

Identity theft: is there a need for a specific legislation?

Dagmar Ösp Vésteinsdóttir & Fanney Björk Frostadóttir

What is identity theft?

Our society is nowadays increasingly relying on personal identity to identify individuals in various circumstances such as national security and crime but also immigration and taxation. The private sector as well as individuals also use identity for banking, property ownership and a wide range of other transactions. But what is identity?

Identity may take the form of a set of information and documentation that can be used to establish who we are as unique individuals and also link to other information about us.¹ Identity may be defined as the fact of being who or what a person or thing is.² According to that identity can be a number of personal information such as a name, date and place of birth, social security number, a fingerprint, a person's parent's name, driver's license, passport, computer usernames and passwords, e-mail addresses, pictures that can be found on social media. In fact whatever a person uses in real life to identify themselves. When someone uses another person's identity and the person doesn't know about it or it is done without their permission it might be what is called identity theft. The criminal misuse of identity is a major concern precisely because of its universal and ubiquitous nature, and because of its pivotal role in structuring societal interactions.

There are a number of ways in which identity theft may be perpetrated, both with and without the use of technology. The following list is just examples, number of other methodologies exist, but it is known that identity theft can be perpetrated by³:

- Rummaging through rubbish for personal information.

¹ „Scoping Paper on Online Identity Theft. Ministerial Background Report DSTI/CP(2007)3/FINAL“: <http://www.oecd.org/sti/40644196.pdf>

² „Oxford dictionary definition“: <https://www.lexico.com/en/definition/identity> (11 júní 2019)

³ „Scoping Paper on Online Identity Theft. Ministerial Background Report DSTI/CP(2007)3/FINAL“: <http://www.oecd.org/sti/40644196.pdf>

- Retrieving personal data from redundant IT equipment and storage media including PCs, mobile phones, USB memory sticks and hard drives that have been disposed of carelessly at public dump sites, given away or sold on without having been properly sanitized.
- Using public records about individual citizens, published in official registers such as electoral rolls.
- Stealing bank or credit cards, identification cards or passports. Skimming information from bank or credit cards using compromised or hand-held card readers, and creating clone cards. Using contactless credit card readers.
- Stealing personal information from computers using breaches in browser security or malware such as Trojan horse keystroke logging programs or other forms of spyware.
- Hacking computer networks, systems and databases to obtain personal data, often in large quantities.
- Exploiting insider access and abusing the rights of privileged IT users to access personal data on their employers' systems, infiltrating organizations that store and process large amounts or particularly valuable personal information.
- Brute-force attacking weak passwords and using inspired guesswork to compromise weak password reset questions.
- Obtaining castings of fingers for falsifying fingerprint identification.
- Browsing social networking websites for personal details published by users, often using this information to appear more credible in subsequent social engineering activities.
- Diverting victims' email or post in order to obtain personal information and credentials such as credit cards, billing and bank/credit card statements, or to delay

the discovery of new accounts and credit agreements opened by the identity thieves in the victims' names.

- Low security/privacy protection on photos that are easily clickable and downloaded on social networking sites.
- Befriending strangers on social networks and taking advantage of their trust until private information is given.

The most common type of identity theft is financial identity theft. That is when someone wants to gain economical benefits in someone else's name. This includes getting credits, loans, goods and services, by claiming to be someone else. Then we have Criminal identity theft that is when a criminal identifies himself to police as another individual at the point of arrest. In some cases, charges may be placed under the victim's name, letting the real criminal off the hook. Victims of Criminal identity theft might only realize such incidents by chance, for example by receiving a court summons or through background checks performed for employment purposes.

In a case from Sweden from 2017 the Stockholm District Court declared the CEO of Sweden's largest security firm, Securitas, bankrupt after his identity was stolen. The ruling was reversed quickly as soon as the CEO was made aware of the incident, but not before Securitas removed him as the company's CEO. It turned out that his identity was first hacked back some months before, at which time it was used to open a personal loan of an undisclosed amount. Four months later, his identity was then used to file for bankruptcy.⁴

In the United States child identity theft is well known but it occurs when a minor's identity is used by another person for the impostor's personal gain. The impostor can be a family member, a friend, or even a stranger who targets children. Medical identity theft is a specific type of identity theft which occurs when a person uses someone else's personal health identifiable

⁴ „Securitas VD och koncernchef Alf Göransson utsatt för stulen identitet och förfalskad konkursansökan”: <https://www.securitas.com/sv/media/regulatoriska-pressemeddelanden/securitas-vd-och-koncernchef-alf-goransson-utsatt-for-stulen-identitet-och-forfalskad-konkursansokan/>

information, such as insurance information, social security number, health care file, or medical records, without the individual's knowledge or consent to obtain medical goods or services, or to submit false claims for medical services.

In a Case from Finland in 2012 thieves broke into a car, and stole a purse with some personal documents. The person was advised to apply to self-block of credit applications in a bank, however, the block was active only for two years. Soon after the two year period the woman noticed that there were loans granted on her name, the largest was 10.000 Euro. Further, someone used her identity to sign into a maternity hospital, and she didn't find out until eventually child protection officers came to visit her in order to question and enquire her about her child (which she did not have). So, someone used her personal documents to give birth in a hospital.⁵

It is also known that identity theft doesn't even stop after death. A thief may use a deceased person's details to drain accounts, set up new loans or steal government benefits. The latest form of identity theft is what we can call social media identity theft that happens when a person's name or likeness is either imitated or hijacked online. This can be the result of someone hacking into another person's accounts or someone creating duplicate accounts which claims to belong to someone else. When compared to other types of identity theft this might seem to be more innocent than the others, but this type of identity theft can have really serious consequences for the person whose account is stolen from.

In a case from Iceland a guy used another guys profile to create a snapchat profile in order to get in contact with a girl. He already knew the girl but she wasn't interested in him so in order to be able to have physical relations with her he decided to pretend to be someone else. He ended up meeting with her twice and convinced her to wear a blindfold during their meetings. He was prosecuted for raping the girl by using her deception that he was indeed another guy.⁶

⁵ „Identiteettivarkaus pilasi elämän – tuntematon nainen synnytti Ninan nimissä:<https://www.iltalehti.fi/uutiset/a/2016061421723382>

⁶ „District Court of Reykjanes case no. S-299/2018“ <https://www.heradsdomstolar.is/domar/domur/?id=5de11c79-1783-455c-b751-e8395ad4b3d9>

However because Iceland does not have a specific law concerning identity theft, the guy who owned the profile, could not get any compensation and the thief was not prosecuted for stealing his identity.

In another case from Norway in april 2019, a girl woke up in the middle of the night, when a guy rang her doorbell. He had been in contact with someone on Tinder who pretended to be the girl. The person who stole the girl's Tinder profile claimed she wanted to meet the guy and invited him to her address in the middle of the night.⁷

As the aforementioned cases reveal identity theft has direct consequences for the individual whose identity is stolen. There may be longer-term indirect consequences including the loss of trust that may occur as a result of abuse of identity infrastructures and the increased costs that may be passed onto consumers and citizens as a result of public and private sector organisations having to invest more in possibilities to secure identity and authentication infrastructures. Direct consequences to the individual include the money that is stolen from them, the amount they have to pay in reconstituting their name, the loss of earnings or lost opportunity cost as a result of damage to reputation caused by becoming an identity theft victim, and time and effort spent in taking restorative action. Victims might also suffer opprobrium from being mistakenly associated with crimes where their identity was used for example, illegal immigration or terrorism. This might be exacerbated by false imprisonment and other consequences of not being able to clear their name.⁸ According to this, it is important that countries try to eradicate identity theft through legislations or by other means.

⁷ „Martines ID ble misbrukt på Tinder – fikk fremmed mann med kondomer på døra“ https://www.nrk.no/norge/martines-id-ble-misbrukt-pa-tinder-_fikk-fremmed-mann-med-kondomer-pa-dora-1.14538693

⁸ „Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crima: Final Report 2011“ https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/rand_study_tr-982-ec_en.pdf

Definitions and legislations

There is no international definition for identity theft but some public institutes have their own definitions about the concept. The OECD definition is that: *“Identity theft occurs when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes.”*⁹

The European Commission uses the same definition as CIFAS (The UK’s Fraud Prevention Center), they state that: *“Identity theft (also known as impersonation fraud) is the misappropriation of the identity (such as the name, date of birth, current address or previous addresses) of another person, without their knowledge or consent. These identity details are then used to obtain goods and services in that person’s name.”*¹⁰ Some countries view identity theft as a specific crime, while others regard it as a preparatory step in the commission of other wrongs or crimes. Whether it should be treated as a standalone offence and criminalized needs to be considered. The lack of a common definition may however complicate efforts to combat Identity theft across borders.

One of the first countries to set a legislation regarding identity theft was The United States of America. In 1998 the Congress passed the US Identity Theft and Assumption Deterrence Act into law after identity theft rose dramatically in the 1990’s. The Act states that whoever knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or otherwise promote, carry on, or facilitate any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law. The penalty for identity theft according to the Identity Theft and Assumption Deterrence Act of 1998 is up to 15 years imprisonment and a maximum fine

⁹ Scoping Paper on Online Identity Theft. Ministerial Background Report DSTI/CP(2007)3/FINAL: <http://www.oecd.org/sti/40644196.pdf>

¹⁰ Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crima: Final Report 2011: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/rand_study_tr-982-ec_en.pdf

of \$250.000. In 2004 the Congress passed another law, the Identity Theft Enhancement Act. It was passed after the investigation of the terrorist attacks in 9/11 revealed that six of the nineteen terrorists used fake passports and suddenly identity theft was seen as instrumental in much more serious crime, such as terrorism¹¹. This law presents higher penalties when identity theft is used for significant criminal intent and focuses on the use of identity theft with the severity of the crime. In 2008 the Congress passed the Identity Theft Enforcement and Restitution Act. This law offers better legal redress for victims. Identity theft can be up for federal prosecution even though the victim and defendant are in the same state¹².

Since 2008 NorSIS¹³ (Norwegian center for the protection on information) has been running a project against identity theft. In 2009 Norway was the first of the Nordic countries to set a special legislation regarding identity theft. In the Criminal Penal Code of Norway (28/2005) with amendment no. 74/2009 in Chapter 21, concerning protection of information and exchange of information, section 202, it is stated that, a penalty of a fine or imprisonment for a term not exceeding two years shall be applied to any person who illicitly gains possession of another person's proof of identity or uses another person's identity or an identity that is easily mistakable for the identity of another person, with intent to: a) make an illicit gain for himself/herself or for another person, or b) cause another person loss or inconvenience. The reason Norway decided to set a special legislation on identity theft was according to Knut Storberget, the former Minister of Justice and the Police, to prevent people from using other person's identity and to enable the police to intervene earlier. He said that it was also very

¹¹ „False identity, federal crime: the Identity Theft and Assumption Deterrence Act“
<https://www.comparitech.com/identity-theft-protection/identity-theft-assumption-deterrence-act/>

¹² „False identity, federal crime: the Identity Theft and Assumption Deterrence Act“
<https://www.comparitech.com/identity-theft-protection/identity-theft-assumption-deterrence-act/>

¹³ NorSIS (Norsk senter for informasjonssikring) was first established as a project in 2002, and after evaluation, founded on February 2, 2010 by request from the Norwegian government.

important to send out the message to those who are using another person's identity that the community sees it as a serious crime to tamper with other person's ID¹⁴.

In 2015 Finland criminalised identity theft. In the Criminal Code of Finland (39/1889) in Chapter 38, concerning Data and communication offences, section 9 (a) it is stated that a person who in order to deceive a third party unlawfully uses the personal information, access codes or other corresponding identifying information of another and in this manner causes economic loss or more than petty impediment to the person to whom the information belongs, shall be sentenced for identity theft to a fine. According to Section 10, paragraph 4, the prosecutor may only bring charges for identity theft if the injured party reports the offence for the bringing of charges.¹⁵ According to Inspector Sami Kalliomaa the legislation clarified the law and filled a gap, especially when it comes to the more recent phenomenons of fake profiles on social media¹⁶. The Office of the Prosecutor General expressed its firm support for the enactment and stated that such mischief might have serious repercussions¹⁷.

One year later, in 2016, Sweden criminalised identity theft with amendment no. 485/2016 on the Criminal Code of Sweden (700/1962). In Chapter 4, concerning crimes against liberty and peace, section 6 (b) it is stated that anyone who illegally uses another person's identity data and pretends to be him or her and thereby causes harm or inconvenience to him or her, is sentenced for unlawful use of identity for fines or imprisonment for a maximum of two years¹⁸.

However Denmark and Iceland do not have any legislation that focuses explicitly on identity theft as a specific crime or that defines such a crime. That means that the identity theft

¹⁴ „Skjerper straffen for ID-tyveri“ <https://www.nrk.no/norge/skjerper-straffen-for-id-tyveri-1.6360390>

¹⁵ The Criminal Code of Finland no. 39/1889, with amendment no. 368/2015.

¹⁶ „Identity theft on the rise“ https://yle.fi/uutiset/osasto/news/identity_theft_on_the_rise/9126220

¹⁷ „Finland to criminalise identity theft“ <http://www.helsinki.fi/finland/finland-news/domestic/10488-finland-to-criminalise-identity-theft.html>

¹⁸ Translation to English from authors. The Swedish provision is; „*Den som genom att olovligen använda en annan persons identitetsuppgifter utger sig för att vara honom eller henne och därigenom ger upphov till skada eller olägenhet för honom eller henne, döms för olovlig identitetsanvändning till böter eller fängelse i högst två år*”

itself is not criminalised and it has to be a part of a bigger crime, such as e.g. fraud, theft or forgery in order for the victim to be able to file a complaint to the police.

Comparison of the legislation in Norway, Finland and Sweden

When the legislation in Norway, Finland and Sweden is compared it is obvious that identity theft is a crime that is frowned upon. All three countries have made it a part of their Penal Code. However it is interesting that it varies where they place the provisions within their Penal Codes. In Norway it is in a chapter concerning protection of information and exchange of information, in Finland it is in a chapter concerning data and communication offences and in Sweden it is in a chapter concerning crimes against liberty and peace. These three different chapters protect various aspects of people's rights and liberty. The question is whether it matters where the provision is placed in order for the injured party to seek its rights? It is possible that the utilization of the provision is limited if it is placed in certain chapters of the Penal Code. For example a provision that is placed in a chapter concerning enrichment violation cannot be used against a crime that has no intent for financial gain. Identity theft is a crime that has many various forms and often seems to have no special intent other than to use someone's else's identity. It can be nothing more than to make a fake profile on social media in the name of someone else. The intention may not involve any financial gain, any deception against a third party, but more the intention of making a little bit of inconvenience to the injured party. It seems, in order for the provision to protect the injured party rights in no matter the form of the identity theft, that the Swedish legislation, and where they place the provision, includes the most protection for the injured party. The identity theft can occur online, it can occur offline, it does not have to involve any financial gain or financial loss for the injured party. Simply the act of using someone's identity that gives rise to injury or inconvenience for the injured party is a crime.

In both Norway and Sweden the penalty for identity theft is a fine or up to a two year imprisonment. However in Finland the penalty is only a fine. Finland seems to have restricted the possibility to charge someone for identity theft within their legislation. In their legislation it is a condition that a third party was deceived and the bringing of charges is subject to a report of the offence from the injured party. The provisions in the Norwegian and Swedish legislations seem to be more open and not subject to any restrictions.

Conclusion

After reviewing what is identity theft, the many faces of its appearance and how the intention behind it can vary it is our conclusion that there is a real need for addressing those crimes with a specific legislation.

Identity theft is a very personal crime that can have severe consequences for the victim, not only direct consequences such as financial but also very emotional consequences. To steal a person's identity and use it in a manner the person would not be making the person very vulnerable. The identity is one of the most sacred things a person has and can easily be completely ruined.

However a legislation regarding identity theft has to be thought carefully. It is our opinion that in order to give identity the protection it needs by law the legislation needs to be open enough to conclude any kinds of mischief on a person's identity. It should not be restricted to any certain methods, any specific gain or an involvement or a deception of a third party. It is clear to us that the specific legislation in Norway, Sweden and Finland has proven its point, even though the legislation varies between those three countries. It is our further opinion that Iceland and Denmark should seriously consider to set a specific legislation regarding identity theft. After all, the fact is that especially in the most recent years when a large amount of people puts their personal information, photos and live events on social media identity theft can easily be perpetrated and is a growing and glooming business in the world.

References

Mcintosh, Victoria: *False identity, federal crime: the Identity Theft and Assumption Deterrence Act*

<https://www.comparitech.com/identity-theft-protection/identity-theft-assumption-deterrence-act/> - Published December 24, 2018.

Kumano-Ensby, Anne and Omland, Ellen: *Skjerper straffen for ID-tyveri*
<https://www.nrk.no/norge/skjerper-straffen-for-id-tyveri-1.6360390> - Published December 8, 2008.

Identity theft on the rise

https://yle.fi/uutiset/osasto/news/identity_theft_on_the_rise/9126220 - Published August 28, 2016.

Reinboth, Susanna: *Finland to criminalise identity theft*

<http://www.helsinkitimes.fi/finland/finland-news/domestic/10488-finland-to-criminalise-identity-theft.html> Published May 8, 2014.

OECD: *Scoping Paper on Online Identity Theft. Ministerial Background Report DSTI/CP(2007)3/FINAL*: <http://www.oecd.org/sti/40644196.pdf> Published 2008.

Securitas VD och koncernchef Alf Göransson utsatt för stulen identitet och förfalskad konkursansökan:

<https://www.securitas.com/sv/media/regulatoriska-pressmeddelanden/securitas-vd-och-koncernchef-alf-goransson-utsatt-for-stulen-identitet-och-forfalskad-konkursansokan/>
Published July 12, 2017.

Egutkina, Anna: *Identiteettivarkaus pilasi elämän – tuntematon nainen synnytti Ninan nimissä:*
<https://www.iltalehti.fi/uutiset/a/2016061421723382> Published June 14, 2016.

Ording, Oda and Tinmannsvik, Ingrid: *Martines ID ble misbrukt på Tinder – fikk fremmed mann med kondomer på døra:* <https://www.nrk.no/norge/martines-id-ble-misbrukt-pa-tinder--fikk-fremmed-mann-med-kondomer-pa-dora-1.14538693> Published May 5, 2019.

Robinson, Neil, Graux, Hans, Parrilli, Davide Maria, Klautzer, Lisa and Valeri Lorenzo: *Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crima: Final Report 2011*

https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e_library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/rand_study_tr-982-ec_en.pdf
Published June, 2011.

District Court of Reykjaness case no. S-299/2018 of May 21, 2019:

<https://www.heradsdomstolar.is/domar/domur/?id=5de11c79-1783-455c-b751-e8395ad4b3d9>