The Problems of Investigation of Identity Theft in SNS[i]

Arkadiusz Lach

Nicolaus Copernicus University in Torun

Faculty of Law and Administration

Ul. Bojarskiego 3, 87-100 Torun, Poland

arkadl@umk.pl

ABSTRACT

The investigation of identity theft is not an easy task. The electronic environment of the Internet makes the task even more difficult. The problem is complex and therefore it is worth looking at chosen aspects. The author presents the issue of the modus operandi of the perpetrators, the criminalization of identity theft, and problems in the gathering of evidence by law enforcement and the victims. The problems are presented in the light of digital forensic and new legal tools for gathering of evidence. The specific environment of Social Networking Sites was chosen to present the issues because of the popularity of the services, especially among minors.

KEYWORDS

identity theft, social networking sites, electronic evidence, digital forensic, cybercrime, investigation.

THE GROWING THREAT OF IDENTITY THEFT

Identity theft is sometimes called the crime of the 21st century. The growth of the crime in the last 20 years is without precedent. ID theft poses a threat not only to individuals, but also to e-services, especially the financial ones. A survey conducted recently in Australia shows that 20 percent of the respondents reported misuse of their identity in the past[ii]. Also a survey conducted in the UK shows that 8.8 percent of respondents were identity fraud victims in the previous 12 months and 27 percent at some point in time[iii]. It is estimated that the loss to individuals in the UK because of identity fraud is 3,3 billion pounds[iv]. Besides, the victim must spend a considerable period of time to restore credibility and prove innocence.

Similarly, Social Networking Sites (SNS) are a phenomenon of the 21st century. The number of registered users and the time spent by them on the sites are enormous.

Identities have become a valuable commodity, which can be sold and bought in the underworld. The same has happened with social network accounts. They are used by criminals and criminal organizations to commit a crime or to evade criminal responsibility.

Therefore the issue of identity theft in SNS is a serious problem for law enforcement and the users of SNS. It is worthwhile to look at what are the most important problems of identity abuse in SNS and what are the solutions for prevention and effective prosecution.

MODUS OPERANDI OF THE PERPETRATORS

ISBN: 978-1-941968-02-4 ©2014 SDIWC

There are many different ways of committing ID theft in SNS. Generally ID theft in the SNS environment can be committed as a false account creation or a real account takeover (hijacking).

Creation of a false account in SNS can be done quite easily, as the services generally do not check the identities of their users. Therefore it is easy to gather some data about an individual and create his or her profile with at least some information being true. The data could be obtained from open source databases or could be known to the perpetrator from other sources.

Example: during a party three teenagers decided to send on the Internet hate post concerning their teacher. In order to conceal their identity, they decided to create a fake profile of one of their colleagues on SNS. They took his image from class picture and entered some data they knew and some which was fictional in the profile. They also placed some insulting remarks concerning the teacher in the profile and sent a hate message to her.

An account takeover happens when a legitimate user is deprived of access to his account. This may be done by different means. Phishing and hacking are the most popular methods, but there are also cases when the victim voluntarily hands out login and password to the perpetrator (especially in the case of teenagers) and the latter then changes the password, closing the victim access to the account.

Example: as a sign of love and mutual trust two teenagers exchanged the passwords to their profiles on Facebook. Shortly after that the relation broke down and the boy changed password to the profile of his ex-girlfriend making access for her impossible and then published some intimate pictures on the profile, sending information about that to all friends.

As indicated in the above examples, after the creation or takeover of the profile, the perpetrator usually commits further unlawful acts: defamation, insult to other users, cyberstalking.

Besides SNS may be used to gather personal information needed for identity crime. As the users place plenty of information on their profiles, they are very valuable sources of data.

The evidence of the above mentioned unlawful activities could be: the IP address of the person creating the account, the IP addresses of logging on to the service, post or messages sent or received, files stored or displayed in the profile, lists of contacts, addresses, e-mails, phone numbers, and other contacts and personal data presented on the websites. Unfortunately, there are significant differences between SNS concerning processing of user data. For example some of them retain the first and last IP logs while others do not have them available.

THE CRIMINALIZATION OF IDENTITY THEFT

The natural answer to the negative behavior is criminalization of the act. This has been done in the case of ID theft by many states. However, the models of criminalization are different. Most of the states have criminalized the unauthorized use of personal data of another person with the intent to commit a crime. This usually is connected with financial crimes. However, some states criminalize also the unlawful use of someone's else personal data in order to harass the person. There are also provisions concerning impersonation and defamation. The European Union is calling for the criminalization of ID theft[v]. Also the Council of Europe experts have expressed the opinion,

ISBN: 978-1-941968-02-4 ©2014 SDIWC

that the Budapest Cybercrime Convention 2001 obliges the parties to criminalize certain aspects of ID theft[vi].

EVIDENTIAL PROBLEMS ENCOUNTERED BY LAW ENFORCEMENT

ID theft is a challenge for law enforcement for several reasons. First of all, the victim usually did not see the perpetrator or have physical contact with him during the commission of the crime. Secondly, in the prevailing number of cases, the trail is only in an electronic form which calls for forensic examination. The development of wireless networks is the next problem.

It could be observed, that although there is no physical contact, in many cases of ID theft on SNS the perpetrators know the victims, as such crime is usually not committed for financial purposes, but rather for harassment of the victim or other persons. Typical examples of perpetrators are school friends and ex-friends or ex-partners. Therefore the investigator must ask the victim about any persons in a possession of passwords or personal data used, who could be potential culprits.

The fact that evidence is in an electronic form will not render it inadmissible. Usually the same rules as in the case of paper documents apply, and evidence in such form is accepted nowadays worldwide. However, there are two issues which must be underlined. First, the evidence must be secured in a way which ensures its authenticity, especially if it is likely to be challenged in a court. Secondly, it is very important to have the precise time of preservation of evidence. In case of content it is important if the content in the profile changed. In case of logs they must correlate with other evidence. It happens, that when the time of logging into the services shown by the server is not compared with a real time at the moment of gathering, they later do not match with the internet access logs and therefore there is reasonable doubt resulting in the acquittal of the accused.

The investigator must look in the computer of the victim and ask service providers for traffic and user data. As it is pointed out, Social Networking Sites contain a huge amount of various evidence, which makes them a particularly valuable source of evidence[vii]. One of the most significant problems is that often the SNS have headquarters abroad with the biggest of them located in the US. Therefore it is often difficult or even impossible to get information from them. One of the best examples is Facebook and Google services. If the evidence is not provided voluntarily, the investigator must use mutual assistance channels which are very time consuming and offer little chance of success. However, some of the data, especially content, are publicly available and can be obtained by the investigator without any request.

The next issue is the use of wireless networks by criminals. Having in mind that the offenders often use publicly the available wireless networks or badly secured wireless networks of private persons and institutions, the only possibility is to detect them in real time. But in many legal systems the interception of communications can be applied only in case of the most serious crimes. Identity theft is rarely punished severely enough to be regarded as a serious crime. Therefore the severity of the punishment is not a reason for including the crime on the list of crimes where interception is possible. On the other hand, if detection of the perpetrator is possible only by the use of

ISBN: 978-1-941968-02-4 ©2014 SDIWC

interception, lack of the ability to use it would result in the impunity of the offenders.

A very sensitive problem is the use of remote search for computer investigations. The tool is very attractive for law enforcement agencies, but also very controversial concerning the right to privacy. In Germany the instrument was challenged before the Constitutional Court, which declared the state regulation unconstitutional[viii]. Despite that, a slightly modified regulation was introduced at the federal level, enabling the police to search secretly computer systems and networks[ix]. Similar regulations exist also or are proposed in other countries. The remote search gives law enforcement the ability to check the computer of the suspected person without alarming the person. Fortunately, in the case of ID theft, remote search does not seem to be a key instrument for gathering evidence and bearing in mind that identity theft is not a serious crime, it rather will not be possible to use it for investigative purposes under domestic law.

An increasing number of SNS users access their profiles from mobile devices which makes the gathering of evidence more difficult[x]. The other problem is the growth of cloud computing services. This forces law enforcement agencies and digital forensic experts to look at which provider is processing the data and in the case of foreign providers there is again the problem of getting data from them. Besides, the processing of personal data in the countries with low data protection increases the danger of data breach or unauthorized access.

The investigator must also look for any sign of malicious software which may raise the question of the use of the computer by a third person, especially as a piece of botnet. It may happen that the legitimate user is not aware that his computer is being used to commit a crime.

As access to accounts in SNS is password protected, there is the problem of requiring the suspect to reveal the password. Courts in some legal systems, including England, have allowed such an order, arguing that the password is something existing independently of the will of the suspect[xi]. However, if the privilege against self-incrimination is to be treated seriously, it cannot be accepted that information which is in the mind of the suspect and could be only communicated by him to the authorities, has an existence independent of the will of the suspect[xii]. Therefore the investigators must oblige the SNS operators to provide access data or order a forensic expert to break or circumvent the protection.

EVIDENTIAL PROBLEMS ENCOUNTERED BY VICTIMS

In some legal systems criminal acts which could be regarded as ID theft are prosecuted by the victims acting as private prosecutors. In this case, the burden of identifying the offender, prosecuting him, and proving guilt rests on the victim. Having in mind the specific sources of evidence and legal protection of certain kinds of data, it is sometimes very difficult or even impossible to secure conviction of the offender.

It is relatively easy to get the content of SNS as normally it is publicly available. However, owing to the fact that it usually will be presented as evidence in several months, it is necessary to ensure proper authentication, as the perpetrator may change or even remove the profile. Therefore it is necessary to prove that certain content was available at a certain date. This could be done by screen shots, photographs, witnesses, and so on. One of the

ways practised sometimes in Poland is to make screen shots in the presence of a notary, who confirms in a protocol that such content existed at a certain point of time. This method is accepted by courts, despite the fact that such evidence could be easily forged. Certainly the best way to preserve evidence in the circumstances is to make a digital copy of the profile with digital watermarks and check-sums.

One of the key problem is the protection of telecommunication data. Under domestic law it is often available only for law enforcement agencies. So even if the victim knows the IP address of the perpetrator, it is impossible for him to establish who is the user of the address.

This issue was analyzed by the European Court of Human Rights in the case KU v Finland[xiii]. In the case somebody created a profile of real teenager on dating sites, posting information that the boy was interested in homosexual relations. The telephone of the boy was given in the profile, so he received many indecent calls from adults, which had a very negative impact on the child. As the parents intended to identify the perpetrator, they asked the service provider for user data. This was refused, because under Finnish law only law enforcement agencies were authorized to demand traffic and subscriber data. This led to the impunity of the offender and the victim complained to the European Court of Human Rights. Finding a breach of the article 8 of the European Convention on Human Rights, the Court underlined that a state has a positive obligation to protect the privacy of its citizens and therefore it is obliged to provide them with effective legal tools necessary to detect and prosecute offenders, especially in cases like that, when the victim was a child. As the Court observed:

"the existence of an offence has limited deterrent effects if there is no means to identify the actual offender and to bring him to justice. Here, the Court notes that it has not excluded the possibility that the State's positive obligations under Article 8 to safeguard the individual's physical or moral integrity may extend to questions relating to the effectiveness of a criminal investigation even where the criminal liability of agents of the State is not at issue (…). For the Court, States have a positive obligation inherent in Article 8 of the Convention to criminalize offences against the person, including attempted offences, and to reinforce the deterrent effect of criminalization by applying criminal-law provisions in practice through effective investigation and prosecution".

The judgment of ECHR obliges all parties to the European Convention on Human Rights to introduce adequate legal instruments of identity theft investigation. It is not enough to criminalize identity theft. The law must be enforced effectively as well. Therefore identity crime must not be prosecuted by private persons, but by law enforcement agencies. In the case of defamation, the public prosecution service in Poland has an opportunity to initiate investigation or take over the proceedings from the victim if the public interest calls for that.

A very interesting problem is what is the legal basis for an identity theft victim demanding personal data from SNS. In Poland two possibilities are generally available for private persons: a demand by the subject of the personal data to access his data or a demand by another person showing lawful interest in obtaining personal data of somebody else. The issue is if the victim is the data subject in the case. From one side, it is his name in the profile, from the other he denies creation of the account. Having in mind the need for the

ISBN: 978-1-941968-02-4 ©2014 SDIWC

protection of the victim, the first possibility should be advocated.

The issue raised before the Polish courts in private prosecutions was whether in cases of private prosecution an indictment could be filed against unknown person with a view to identifying the person during court proceedings. Generally such a possibility is rejected, as judicial proceedings are conducted against certain persons and the lack of indication of the accused is regarded as the lack of a formal requirement of the indictment. Nevertheless some courts allow anonymous indictments, then ordering the police to identify the offender.

WHICH SYSTEM OF IDENTIFICATION?

The evidential problems experienced in the case of ID theft in SNS pose a question as to which system of authentication should be used in the services. Traditionally it is possible to create anonymous or fake accounts which also provide an opportunity of abuse for the criminals. On the other hand, the possibility of the creation of such a profile may be regarded as a question of the privacy of individuals. There is no doubt that requiring proof of identity would discourage many persons from using SNS. It would also be very difficult from an organizational and technical point of view. Therefore the existence of so called digital identities must be accepted. The introduction of highly advanced methods of authentication to SNS would sacrifice privacy for the sake of security, which does not seem to be rational and necessary.

CONCLUSIONS

ID theft is a growing threat to society with potential long-lasting effects, which are sometimes overlooked or underestimated. Therefore effective prosecution is very important and the incidents must not be trivialized. Of course, the key issue is the education of the Internet and SNS users not to expose their personal data in ways which may result in hard to detect identity theft. It is also necessary to train law enforcement and digital forensic experts in new areas of cybercrime, where the gathering of evidence is specific and difficult. Joint seminars of LEA and operators of SNS are also necessary to strengthen public – private partnership in combating cybercrime and to exchange information about new threats and technical possibilities of detection.

REFERENCES:

[i] The publication was prepared within the research project „Penal law reaction on the identity theft phenomenon". The project was financed by the National Science Centre in Poland on the base of the decision number DEC-2012/07/B/HS5/03792.

[ii] R. G. Smith, A. Hutchings, Identity Crime and Misuse in Australia: Results of the 2013 online survey, AIRC Reports 128, p. x.

[iii] National Fraud Authority, Annual Fraud Indicator, June 2013, p. 24

[iv] National Fraud Authority, Annual Fraud Indicator, June 2013, p. 30.

[v] Commission of the European Communities, Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. Towards a general policy on the fight against cyber crime, Brussels 22.05.2007, COM (2007) 267 final, p. 8. .

[vi] Cybercrime Convention Committee (T-CY), *T-CY* Guidance Note # 4. Identity theft and phishing in relation to fraud, Strasbourg, 5 June 2013, T-CY (2013) 8E Rev, pp. 3-6.

[vii] J. P. Murphy, A. Fontecilla, "Social Media Evidence in Government Investigations and Criminal Proceedings: A frontier of New Legal Issues", Richmond Journal of Law and technology, vol. XIX, issue 3, s. 4.

[viii] Judgment from 27 February 2008, available at http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

[ix] Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (BKATerrorG), G. v. 25.12.2008 BGBl. I S. 3083.
[x] N. Al Mutawa, I. Baggilli, A. Marrington, "Forensic analysis of social networking applications on mobile devices", Digital Investigation 9 (2012), pp. 524-533.
[xi] M. O'Floinn, D. Ormerod, "Social Networking Material as Criminal Evidence", Criminal Law review 7 (2012), pp. 508-509.
[xii] Compare the judgment of the ECtHR in Funke v. France from 25 February 1993, application nr 10828/84, http://hudoc.echr.coe.int/sites/eng/Pages/search.aspx#{"fulltext":["funke"],"itemid":["001-57809"]}
[xiii] KU v Finland, judgment of the ECtHR from 2 December 2008, application nr 2872/02, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-89964#{"itemid":["001-89964"]}

ISBN: 978-1-941968-02-4 ©2014 SDIWC