Identity-Theft Through e-Government Services – Government to Pay the Bill?

Jessica Schroers, Pagona Tsormpatzoudi

Identity-theft through e-Government services – Government to pay the bill?

Jessica Schroers[1], Pagona Tsormpatzoudi[1],

K.U. Leuven – Interdisciplinary Centre for Law & ICT – iMinds, Leuven, Belgium

{jessica.schroers, pagona.tsormpatzoudi}
@law.kuleuven.be

Abstract. The expansion of e-Government and online authentication possibilities in recent years increases the risk of not properly implemented authentication systems. This may often give rise to subsequent risks, such as identity theft. Whereas the legal framework has primarily focused on identity theft as a criminal act, less attention has been given to the way the Government handles information in its identity management systems. This paper considers traditional theories of European extra-contractual liability/tort law to assess whether the Government can be liable for failures in the authentication procedure.

1 Introduction

In the digital age, strong online authentication is an important step in fostering online services with a higher risk but also higher value (OECD, 2011). With that in mind, different states have developed their own national eID systems through which citizens can access e-Government services on the basis of secure citizen authentication. This has opened the stage for a new era in citizens' interaction with governments. Transactions on a government's portal are often inherently related to the official identity of a person and involve personal data. In that sense, simple online activities, such as access to portals and modifications of personal details may entail significant risks to citizens' identity information. One of such risks which is rapidly growing and affects

adfa, p. 1, 2011.

all types of stakeholders, including governments and citizens, is the phenomenon of identity theft (European Commission, 2004). Identity theft is described as any unlawful activity where the identity of another person is used as a target or principal tool without that person's consent (Koops & Leenes, 2006). The harmful consequences of identity theft do not end with the compromise of one's identity but rather often lead to financial loss. For instance, in case a thief replaces the bank details of an account holder with his own on a web-tax portal, the person entitled to the tax return will not receive it.

The risk of identity theft can appear as a result of faulty online authentication and may lead to potential liability risks for all participants in the Identity Management ("IdM") system, including the government as a relying party[1]. Furthermore, a denial for access to e-Government services or unauthorised access to personal files may be some of the harmful consequences. In order to prevent such consequences, there is a need to enhance the privacy and security of citizens' identity information and ensure that all participants perform their obligations properly (Smedinghoff, 2012).

This paper examines the potential civil liability of the government for failures in e-Government authentication systems resulting in identity theft. Departing from the general notions of e-Government (Section 2), section 3 describes the way the European extra-contractual liability/tort law could create liability of public services providing e-Government services. Namely the paper first studies the three most common elements that need to be fulfilled in order to establish liability: fault, damage, causation (Sub-sections 3.2, 3.3, 3.4). In addition, it illustrates whether each of these elements can be applied to establish liability in case of identity theft caused by failures in e-Government authentication systems.

2 The rise of e-Government

The use of ICT in administration is not new and has been present for quite some time. Nevertheless, it significantly expanded in the last couple of years and the notion of 'e-Government' has become "one of the topics most frequently debated in administration". (Schedler & Summermatter, 2003) As per van der Meer et al., e-Government could be generally understood as

> "the major initiatives of management and delivery of information and public services taken by all levels of government […] on behalf of citizens, business, involving using multi-ways of internet, website, system integration, and interoperability, to enhance the services (information, communication,

[1] Typically participants in an IdM system are: i.User ii.Identity Provider (party providing identity assertion on the user) iii.Relying Party (the party relying on the identity assertion provided by the Identity Provider).

policy making), quality and security, and as a new key (main, important) strategy or approach."[2]

Even though e-Government covers an extensive range of services and technologies, the scope of this paper covers the provision of public services using electronic authentication (i.e., e-Government services) which is growing at a fast pace. One factor fostering the use of e-Government services are legal and policy developments at both the European and national level. An example at the European level is Article 6 of the Directive 2006/123/EC which requires Member States to establish 'Points of Single Contact' (PSCs) in order to simplify procedures and formalities relating to access to a service activity. The Directive provides that all procedures and formalities "may be easily completed, at a distance and by electronic means"(Article 8). This entails the provision of the service online, and often necessitates electronic authentication. At the national level, an example can be found in § 2 of the German e-Government law[3], which requires every federal authority in Germany to provide the possibility to use the eID in administrative procedures when identification of a citizen is required by law or necessary for other reasons.

2.1 The government as relying party

The increase of e-Government services necessitates ways to authenticate the citizen in order to ensure that the person authenticating online, accessing the service and eventually receiving the benefit, is indeed the eligible person. Traditionally, citizens had to go to the public authority in order to authenticate and use a public service, or at least send a personally signed document in paper (e.g., the application for a new ID card or filing a tax return form). In e-Government this can be done electronically and at a distance. However, such an electronic action requires reliable electronic authentications. As a result, different states have developed their own national eID systems through which citizens can authenticate themselves to use e-Government services.

These systems are often linked to the national ID card of the country, such as in Germany (i.e. the nPA) or in Belgium (i.e. the eID). Other national eID systems may differ, such as the Austrian 'Citizen Card' (Bürgerkarte), which is a logical unit that can be integrated on different tokens (e.g. a smart card or cell phone)[4]. The national eID systems can vary extensively, but often the current systems use certificates and

---

[2] T. van der Meer, D. Gelders, S. Rothier, "E-Democracy: Exploring the current stage of e-Government", Journal of Information Policy 4 (2014), p. 489; referring to: Guanwei Hu, Wenwen Pan, Mingzin Lu and Jie Wang, "The Widely Shared Definition of E-Government. An Exploratory Study.", The Electronic Library 27 (2009): 979.

[3] Entered into force on the 1st of January 2015; § 2 (3) Gesetz zur Förderung der elektronischen Verwaltung (E-Government Gesetz – EGovG) from 25.7.2013 (BGBl. I S. 2749) ('EGovG').

[4] E. Schweighofer, W. Hötzendorfer, "Electronic identities – public or private", International Review of Law, Computers & Technology, 27:1-2, 230-239, 2013, p. 233. In case of a 'handy signature', the authentication with a cell phone the secure signing module is on a special server.

require the relying party to integrate specific software or hardware for the authentication system. Implementation of authentication systems in e-Government services not only takes place in large scale systems (for example for purposes of tax administration), but also by small scale regional e-Government public services.

In the future, local government services which generally operate on a smaller scale and might not have the necessary IT know-how will need to be able to accept different types of eIDs and keep the information secure. This obligation results from the new eIDAS Regulation (No 910/2014) of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC**.** The Regulation introduces obligations for mutual recognition of electronic identity means in order to facilitate cross border authentication and improvement of the availability of interoperable e-Government services in the EU (Recital 6). The Regulation ensures that Member States also have to accept eID means of notified eID schemes of other countries for access to their own public services, if they require their national eID means for access (Article 6).

Considering that public services often have neither extensive IT resources/knowledge nor much funding to implement systems able to accept foreign eIDs, the obligation to accept notified foreign eIDs might result in poorly implemented authentication systems and a reduced security level. Although the eIDAS Regulation includes provisions on liability, it only entails liability for (1) the Member State, (2) the issuing party and (3) the operating party of the eID systems, yet not for the relying party (i.e. the government in this case). Therefore traditional approaches to extra-contractual liability/ tort law and laws entailing certain obligations for the relying party may form the basis of liability for failures attributed to the relying party.

3 Liability of Government as Relying Party

In most cases e-Government services are provided by public services, which may in principle be held liable under specific provisions on the liability of public services as well as general extra-contractual liability or tort law. This section analyses how the latter may be applied in case of poorly implemented authentication systems which resulted in identity theft.

3.1 Extra-contractual or Tort Law liability in Europe

Civil or tort law liability has developed in different ways across Europe. European legal traditions have adopted various approaches vis-à-vis the concept of extra-contractual liability or tort law. Terminology has varied accordingly. In civil law traditions, extra-contractual liability is derived from an unlawful conduct which causes damage, whereas in common law this notions is referred to as "tort". According to Van Dam, '*European extra-contractual liability law excluding agency without au-*

thority and unjust enrichment' might be a more accurate description, however, it has become common to use the word tort in English academic writing (Van Dam, 2013). For the purposes of this paper, we will use the the term "tort" as a general term.

Tort liability has different functions. The main one is generally the restitutory function, i.e. the duty to indemnify the damage caused, which can be assigned to the person who commits a tort (i.e. the tortfeasor) (Dimitrov, 2007). In certain legal systems civil liability also has other functions, such as a punitive function. In this case the objective is to punish the tortfeasor for the negligent non-performance of his/her duties, in order to discourage future negligent behaviour (Dimitrov, 2007). In this regard, it is important to assess whether a relying party can be liable under tort law for faulty online authentication and whether potential liability might provide incentives to increase security.

In order to derive liability from tort in Europe, there are certain elements that have been generally accepted as relevant despite the fact that there is no generally applicable European law:

1. Most countries base tort liability on the principle of **fault**. Fault liability refers to liability for intentional as well as negligent conduct (Van Dam, 2013). However, nearly all systems also have some categories of tort liability that are not based on fault, usually a form of strict liability (Widmer, 2005). Strict liability implies that someone is liable regardless of whether he acted intentionally or negligently (Van Dam, 2013).
2. Another requirement for liability is **damage**. Damage refers to the harm one suffers.
3. A final requirement is that there should be a **causal connection** between the damage and the harmful behaviour (causation).

3.2 Fault

Requirements to prove fault may differ in various countries. For example in France, liability is established when the requirement of fault (faute) stemming from negligent conduct is fulfilled. In England, however, this would not be sufficient, as two requirements need to be fulfilled to establish fault: duty of care and breach of duty. In Germany, there are even three requirements: the violation of a codified normative rule (Tatbestand), unlawfulness (Rechtswidrigkeit) and intention or negligence (Verschulden) (Van Dam, 2013). Aside from the differences, the common denominator amongst these cases is the basic requirement for fault liability, namely intentional or negligent conduct (Van Dam, 2013). English and German law do contain additional requirements which mean that not every type of misconduct is sufficient for liability (Van Dam, 2013).

It is difficult to define fault in a universal way, since its building blocks vary in different countries. Additionally, the way it is interpreted has changed overtime from a more subjective approach to a more objective one. The subjective fault approach considers the individual qualities of the tortfeasor, while the objective fault approach considers the behavior itself (Widmer, 2005). Since it is difficult for the judge to

evaluate the personal qualities of the tortfeasor, the definition changed towards a more objective standard. Therefore, at the moment, the majority of European countries use the objective standard, frequently presented as the famous 'bonus pater familias'. The 'bonus pater familias' is a model of an average person, "not exceptionally gifted, careful or developed, neither underdeveloped nor someone who recklessly takes chances or who has no prudence" (Widmer, 2005). For some countries the concept can be adapted to the personal circumstances or time and place ('reasonable surgeon', 'careful barkeeper') (Widmer, 2005) and for specialists generally a higher 'due care' is evaluated according to their above average capacities. The behaviour of the tortfeasor is then measured against this standard. If the behaviour does not comply with this standard and the tortfeasor did not act with due care, the fault criterion is fulfilled.

Other factors that form part of the fault assessment can be, for example, foreseeability (Widmer, 2005). In Germany, the foreseeability of the damage-producing situation and preventability of the damage are considered a factor of fault, since "if a certain situation or damage never occurred before, it might have been impossible for the tortfeasor to anticipate its emergence" (Widmer, 2005). Another factor can be conformity or lack of conformity with prescriptions, technical or deontological norms (Widmer, 2005). This conformity or lack of conformity can serve as a yardstick for the assessment of fault.

Fault of the government as relying party. This section examines on what conditions a conduct of an e-Government service can constitute a fault if the authentication service has not been properly implemented. An example of a faulty implementation could be a system that does not perform a necessary check of a (certificate) revocation list. In this case the risk arises that an unauthorised person gets access to the service with a stolen eID, even if the owner of the eID has reported the eID theft and blocked the eID.

Another example could be when a system for the provision of a public service does not adequately check whether the user requesting the service is actually entitled to do this. This happened in the Netherlands, where identity theft and fraud cases took place when the tax authority allowed to make requests in the name of someone else. Since no adequate checks were put in place, unauthorised users could make requests through the Dutch eID system in the name of other persons, to receive benefits on their own bank account.[5] As possible under the Dutch social system, the tax administration requested the money back from the beneficiaries.[6] In a relevant court case, the court decided that since the official beneficiaries never received the benefit, the tax administration could not request benefit return from them.[7] It also underlined that

[5] See e.g. RvS 201202458/1/A2 en 201202462/1/A2, with noot of Prof. G. Overkleeft-Verburg, Jurisprudentie Bestuursrecht 2013 – 125; RvS 201400357/1/A2; Rechtbank Midden-Nederland, 16-994253-13.

[6] In the Netherlands, a specific system of benefits exists, in which case the benefits will first be disbursed, and later be checked if the person was entitled to receive it, and in case not, the benefits need to be returned.

[7] See RvS 201202458/1/A2 noot 5.3.

since unlawful activity with the DigiD system was possible and had happened before, the tax administration should have checked the bank accounts to which the money was transferred. Additionally, the court stated that the tax administration was not able to discover whether the beneficiary possessed a DigiD (the Dutch eID) or with the use of whose DigiD the request had been placed.[8] In this case the court decided that the request could not be attributed with sufficient certainty to the official beneficiary, however, in similar other cases it was attributed and the beneficiaries had to pay the benefit back.

This shows that a general problem to establish liability remains the challenge to notice failures and to identify and prove one's fault. In this regard logging or specific accountability mechanisms might be helpful. However, if the relying party logs the actions, it would still be necessary that these logs are tamper proof and possibly time stamped, in order to be usable as evidence. An additional difficulty might be the fact that the user might not be able to obtain the information of the logs, as they are in the hands of the relying party. Furthermore, the recognition of failures could often appear on the relying party's side, which is in a better position to recognise if the system does not work/has not been implemented adequately. However; considering that a part of the system might be the responsibility of the IdP, in case failures appear on the IdP's side, it might be more difficult for the relying party to prove the failure.

Independent from the problem of recognising failures, for establishing fault one should examine what can be expected from a public service providing an e-Government service, and whether this was fulfilled or not. In this regard laws and generally accepted standards can be useful. Laws and standards describe the 'duty' of the public services and their employees. Breaching such duties may hold them liable under tort law.

An example of such a law is the main provision with regard to tort liability §823 of the German Civil Code 'Bürgerliches Gesetzbuch' ('BGB'). For liability based on this provision, it is either necessary that an absolute right has been infringed, which in case of identity theft could be a misuse of the identity or rather the name of the identity owner, which is considered an absolute right according to §12 BGB (Borges, 2010, p. 182). Or a "protective law" needs to have been infringed. "Protective law" in the German legal system is a law which protects a person; according to the legislator's incentives, such a law in its substance serves protection of an individual against a defined type of damage (BGH Urteil, 1982). For instance when government tortious behaviour leads to an unauthorised access to data which may be related to identity theft, such a protective law could be § 9 of the German federal data protection law, 'Bundesdatenschutzgesetz' (BDSG). This clause requires the relying party to take the necessary technical and organisational measures to ensure the implementation of the provisions of the data protection act, ensuring especially the security of the data (Borges, 2010, p. 199).

[8] RvS, 201202458/1/A2 en 201202462/1/A2, 2.4.2013, Rn. 5.3.

Data protection liability. The above example shows that laws can provide the basis of tort liability. However, laws often provide liability clauses themselves. An example of a law providing a basis for potential liability for the government as a relying party in case of unauthorised transmission of data is the Data Protection Directive 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 and on the free movement of such data (1995/46/EC). Article 23 para 1 and Recital 55 of the Data Protection Directive provide that any person who has suffered damage as a result of an unlawful processing operation is entitled to receive compensation from the controller for the damage suffered. Such damage may occur to the actual identity owner in the case of unauthorised access to his/her data in a governmental portal without his/her consent. In such a case the relying party acting as a data controller had the responsibility to implement appropriate technical and organisational measures to protect the actual identity owner from identity theft (Article 17).

The data controller is in principle liable for the damage caused to citizens when data processing is not compatible with data protection law. In that sense, the lack of technical and organisational measures and in general the way data has been treated has led to wrong online authentication and possibly to identity theft. Article 23 paragraph 2 states that the controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage. As Huysmans explains, the mentioned article is an "objective" liability provision, because there is no need to prove the fault of the data controller to hold him/her accountable for a certain action: the mere fact that he/she infringed the data protection law leads to liability, of course only if there is a causal link between the damages and this infringement of the law (Huysmans, 2008)

All Member States have implemented this provision in their national legislation, often using identical or similar terms (Korff, 2002). For instance, in Germany § 7 and § 8 BDSG provide for liability of breaches of the German federal data protection law, whereby §8 BDSG provides a liability for public services in case of automated data processing. Yet, the General Data Protection Regulation to be adopted by the European Parliament in 2016 and to enter into force in 2018 (Council of the European Union, 15 December 2015), having a direct application in all Member States may lead to further harmonization of the handling of liability issues with respect to data protection. The regulation provides a detailed regime for liability issues stemming from data protection law infringements in Chapter VIII and in particular underlines that both material or immaterial damage suffered by the data subject grant her the right to receive compensation from the controller or processor (Article 77).

3.3 Damage

Most Member States do not include a definition of damage in their legislation. An exception is Austria, which has a statutory definition (§1293 Austrian Code: "Damage is called every detriment which was inflicted on someone's property, rights or person.

This is distinguished from the loss of profit which someone has to expect in the usual course of events") (Magnus, 2001). Even though it may start from a 'natural' meaning of damage, damage is a legal concept and only that damage which can be recovered is damage in the eyes of the law (Magnus, 2001). Courts and scholarly writing provide definitions in other countries, for instance in Germany 'any loss that somebody suffered with respect to his legally protected rights, goods and interests', in Italy 'a detriment capable to be evaluated from an economic standpoint' and in the Netherlands 'factual detriment arising from a certain occurrence' (Magnus, 2001). All attempts agree that they presuppose a negative change (attributable to the wrongdoer) which must have taken place in the legally protected sphere of the injured party (Widmer, 2005). In order to judge whether a change is negative, the judge will draw a comparison between two states of affairs (the "Differenzhypothese") (Magnus, 2001). However, the outcome depends on the positions which are included in the comparison and which worth is attributed to them. Therefore the comparison is a method of assessing damages, but it does not in itself decide what constitutes recoverable damage (Magnus, 2001).

Damage in the case of e-Government. Smedinghoff (Smedinghoff, 2012) has observed several consequences resulting from failed authentication. First, the government as relying party and/or citizens may suffer damages when the former either acts in reliance on a false credential or assertion which they considered as valid (e.g., by granting unauthorized access or allowing transaction), or fails to act in reliance on a valid credential that it mistakenly believes to be false. Second, citizens may suffer damages when either their personal information is misused or compromised or, when they are improperly denied access or are unable to conduct a transaction they are otherwise entitled to.

In sum, damages mainly occur at the side of the relying party/government and/or the citizens. As illustrated in the previous section, the scope of these damages depends upon the specific situation and is subject to the discretion of the judge.

It is unlikely that the government providing the e-Government service would request compensation in case it suffers damage from its own negligent behaviour. On its turn this may result in two possible consequences. On one hand, the damage itself would be high enough to provide an incentive to increase security, which ensures no repetition of the resulted damage. On the other hand, the service would accept the damage since the costs related for example to increased security or better organisation might be higher than the damage. A court proceeding will in this case not be initiated.

With regards to the citizen, tort law provides a possibility to indemnify the citizen for the damage suffered. In case of denial of access, the damage would be difficult to prove, as the purpose of e-Government services is to provide an alternative to contacting the public services through traditional channels. As long as these traditional alternatives are available, the only harm caused is reduced convenience, which may not qualify as a damage in the sense of recoverable negative change as presented above.

Consequently, the most prevalent case of damage which might occur to a citizen would result from granting access (and allowing transactions) to unauthorised persons. This will be further explained in the next section.

Damage in the case of identity theft?. A lack of secure online authentication systems may have detrimental consequences, since unauthorised access and information misuse may cause a domino of further risks. As described above, identity theft is a risk that has gained momentum in recent years and entails severe consequences for governments and citizens. (European Commission, 2004). But its consequences do not end when it has been completed as in the aftermath of identity theft additional risks may occur. Identity theft may be part of a conspiracy to commit other crimes, an aggravating circumstance in other crimes or it may be included in other forms of crime such as fraud, forgery, computer crimes, counterfeiting (European Commission, 2004). For instance, if someone (with or without stolen credentials) accesses personal data in an e-Government portal because of poorly implemented authentication in an e-Government portal, this may subsequently lead to tax fraud. Tax fraud involves circumstances where an identity thief receives money from the government to which he is not entitled (McKee & McKee, 2011)**,** as in the case of DigiD in the Netherlands as described above.

Overall, it is difficult to assess and prove recoverable damage in case of stolen personal data. There is often a gap between the real damage and what can be claimed as damages. For example, the largest costs of identity theft arguably is the time lost due to administrative procedures amongst others, and not the money stolen per se. A recent study showed that victims in the US spend on average $1400 to clear up an identity theft crime, but also spend on average 600 hours. Further, it takes up to 10 years to clear up the crime with creditors (Demby, 2005). Victims are often faced with increased insurance, credit card fees and similar costs.

In general only direct pecuniary losses, i.e. measurable financial losses are typically considered damage. In this regard a recent UK case provides a change of the current understanding of damage in the UK Data Protection Act (Vidal-Hall & Ors v Google, 2015). This is interesting, since, as previously explained, data protection legislation includes provisions regarding security, whose breach could give rise to liability. In the UK Data Protection Act damage was considered pecuniary loss, and only distress was not acceptable for compensation except for certain specific cases. However, in Vidal-Hall & Ors v Google the court ruled that misuse of private information, which cannot be considered as pecuniary loss as such, is a tort. The judges concluded that article 23 Directive 95/46/EC has a wide meaning, including both material and non-material damage. As the definition of damage in the UK act only referred to material damage, the judges ruled that the definition of damage in the UK act is not in line with the European Data Protection Directive 95/46/EC.

3.4 Causation

In order to establish liability for a certain damage there needs to exist a causal link between the liable person/entity and the damage. To establish such causality the different legal systems have developed similar tests. Most legal systems consider conditio sine qua non as a first test. Only in Belgium conditio sine qua non is the sole requirement to be established and officially rejects the two step-approach which other

jurisdictions take as a theoretical framework (Spier & Haazen, 2000). Conditio sine qua non means that in order to determine whether an act or omission was a cause of the loss, consider whether the loss would still appear if the act or omission was eliminated. If the loss does not occur, the act or omission was not causal for the loss, if it does, the loss has been caused by the act or omission (Spier & Haazen, 2000).

The second step can vary in the different legal systems. Common law considers the 'proximate cause', which includes proximity in time and space, foreseeability of the harm and other factors (Spier & Haazen, 2000). Other countries such as France, Germany, Greece and Austria use the test of adequate causation (Spier & Haazen, 2000). In this regard the degree of probability is decisive. For example in Austria, adequacy is established if the damaging event was to a considerable extent generally suitable for increasing the possibility of such a damage as in fact occurred (Spier & Haazen, 2000).

Causation between e-Government fault and identity theft. It should be noted that vulnerabilities in the governments' authentication systems are not created by the identity thief; but rather, as Solove points out, exploited by him (Solove, 2003). Unauthorised access to personal files is then a result of an inadequately protected architecture with flawed security safeguards and limited degree of participation on the citizen in the collection, dissemination, and use of personal data. This is something that the traditional approaches to identity theft focusing on it from a criminal law perspective fail to capture; identity theft which occurred as a result of vulnerabilities in an information system forms part of a larger problem regarding the way our personal information is handled (Solove, 2003). Even the term of "identity theft" views it as an instance of crime - a "theft" rather than as the product of inadequate security (Solove, 2003). This is why to counter the risks of identity theft, amongst other, particular attention should be paid to the development and deployment of secure identity management systems (Meulen, 2006).

Useful for the claimant with regard to her awareness of security breaches could be the notification obligation in the proposed Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The choice to introduce a general obligation for data controllers to notify personal data breaches (Article 31) (Council of the European Union) is in line with the proposal for a NIS Directive and may be an element to help the claimant establishing the causal link.

In order to establish causation, it has to be assessed whether the identity theft still could have taken place without the failure of the e-Government service. If it can be established that the identity theft could not have taken place without the failure, the e-Government service might be held liable for its failure.

4 Conclusion

The paper has demonstrated that bringing claims to court in cases of identity theft due to a failure of authentication in e-Government services could be complex. Difficulties relate to all the three elements that need to be fulfilled in order to establish liability

from tort law. Firstly, with regard to the fault criterion, victims might not be aware that the relying party was at fault or find it difficult to prove that the relying party was at fault. Secondly, with regards to causation, it might be hard to prove that the identity theft resulted from a failure of the relying party. Finally, proving damages would often be a problem, especially in case of misuse of data without obvious pecuniary loss. The difficulties explain why the amount of court cases so far has remained limited.

However, this might change in the future. As described, the amount of e-Government services is increasing, and with them the opportunities for identity thieves to use them for fraudulent acts. Additionally, the implementation of various software might, if not conducted properly, in the frame of adhering to the provisions of the eIDAS Regulation, provide security lacunas, which can be used by identity thieves. This might result in rising numbers of identity theft in the future.

Also the reluctance of citizens to sue the government might reduce in time. Considering that the UK court recently ruled that pecuniary damage is not necessary for a tort claim for breach of the data protection act, privacy advocates already foresee a rising amount of claims based on breaches of the data protection act.[9] Data protection law may also provide a legal basis for liability in case of failures of security of authentication for e-Government services.

Since it will be in future easier for data subjects to become aware of security breaches (because of breach notification obligations), they might be encouraged to bring claims based on a breach of data protection law. In turn, this may lead to an increased risk of liability for the relying party.

In any case, relying parties will need to be able to document and proof that they adhered to the state of the art security standards. This might not completely avert security breaches, but at least will make them more difficult. The increased liability risk stemming from tort law could therefore exert pressure to public services to improve the security of their e-Government systems.

5 Acknowledgments

This paper was made possible by the funding of the project FutureID (Shaping the future of electronic identity), EU FP7, under the Grant Agreement n° 318424and the project EKSISTENZ (Harmonized framework allowing a sustainable and robust identity for European Citizens), EU FP7, under the Grant Agreement n° 607049.

[9] See e.g. Jon Baines, http://informationrightsandwrongs.com/2015/03/27/vidal-hall-v-google-and-the-rise-of-data-protection-ambulance-chasing/

References

1. Belanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems*, 165-176.
2. BGH Urteil, VI ZR 33/81 (BGH 6 29, 1982).
3. Borges, G. (2010). *Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis - Ein Gutachten für das Bundesministerium des Innern.* http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/PaesseAusweise/rechtsfragen_npa.html.
4. Council of the European Union. (15 December 2015). *Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data - Analysis of the final compromise text with a view to agreement.* Presidency to Permanent Representatives Committee. Availlable at http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf.
5. Council of the European Union. (19 December 2014). *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).*
6. Demby, E. (2005). Identity Theft Insurance - Is it worthwile? *Collections&Credit Risk*, 10-11.
7. Dimitrov, G. (2007). *Liability of Certification Service Providers, PhD.* Leuven: KU Leuven.
8. European Commission. (2004). *A New EU Action Plan 2004-2007 to Prevent Fraud on Non-cash Means of Payment. COM (2004) 679 final, 20.10.2004.* . Brussels.
9. European Commission. (2004). *Minutes of the Forum on Identity Theft.*
10. European Commission. (2013). *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union /* COM/2013/048 final - 2013/0027 (COD) */* .
11. Huysmans, X. (2008). Privacy-friendly Identity Management in eGovernment. In S. F. Hubner, P. Duquenoy, A. Zuccato, & L. Martucci, *The Future of Identity in the Information Society: Proceedings of the Third IFIP WP9.2, 9.6/11.6, 11.7 FIDIS Summer School on the Future of Identity in the Information Society.* Springer.
12. Koops, B.-J., & Leenes, R. (2006). Identity Theft, Identity Fraud and/or Identity Related Crime. *Datenschutz und Datensicherheit* , 553-556.
13. Korff, D. (2002). *EC Study on Implementation of Data Protection Directive - comparative summary of national laws.* Cambridge.
14. Magnus, U. (2001). *Unification of Tort Law: Damages.* Kluwer.
15. McKee, T., & McKee, L. (2011). Helping Taxpayers Who Are Victims of Identity Theft. *CPA Journal*, 81, 7, 46.
16. Meulen, N. v. (2006). *The Challenge of Countering Identity Theft: Recent Developments in the United States, the United Kingdom, and the European UnionReport Commissioned by the National Infrastructure Cyber Crime program (NICC)* . NICC.
17. OECD. (2011). *OECD report on "Digital Identity Management of Natural Persons: Enabling Innovation and Trust in the Internet Economy".*
18. Schedler, K., & Summermatter, L. (2003). E-Government: What countries do and why: a European perspective. In G. Curtin, M. Sommer, V. Vis-Sommer, & (ed), *The Wolrd of E-Government.* The Haworth Press, Inc.

19. Smedinghoff, T. (2012). Solving the Legal Challenges of Trustworthy Online Identity. *Computer Law and Security Review*, 532-541.
20. Solove, D. (2003). Identity, Privacy and the Architecture of Vulnerability. *Hastings Law Journal*, 1228-1277.
21. Spier, J., & Haazen, O. (2000). Comparative Conclusions on Causation. In J. S. (ed), *Unification of Tort Law: Causation.* Kluwer.
22. Van Dam, C. (2013). *European Tort Law.* Oxford: Oxford University Press.
23. Vidal-Hall & Ors v Google, EWCA Civ 311 (Court of Appeal 2015).
24. Widmer, P. (2005). *Unification of Tort Law: Fault.* The Hague: Kluwer.