitable that at least as a first step, the Greek legislation regarding cybercrime in general should be enriched by the enactment of the ratification of the Convention on Cybercrime[83]. Alt-

[82] "Electronic Crime."

[83] *Convention on Cybercrime*.

hough this convention has been signed on behalf of Greece, it has not been implemented in any Greek piece of legislations yet. Nevertheless, this implementation would be a positive first step towards the regulation of the internet, especially in terms of criminal law and cybercrime.[84]

Moreover, identity theft as a crime and a cybercrime in particular cannot be left unregulated. The US laws provide the Greek legislator with an arsenal of possible approaches and available options. Therefore, given that identity theft as a criminal offence – especially within the digital environment– is quite new and that the already existing laws struggle to regulate it, it seems reasonable that a new provision on identity theft should be added to the Greek P.C. Namely, a new provision defining the crime of identity theft seems necessary for the time being, so as to consider what qualifies as an identity theft, what kind of information can be considered as personal identifying information, and by which actions one can be prosecuted for committing identity theft,. In order to draft a useful provision though, the Greek legislator has to take under consideration not only other legal regimes, but also the Greek reality, along with the general interaction between the Greek citizens and the Internet. This can be justified by thinking that the less experienced someone is with something new, the greater the legal protection should be. Consequently, since the internet only relatively recently became a tool of people's everyday lives in Greece, the Greek legislator has to protect its users from the criminals.

However, perhaps the most desirable thing regarding the regulation of identity theft as a cybercrime, along with all the other known cybercrimes, would be the enactment of a global legislation regulating the internet, as a means of communication, regardless of the actual national borders, applicable to every country. Of course that sounds and probably is very difficult to achieve but, given that in most of the cases of identity theft the perpetrator is usually located miles or even continents away from his victim that appears to be the only efficient solution. In the meanwhile though, and until this goal of a global legislation is achieved, the Greek legislator has to confront the constantly growing threat of identity theft with a piece of targeted and exclusive legislation, within the legislative borders of Greece.

[84] "Electronic Crime."

6 Conclusion

The identity theft cybercrime is undoubtedly one of the most frequently committed cybercrimes nowadays. This is due to the fact that identity theft is not new. Rather, it existed long before the Internet and other new technological means entered our everyday lives, but not in its cyber form. In the so-called information age, however, the identity theft incidents have multiplied. Subsequently, the need for legislative actions encompassing this new facet of the erstwhile identity theft offence is now even more unquestionable. Back in the days, perhaps the regulation of offences that followed the identity theft offence was enough to protect the interests of the victims. However, the new technology has rendered the personal identifying information of every member of the society more vulnerable than ever before. As we saw, countries that are more familiar with the Internet and its effects, such as the USA, already have a legal framework tailored in a suitable way to handle identity theft as a unique and independent offence, whereas in countries lacking this long-lasting experience with the Internet, such as Greece, the legislation lacks of effective provisions and confrontation tools against this new offence.

Accordingly, it seems crucial that the Greek legislator addresses this new facet of identity theft with a new set of penal provisions, so as to clarify what the definition of the specific offence is; which are the ways in which it can be committed; and whether or not one can be found guilty for the mere possession of personal identifying information, regardless of the fact if the information is used for the commitment of a following offence. It is rather important though, that this new piece of legislation is as technologically neutral as possible and that it will not criminalize the mere acquisition of someone's personal identifying information, by someone else, for legitimate purposes.

The identity theft provisions under the US legal framework appear quite organized and encompassing the full spectrum of the offence and its variations. Hence, something similar has to be the aim for the Greek legislator as well. This will help the Greek state to protect the interests of its citizens who are users of the Internet and set the foundations in the legislation for the modernization of the Greek legislation as a whole. The implementation of the findings of the Convention on Cybercrime would certainly be a good first step, but in terms of criminal law, a more specialized and suitable legislation would create the safety net needed to regulate the criminal activities taking place online.

Having said that, and bearing in mind that a global legislative approach based on the Internet and at the same time applicable in every country seems rather unrealistic, if not utopic at the time being, identity theft along with the other cybercrimes have to be addressed as soon as possible, in order to fill the legal gaps that exist in the Greek penal laws. Therefore, if a respective legislation stipulating identity theft gets enacted, the phenomenon of stolen personal identifying information for economic and non-economic purposes will stop and the perpetrators will have to think twice every time they try to unlawfully obtain these information. In addition, the Internet users will feel safer and more protected, at least against identity thefts occurring within the borders of the Greek state.

7 Table of references

List of judgements/Decisions

Board of appeals of Thessaloniki 28/2010, (Thessaloniki Board of appeals 2009).

Statutes and Treaties

Alabama Consumer Identity Protection Act. *ALA CODE*, 2006. http://codes.lp.findlaw.com/alcode/13A/8/10/13A-8-192.

Counsil of Europe. *Directive 95/46/EC of the European Parliament and the Counsil of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, 1995. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

———. *Directive 2002/58/EC of the European Parliament and of the Counsil of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, 2002. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002L0058.

Criminal Use of Personal Identification Information. *Florida Code, Title XLVI*, 2001. http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0800-0899/0817/Sections/0817.568.html.

Identity Theft and Assumption Deterrence Act of 1998. *U.S.C. Title 18*, 1998. http://www.gpo.gov/fdsys/pkg/PLAW-105publ318/pdf/PLAW-105publ318.pdf.

Law 2472/1997 on the Protection of Individuals with Regard to the Processing of Personal Data, 1997. http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%202472-97-APRIL010-EN%20_2_.PDF.

Law 3471/2006 on the Protection of Personal Data and Privacy in the Electronic Communications Sector and Amendment of Law 2472/1997, 2006. http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW_%203471_06EN.PDF.

Md. CRIMINAL LAW Code Ann. § 8 - 301. *Maryland Criminal Law*. Accessed December 8, 2015. http://www.lexisnexis.com/hottopics/mdcode/.

NY Penal Code. *Part 3*. Vol. Title K. Accessed November 12, 2015. http://ypdcrime.com/penal.law/article190.htm#p190.81.

The Convention on Cybercrime of the Council of Europe, 2001. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

The Greek Penal Code, 1985. http://www.eayth.gr/misc/pd_fek106_85.pdf.

Secondary Literature

Biegelman, Martin T. *Identity Theft Handbook: Detection, Prevention, and Security*. Hoboken, N.J: Wiley, 2009.

Christensson, Per. "Botnet Definition." *TechTerms*, June 9, 2010. http://techterms.com/definition/botnet.

———. "Cyberbullying Definition." *TechTerms*, September 15, 2009. http://techterms.com/definition/cyberbullying.

———. "Cybercrime Definition." *TechTerms*. Accessed October 16, 2015. http://techterms.com/definition/cybercrime.

———. "Denial of Service Definition." *TechTerms*, August 11, 2011. http://techterms.com/definition/denial_of_service.

———. "DNS Definition." *TechTerms*, August 30, 2014. http://techterms.com/definition/dns.

———. “Malware Definition.” *TechTerms*. Accessed October 17, 2015. http://techterms.com/definition/malware.
———. “P2P Definition.” *TechTerms*. Accessed October 17, 2015. http://techterms.com/definition/p2p.
Clough, Jonathan. *Principles of Cybercrime*. Cambridge, UK; New York: Cambridge University Press, 2010. http://site.ebrary.com/id/10392920.
Easttom, Chuck, and Jeff Taylor. *Computer Crime, Investigation, and the Law*. Boston, MA: Course Technology, 2011.
“Electronic Crime.” *Hellenic Police*. Accessed November 19, 2015. http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414ENEN.
“European Union - Data for the Member States of the European Union - GREECE.” *Internet World Stats*, December 31, 2014. http://www.internetworldstats.com/europa.htm#gr.
Gomes, Norberto Nuno. *Electronic Identity*. New York: Springer, 2014.
Internet World Stats. “Internet Usage Statistics: The Internet Big Picture - World Internet Users and 2015 Population Stats.” *Internet World Stats*. Accessed October 16, 2015. http://www.internetworldstats.com/stats.htm.
Jakobsson, Markus, and Steven Myers, eds. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Hoboken, N.J: Wiley-Interscience, 2007.
Kitten, Tracy. “ID Theft: Insider Access Is No. 1 Threat.” *Bank Info Security*, November 9, 2010. http://www.bankinfosecurity.com/interviews/id-theft-insider-access-no-1-threat-i-836/op-1.
Kowalski, Robin M, Sue Limber, and Patricia W Agatston. *Cyber Bullying: Bullying in the Digital Age*. Malden, MA.: Blackwell Pub., 2008. http://public.eblib.com/choice/publicfullrecord.aspx?p=320066.
NoBullying.com. “Is Cyberbullying a Crime? Hopefully Soon!” *NoBullying.com*, May 21, 2015. http://nobullying.com/is-cyberbullying-a-crime/.
Steadman, Ian. “Hacker Arrested for Allegedly Stealing ID Info of Most of Greece.” *WIRED.CO.UK*, November 22, 2012. http://www.wired.co.uk/news/archive/2012-11/22/greece-id-theft.
Timm, Carl, Richard Perez, and Adam Ely. *Seven Deadliest Social Network Attacks*. Syngress Seven Deadliest Attacks Series. Burlington, MA: Syngress/Elsevier, 2010.
“United States of America - Internet Usage and Broadband Usage Report.” *Internet World Stats*, 2014. http://www.internetworldstats.com/am/us.htm.
US Department of Justice. “Identity Theft.” *The United States Department of Justice*. Accessed November 9, 2015. http://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.
Vaughan, Annie. “Teenage Flash Mob Robberies on the Rise.” *FoxNews.com*, June 18, 2011. http://www.foxnews.com/us/2011/06/18/top-five-most-brazen-flash-mob-robberies/.
Vlachos, Vasileios, Marilena Minou, Vasillis Assimakopoulos, and Androniki Toska. “The Landscape of Cybercrime in Greece.” *Emerald Group Publishing Limited*, Information Management & Computer Security, 19, no. 2 (2011): 113–23. doi:10.1108/09685221111143051.
Wall, David S. *Cybercrime: The Transformation of Crime in the Information Age*. Vol. 4. Crime and Society Series. Polity, 2007.
Yar, Majid. *Cybercrime and Society: Crime and Punishment in the Information Age*. 1st ed. London ; Thousand Oaks, CA: SAGE Publications, 2006.