The interpretation of '*serious culpable negligence'* in the future fining practices of the Dutch data protection authority and its possible effect on the organization of privacy compliance within organizations.

Tilburg Institute for Law, Technology and Society (TILT)
LL.M. Law and Technology (2015-2016)

Wendy T.N. Tran
ANR: 906834/EMP: 1259997

Thesis Supervisor: Ms. K. La Fors
Second Reader: prof. dr. E.J. Koops
August 2016

Index

Chapter 1 Introduction

1.1 Background

In January 2016 the Dutch Data Protection Act[1] (hereafter: Wbp) went under revision, granting the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, hereafter: AP) a broader competency to fine organizations for the violation of specific provisions of the Wbp[2]. Prior to the expansion of its fining competency the AP could only impose an administrative fine for the violation of administrative requirements as laid down in the Wbp, such as for non registration of data processing. After revision, the AP is able to impose fines for the violation of general obligations and standards as well, for example once it has established that personal data is stored for a longer period than necessary.[3] The AP published policy guidelines for its fining competency regarding violations of the Wbp (hereafter: Fining Policy of the AP)[4]. In these guidelines, the AP explains how the amount of the fine could be established[5].

The AP's fining competency is embedded in art. 66 of the Wbp. Articles 66 Wbp and 6 of the Fining Policy of the AP include the notion of '*serious culpable negligence*'. Art. 66 Wbp provides that where the AP can establish that a respondent has been '*serious culpable negligent'* which lead to the violation of the Wbp, the AP may impose a fine immediately rather than after providing the respondent with Binding Instructions[6]. And the Fining Policy of the AP provides that where the AP establishes that an offense was either intentional or a result of '*serious culpable negligence'*, the AP may assume a significant degree of culpability which allows for the AP to impose a higher fine.

The General Data Protection Regulation (hereafter: GDPR)[7], which will come into force early 2018, lays down general conditions for imposing administrative fines, requiring from Member States' supervisory authorities to ensure that the imposition of fines is effective, proportionate and dissuasive in each individual case[8]. The GDPR also requires from Member States' supervisory authorities that, when deciding whether to impose an administrative fine and

[1] Wet bescherming persoonsgegevens, *Stb*. 2000, 203.
[2] Art. 66 Wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens en enig andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede de uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp), *Stb*. 2015, 230.
[3] https://www.rijksoverheid.nl/actueel/nieuws/2015/07/10/meldplicht-datalekken-en-uitbreiding-boetebevoegdheid-cbp-1-januari-2016-van-kracht, consulted on August 27, 2016.
[4] Beleidsregels van de Autoriteit Persoonsgegevens van 15 december 2015 met betrekking tot het opleggen van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2016), *Stcrt*. 2016, 2043.
[5] https://autoriteitpersoonsgegevens.nl/nl/nieuws/autoriteit-persoonsgegevens-nieuwe-taken-en-nieuw-logo, *Boetebeleidsregels*, consulted on April 8th, 2016.
[6] See art. 66(3) and 66(4) Wbp.
[7] Regulation (EU) 2016/679 of the European Parliament and the of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 5419/16, Brussels, 06.04.2016.
[8] Article 83(1) GDPR.

deciding on the amount of the fine, they have to give due regard to the "intentional or *negligent character*" of the infringement in each individual case[9].

Until the GDPR comes into full effect, art. 66 Wbp will provide the basis for the AP's competence to impose fines for Wbp violations. '*Serious culpable negligence'* however, has not yet been defined nor applied as a norm for a decision as the whether an authority could issue a fine or as a factor for the calculation of the fine. And as the AP and Dutch legislators have not provided guidance for the interpretation and application of '*serious culpable negligence'* in the context of art. 66 Wbp and art. 6 of the Fining Policy of the AP, it is important to clarify how the AP can define and establish '*serious culpable negligence'*, to provide some degree of certainty in this context.

To clarify the notion '*serious culpable negligence'* the author has chosen to analyze the 'fair processing principle', as establishing unfairness could be an indication of culpability or negligence. Also, the author analyzes the notion of gross negligence[10] as provided for in the competency to fine for the violation of specific Dutch tax law provisions and the notions of conditional intent and negligence as interpreted within Dutch law but also negligence as interpreted in common law countries, as these notions may provide guidelines for the interpretation of '*serious culpable negligence'*. Afterwards the author will analyze the establishment of culpability through the application of Chapter Eight of the Federal Sentencing Guidelines (hereafter: FSG)[11]. Chapter Eight of the FSG is applied by US district courts for the establishment of a fine for the violation of a Federal Trade Commission Order, which was imposed or settled upon by the Federal Trade Commission (the de facto enforcer of consumer's privacy rights in the United States) for the (alleged) violation of consumer's privacy rights (see chapter 4). Chapter Eight of the FSG includes factors and rationales for the determination of a culpability score which is part of a calculation method for fines and can, in the case of '*serious culpable negligence'* help establish the level (seriousness) of culpability involved.

On a final note, this thesis includes a brief segment tailored to the question as the whether '*serious culpable negligence'* could affect the organization of privacy compliance within organizations. Data breaches and other "security failures" have become a hot topic amongst some[12], which can make someone wonder how personal data processors organize their compliance with applicable privacy and data protection laws and regulations, whether they have improved their compliance programs over the last couple of years but specifically,

[9] Emphasis added. Art. 83(2)(b) GDPR.

[10] Own translation of 'grove schuld': to clarify, the author in this thesis refers to 'grove schuld' (schuld which is translatable to culpa in Dutch law) when is spoken of 'gross negligence' and refers to 'ernstig verwijtbare nalatigheid' when is spoken of 'serious culpable negligence' (where nalatigheid is directly translatable to negligence). The author notes that the use of negligence for both schuld (culpa) and nalatigheid can somewhat be explained by the definition given to culpa in the Black Law Dictionary (1991) (and via http://thelawdictionary.org/culpa/, consulted on August 27, 2016) which defines culpa as *fault, neglect or negligence*. The author deducts from this definition that there is a degree of overlap between the notions of culpa and negligence, and that negligence can in some circumstances also be used instead of culpa (schuld), even though 'schuld' and 'nalatigheid' in Dutch law (can) have (somewhat) different meanings.

[11] United States Sentencing Commission Guidelines Manual 2015.

[12] See for example www.privacynieuws.nl.

whether the inclusion of '*serious culpable negligence'* can have an effect on the organization of privacy compliance within organizations.

1.2 Research questions

The central research question of this thesis is:

> *What can we learn from the GDPR, Dutch tax- and criminal law and Chapter Eight of the US Sentencing Guidelines for Organizations for the interpretation and application of '*serious culpable negligence' *concerning the competency of the Dutch DPA to impose fines for the violation of provisions of the Dutch Data Protection Act? And what might the effect be of the application of '*serious culpable negligence' *in this context on the organization of privacy compliance within organizations?*

The following sub-topics have been formulated to answer the research question:

1. '*Serious culpable negligence'*: its background in art. 66 Wbp and art. 6 of the Fining Policy of the AP, its alignment with art. 83 of the GDPR and establishing 'fairness' –This chapter provides background information as to why '*serious culpable negligence'* was included in the Wbp and the Fining Policy of the AP and the definition it was given in Parliamentary history. It also includes an assessment of 'how the notion aligns with art. 83 of the GDPR and an assessment of the 'fair processing principle' to show that establishing unfairness could point towards culpability or negligence.

2. Establishing negligence: The application and interpretation of negligence under Dutch law and common law and of the notions conditional intent and gross negligence under Dutch (tax- and criminal) law – In this chapter the author discusses the requirements for the establishment of negligence, gross negligence and conditional intent to help establish an interpretation of '*serious culpable negligence'* by the AP .

3. Establishing culpability: focusses on the rationales underlying and factors determining the culpability score in a fine calculation method laid down in Chapter Eight of the Federal Sentencing Guidelines to apply the same rationales and factors to determine the relevant level of culpability - The author discusses the FTC's authority to enforce consumer's privacy rights, the imposition of or settlement on FTC orders and its competency to impose a fine for the violation of a Commission Order (through a district court). Particularly, this chapter analyzes one of the methods of Chapter Eight of the FSG for the calculation of a fine. This calculation method includes a culpability score and the factors and underlying rationales which make up for the score can affect the interpretation of '*serious culpable negligence'*.

4. What might the effect be of the application of '*serious culpable negligence'* of art. 66 Wbp on the organization of privacy compliance within organizations? – The author questions whether the application of '*serious culpable negligence*' in the determination to issue a (higher) fine for noncompliance with the law has an effect on the organization of privacy compliance, and if so, what that effect could be.

1.3 Significance

The primary goal of this thesis is to clarify '*serious culpable negligence'* as laid down in art. 66 Wbp (and the Fining Policy of the AP). Secondary goal is to figure out whether the application of '*serious culpable negligence'* has an effect on the organization of privacy compliance within organizations. Until the GDPR is fully applicable in the Netherlands, the AP will apply art. 66 Wbp and the Fining Policy of the AP for the imposition of fines and thus '*serious culpable negligence'*, for noncompliance with the Wbp. However, '*serious culpable negligence*' has not yet been used as a norm for a decision to impose a fine immediately and in the determination of the amount of the fine. The author analyses various notions, such as the requirements for establishing negligence, (conditional) intent and gross negligence, embedded in national and international regulation to narrow down an interpretation of '*serious culpable negligence'* so that those to who the Wbp applies to have an idea as to how the AP might apply '*serious culpable negligence'*.

1.4 Research Methodology

To address the research question a doctrinal legal research method will be applied. The conducted research will be desk-based and includes the locating of applicable legislation, case-law and relevant literature. The author will first gather facts, identifying the gap of knowledge surrounding the interpretation of a legal provision and applicable Guidelines. Hereafter the author will assess various similar and relevant notions existing in national and international regulatory fields for a potential solution, to eventually arrive at a conclusion. Sources to be used in the author's research consists of (but is not limited to) the following:

- Official documents, such as the Dutch Data Protection Act, the Dutch Penal Code, relevant Parliamentary Documents, the General Data Protection Regulation (GDPR) and the Federal Trade Commission Act;
- Dutch and US Case-law, such as Hoge Raad 29 mei 2015, V-N 2015/27.17, BNB 2015/146, NJB 2015/1268 and Consent Order No. 142 3156 FTC in the matter of ASUSTeK Computer, Inc., a corporation (2016);
- Publications from authors such as K.A. Bamberger and D.K. Mulligan (2010), J.W. Binkley (2016), P.S. Frechette (2013), W. Hartzog and D.J. Solove (2013/2014), C. Kuner (2012), W.J. Maxwell (2014 and 2015), T.F.E. Tjong Tjin Tai, E.J. Koops, D.J.B. Op Heij, K.K. E. Silva and I. Skorvánek (2015); and
- Reports such as the UK's Information Commissioner's Office's *Review of the impact of ICO Civil Monetary Penalties* and Ponemon Institute LLC's report *Cost of Compliance: A Benchmark Study of Multinational Organizations*.

1.5 Overview of chapters

This thesis is outlined as follows: chapter 2 elaborates on '*serious culpable negligence'* as laid down in art. 66 Wbp, the Fining Policy of the AP, its alignment with art. 83 of the GDPR and the concept of fairness in relation to privacy and data protection. Chapter 3 discusses the

requirements for establishing negligence, conditional intent and gross negligence and assesses how these may affect the interpretation of '*serious culpable negligence'*. Chapter 4 explains the rationales and factors embedded in the Federal Sentencing Guidelines which can apply in the determination of fines to be imposed for the violation of FTC orders by organizations (which were imposed for the violation of consumer's privacy rights) and assesses how these affect the interpretation of '*serious culpable negligence'*. Chapter 5 deals with the question as to what the effect of the application of 'serious *culpable negligence*' might be on the organization of privacy compliance within organizations. Chapter 6 concludes.

Chapter 2 '*Serious culpable negligence*': its background in the Wbp and Fining Policy of the AP, its alignment with art. 83 of the GDPR and the concept of fairness in relation to privacy and data protection

2.1 Introduction

Chapter 2 explains the background as to why '*serious culpable negligence*' was added to art. 66 Wbp and the meaning it was given in its parliamentary history. Afterwards, the author discusses '*serious culpable negligence'* in light of art. 83 of the GDPR. The GDPR will replace the Wbp in the first half of 2018, making it necessary to discuss the 'negligent character of the infringement' as embedded in art. 83 GDPR. Art. 83(2)(b) GDPR grants national supervisory authorities the possibility to impose an administrative fine. The article requires from supervisory authorities to give 'due regard' to the intentional or negligent character of the infringement when deciding on whether to impose an administrative fine and deciding on the amount of the fine. While preparing for the full application of the GDPR, the AP could consider 'the negligent character of the infringement' when imposing a fine on organizations for violating Wbp provisions (instead of '*serious culpable negligence'*). As '*serious culpable negligence'* seems to be a more grave form of negligence or 'negligent character', it could mean that organizations might be subjected to an immediate and or higher fine[13] sooner if the AP decides to apply the 'negligent character of the infringement'-criteria when imposing a fine for the violation of Wbp provisions. Finally, this chapter closes with an analysis on the concept of the fair processing principle to determine if establishing unfairness can pinpoint us towards negligence.

2.2 '*Serious culpable negligence*'

2.2.1 '*Serious culpable negligence*', art. 66 Wbp and (art. 6 of) the Fining Policy of the AP

2.2.1.a 'Serious culpable negligence' in art. 66 Wbp
Art. 66 Wbp was instituted through the Bill of June 4 2015, which expanded the AP's competency to impose administrative fines, and includes the notion of '*serious culpable negligence'.* The parliamentary history of art. 66(4) Wbp shows that '*serious culpable negligence'* is defined as "an abusive, considerably careless, negligent or injudicious act" and provides that if the same type of violations has occurred several times, negligence will be assumed more quickly.[14] The Wbp otherwise provides no other definition or guidance for the interpretation of the notion, besides that '*serious culpable negligence'* was included in the article to protect the right to private life when extraordinary situations require a punitive action

[13] Art. 66(3) and (4) Wbp, art. 6(2) Fining Policy AP.
[14] Own translation; Kamerstukken II 2014/2015, 33 662, no. 16, p. 1: "…indien de overtreding het gevolg is van ernstig verwijtbare nalatigheid, dat wil zeggen het gevolg is van grof, aanzienlijk onzorgvuldig, onachtzaam dan wel onoordeelkundig handelen.".

because of, on the one hand, the severity of the violation of the right to private life and on the other hand, the ease with which the violation could have been prevented[15].

2.2.1.b The application of art. 66 Wbp

Article 66 of the Wbp works with a two-tier system: where a violation of a Wbp provision has occurred, the AP is required to give respondents a Binding Instruction prior to imposing an administrative fine[16] (first-tier). The Instruction is meant to give insights as to which provisions the respondent is in violation of (and the extent of the violation) according to the AP[17]. The Instructions are of importance to the respondent because firstly, the violation could have occurred under particularly complex conditions. Also, the Wbp contains various general, open to interpretation, norms which only become clear after concrete situations arise. Both reasons can lead to a difference of opinions between the respondent and the AP. The Instruction creates clarity about the alleged violation so the respondent can get the opportunity to appeal the alleged violation, but also so it can take appropriate measures to negate the violation and avoid the fine[18].

However, if the AP finds intention for the violation or establishes '*serious culpable negligence*' which lead to the violation of a Wbp provision, the AP has the competency to impose a fine immediately (second-tier) and take it into account when calculating a (higher) fine.[19]

Art. 66(1) and (2) Wbp, in conjunction with articles 2, 3 and 4 Fining Policy AP and art. 23(4) Wetboek van Strafrecht[20] (Dutch Penal Code, hereafter WvSR) depict a categorical fining system per type of violation for calculating a fine: a respondent can either be subjected to a fine up to 820.000 EUR, 450.000 EUR or 20.500 EUR depending on the type of violation. Appendixes 2, 3 and 4 of the Fining Policy AP specify which subcategory of which category will then determine the range (bandwidth) the AP is bound to when calculating the amount of the fine.

[15] Own translation; Kamerstukken II 2014/2015, 33 662, no. 16, p. 2.
[16] Art. 66(3) Wbp.
[17] Kamerstukken II 2014/2015, 33 662, no. 15: "waarin het Cbp gemotiveerd aangeeft in hoeverre gedragingen van de verantwoordelijke in strijd zijn met de Wet bescherming persoonsgegevens (Wbp)".
[18] Kamerstukken II 2014/2015, 33 662, no. 15, p.1-2.
[19] Art. 66(4) Wbp and Art. 6(2) Fining Policy AP.
[20] Wetboek van Strafrecht, Wet van 3 Maart 1881, *Stb*. 35.

2.2.1.c The Fining Policy of the AP (Guidelines)[21]

The Guidelines aim to clarify the way art. 66 Wbp should be interpreted and applied, including the manner of calculation of the fine[22]. However, like the Wbp or its Parliamentary history, the Guidelines does not provide a definition of '*serious culpable negligence'* and thus no further clarification on the interpretation and application of '*serious culpable negligence'*.

In summary

The parliamentary history of art. 66 Wbp defines 'serious culpable negligence' as follows:

- *"an abusive, considerably careless, negligent or injudicious act. If the same type of violations has occurred several times, it will be assumed sooner that a case of negligence has taken place."*
- *The addition of 'serious culpable negligence' is to ensure the protection of the right to private life when extraordinary situations require a punitive action because the severity of the violation of the right to private life and the ease with which a violation can be prevented.*

2.2.2 '*Serious culpable negligence'* in light of art. 83 GDPR

Directive 95/46/EC left it to the EU member states to determine the amount of administrative sanctions, through proper implementation of the obligations as laid down in art. 24 Directive 95/46/EC in national law.[23] As a result, the administrative fines for violating provisions of national data protection laws vary widely amongst the member states[24]. The GDPR however, which was adopted early April and entered into force on May 24 2016, will apply directly to all

[21] Regarding the validity of the Fining Policy established by the AP, the following can be said: when the Fining Policy was still being drafted, a discussion was ongoing between the State Secretary of the Ministry of Security of Justice and the AP regarding the necessity of Ministerial approval of guidelines drafted by the AP. Art. 67 Wbp currently reads: "*The AP ('College') will consult with Our Minister and Our Minister of the Interior and Kingdom Relations prior to establishing guidelines regarding the interpretation of the provisions mentioned in or pursuant to art. 66(2) Wbp*" (own translation). Prior Ministerial approval is thus not mandatory for the establishment of AP Guidelines (prior consultation with 'Our Ministers' is). An amendment to the Bill of June 4 2015 explains that, because the Ministry of Security and Justice and the Ministry of the Interior and Kingdom Relations fall under the supervision of the AP, having both ministries be able to directly influence the interpretation of said supervision through Ministerial Approval is an undesirable situation. The independence requirement laid down in art. 28 Directive 95/46/EC supports this finding. By replacing a Ministerial Approval with prior consultation and leaving the establishment of Guidelines up to the AP, independence of the AP is safeguarded, see Kamerstukken II 2014/2015, 33 662, no. 15, p.3 and Kamerstukken II 2014/2015, 33 662, no. 13 and 22, p.1-2.

[22] https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-krijgt-boetebevoegdheid-en-wordt-autoriteit-persoonsgegevens, consulted on 16.06.2016.

[23] Art. 24 Directive 95/46/EC: Sanctions. The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular imposed in case of infringement of the provisions adopted pursuant to this Directive.

[24] Kuner, C., *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, Bloomberg BNA Privacy and Security Law Report (2012) February 6, 2012, p. 21.

EU member states from May 25 2018 (to foster harmonization)[25][26] onwards and will subsequently replace the Wbp and repeal Directive 95/46/EC.

The GDPR takes a different route from Directive 95/46/EC: the GDPR directly provides national supervisory authorities the competency to impose administrative fines without requiring implementation of a competency in national law. The GDPR lays down general conditions, firstly by requiring supervisory authorities to ensure that "the imposition of administrative fines…shall in each individual case be effective, proportionate and dissuasive"[27]. Secondly, art. 83(2) GDPR requires that "when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: …(b) the intentional or negligent character of the infringement…" amongst various other factors. Thirdly, Art. 83(4), (5) and (6) GDPR determine that when specific conditions are met, the violators of GDPR provisions or those failing to comply with orders from a supervisory authority can be subjected to administrative fines up to either 10.000.000 EUR or 20.000.000 EUR or be fined up to either 2 or 4% of the total worldwide turnover of the preceding financial year (whichever amount is higher). The actual calculation of the fines is left to the national supervisory authorities, as long as they comply with art. 83 GDPR[28].

Regarding 'the negligent character of the infringement' as a factor which needs to be give due regard in a decision to impose a fine and in the calculation of a fine[29], Recital 148 of the GDPR provides only the following: when deciding on whether to impose a fine or when determining the amount of a fine "due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor." Any explanation, definition or guidance as to what a 'negligent character of the infringement' might constitute seem to be lacking.

In summary / Findings

- *Recital 148 of the GDPR gives no specific explanation for the interpretation of the 'negligent character of the infringement' but does lay down several factors which need to be accounted for when applying art. 83 GDPR;*

[25] Kuner, C., *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, Bloomberg BNA Privacy and Security Law Report (2012) February 6, 2012, p. 1.
[26] http://ec.europa.eu/justice/data-protection/reform/index_en.htm, consulted on 16.06.2016.
[27] Art. 58(2)(j) GDPR, art. 83(1) GDPR.
[28] Cuijpers, C., et al., *Een eerste verkenning van het Voorstel Verordening bescherming persoonsgegevens*, Computerrecht afl. 3 juni 2012, pp. 185-199, p. 22.
[29] Art. 83(2)(b) GDPR.

- *Art. 66 Wbp is in line with art. 83 GDPR, yet differs on the inclusion of 'negligent character of the infringement' versus '*serious culpable *negligence' (a graver form of 'mere negligence'*);
- *It seems that art. 83 GDPR gives a wider discretion to the AP than art. 66 Wbp regarding the fining competency: Art. 66 states that 'serious culpable negligence' leading to a violation of the law could give rise to an immediate fine, which does not require a balancing act or assessment of other relevant factors and circumstances. The establishment of a 'negligent character of the infringement' under the GDPR requires that this factor needs to be accounted for by the AP in its decision to impose a fine, but also all other relevant factors as mentioned in art. 83 GDPR and Recital 148, meaning that an immediate fine can ensure but still requires a balancing act by the AP of all other relevant factors.*

2.2.3 '*Serious culpable negligence'* in light of 'fair processing of personal data'

This paragraph discusses the interpretation and application of the principle of fair processing in Europe and the United States. Further down the road in the conclusion the author will find that fair processing in relation to personal data, and especially establishing unfair processing or an unfair act, could help point towards negligence with the respondent.

Fair processing is one of the important principles embedded in data protection legislation in Europe and in the U.S: it is laid down in the OECD Guidelines, the European Charter of Fundamental Rights, the European Data Protection Directive 95/46/EC, the Council of Europe Convention of Data Protection and in Section 5 of the Federal Trade Commission Act[30]. The author will first discuss the application of the 'fair processing principle' as embedded and applied in European data protection law, including the UK and France, after which the interpretation of the 'fairness' in the US by the Federal Trade Commission (FTC) will be discussed.

2.2.3.a Application of the 'fair processing principle' in European data protection law, in the UK and in France[31]

Art. 6 Directive 95/46/EC provides that personal data has to be processed 'fairly and lawfully'. Recital 38 of Directive 95/46/EC explains: "Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection." The Recital connects 'fairness' to the level of information given to the data subject, which is comparable to the FTC's approach as it emphasized individual information and choice (explained further below). Where data subjects

[30] Maxwell, W. J., *Principles-based regulation of personal data: the case of 'fair processing'*, International Data Privacy Law, 2015, Vol. 5, No. 3 (hereafter: Maxwell, W.J., (2015)), p. 205, Maxwell, W.J., *The notion of "fair processing" in data privacy law* (January 2, 2015), Quelle protection des données personnelles en Europe?, Céline Castets-Renard (ed.), University of Toulouse, Forthcoming, 2015 (hereafter: Maxwell, W.J., (2015-2)), p. 1.
[31] Maxwell, W.J., (2015), p. 208.

are given inadequate information, the data subject is not being put in a position to exercise autonomy over his or her personal data: if said information is absent, the processing of personal data is seen as 'unfair'. Art. 10 of Directive 95/46/EC also suggests, in line with Recital 38, that fair processing is linked to the level of information provided to the data subject. Art. 10 Directive 95/46/EC lists the information that has to be provided to data subjects by the data controller which is: 'such further information [as] is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject'[32].

The GDPR[33] includes a provision broadly similar to art. 6 Directive 95/46/EC. Under the heading of 'lawfulness, fairness and transparency', art. 5(a) GDPR sets forth that personal data shall be "*processed lawfully, fairly and in a transparent manner in relation to the data subject*." Recital 39 of the GDPR explains that all personal data processing need to lawful and fair and that transparency needs to be created in regards to the data subjects concerning the type and the extent of the data processing. The principle of transparency requires that any information and communication relating to the processing of those data needs to be easily accessible and easily understandable (clear and plain language).

Fairness under Convention 108 and the European Convention on Human Rights also covers more than transparency, such as under the GDPR. The European Union Agency for Fundamental Rights, the European Court of Human Rights and the Council of Europe characterized fair processing as requiring both transparency and trust in 2014: the data subject should be in a position to 'really understand' what happens to his or her personal data. It requires that the processing operations should not be performed in secrecy and it should not have unforeseeable negative effects. Sometimes fair processing will require from data controllers that they make efforts outside of the minimum legal requirements if the legitimate interests of the data subjects require for them to do so[34]. Thus, the data controller has to account for the data subject's legitimate interests and refrain from processing even if they are otherwise legal: fairness requires the balancing of the interest of both the data subject and the data controller's own[35].

Fair and lawful processing in the UK requires[36] a legitimate ground, transparency regarding the use of the data towards data subjects, handling of the data by the controller in a manner not inconsistent with the data subject's reasonable expectations and no unlawful activities regarding the data. Furthermore, processing is prohibited if it has unjustified adverse effects on the data subjects (which requires a test similar to the cost-benefit analysis the FTC applies in its unfairness test which will be explained in the upcoming part). Schedule I of the UK Data

[32] Maxwell, W.J., (2015), p. 208, Maxwell, W.J., (2015-2), p. 4.
[33] Maxwell, W.J., (2015), p. 208.
[34] Maxwell, W.J., (2015), p. 208 and European Union Agency for Fundamental Rights, European Court of Human Rights, and Council of Europe, *Handbook on European Data Protection Legislation* (Publication Office of the European Union, Luxembourg, 2014) ('Handbook'), p. 73-75.
[35] Maxwell, W.J., (2015), p. 208.
[36] Maxwell, W.J., (2015), p. 208.

Protection Act 1998 also provides guidelines for determining 'fair processing': "In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, included in particular whether any persons from whom they are obtained is deceived or misled as to the purpose or purposes for which they are processed." Fairness, similar to article 10 Directive 95/46/EC, is linked to the provision of a minimum level of information which needs to be provided to the data subjects through Schedule 1 of the Data Protection Act 1998. Under Data Protection Act 1984 a court further established that 'fairness' (then undefined in the Act), requires [the court] to weight up the interests of data subjects and data users'[37].

The French data protection authority Commission Nationale de l'Informatique et des Libertés (CNIL) also links the concept of 'fairness' to the level of information provided to the data subject[38]. French consumer protection law defines 'unfair practices' as: 'commercial conduct that is contrary to the requirements of professional care and that modifies, or may modify, in a significant manner the economic conduct of a consumer'. Practices which are 'misleading' and 'aggressive' are categorized as unfair practices. 'Abusive contractual clauses' which create a significant imbalance between the parties are prohibited under the consumer protection code.[39]

2.2.3.b Application of the 'fair processing principle' in the United States: the FTC's fairness test
The FTC is a US independent government agency, whose mission is to enforce competition and consumer protection laws in the United States. The FTC also tries to ensure that consumers are sufficiently informed and have the opportunity to make choices relating to privacy.

The FTC uses Section 5 of the FTC Act to enforce data protection principles. Section 5 of the FTC Act prohibits: '*unfair or deceptive acts or practices in or affecting commerce'*. The FTC Act also contains the FTC's fairness test, which was inserted into the Act in 1994 by the U.S. Congress. The provision reads as follows: *"The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition…."*.

The fairness test comprises of three steps[40]:

- Step 1: unfairness requires that the practice (act or omission) causes or is likely to cause substantial injury (harm) to consumers or a consumer (data subject(s));

[37] Maxwell, W.J., (2015), p. 209, Maxwell, W.J., (2015-2), p. 4-5.
[38] Maxwell, W.J., (2015), p. 209, Maxwell, W.J., (2015-2), p. 6.
[39] Maxwell, W.J., (2015), p. 210.
[40] Maxwell, W.J., (2015), p. 206, Hoofnagle, C.J., *Federal Trade Commission Privacy Law and Policy,* Cambridge University Press, 2016 (hereafter: Hoofnagle, C.J., (2016-2)), p. 132, Maher, A.V. (2010)), p. 600, Ohlhausen, M.K, (2015), p. 31 and https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection, part. III, consulted on August 27, 2016.

- Step 2: injury (harm) is one which consumers cannot reasonably avoid: consumers need to be given reasonable opportunity to make a choice under the given circumstances;
- Step 3: encompasses a cost-benefit analysis[41]: it requires the evaluation of any countervailing benefits. The FTC needs to inquire whether the practice (action or omission) in question generates new valuable services, or lower prices, for consumers. In its analysis, the FTC has to compare the situation that would exist in absence of regulation by the FTC against the situation that would exist if said practice were halted or regulated[42]. The difference herein represents the costs associated with the FTC's own regulatory action which eventually results in the benefits associated with leaving the practice unregulated[43].

In summary

- *The European approach to fairness relies on the level of information provided to the data subject, the data subject's legitimate interests and the ability to exercise individual autonomy[44]: Directive 95/46/EC links the fair processing principle to transparency (the level of information given to the data subject). Under Convention 108 and the European Convention on Human Rights, fairness encompasses more than just transparency, because it requires from data controllers to go beyond that which is legally required if doing so is necessary to protect the legitimate interests of the data subject. Art. 5 GDPR connects lawful, fair and transparent processing, suggesting that fairness is more than only transparency and requires a good faith consideration of the interests of the data subject;*
- *The FTC acts in the interest of competition and consumer protection: fairness under the FTC relies also on consumers having been given sufficient information and having a reasonable opportunity to make choices in regards to privacy.*

The interpretation of fairness or fair processing will be applied to the notion of culpability and/or negligence in the conclusion (chapter 6), which will show that establishing unfairness or unfair data processing can point towards culpability or negligence.

[41] Maxwell, W.J., (2015-2), p. 6.
[42] Maxwell, W.J., (2015), p. 211.
[43] Maxwell, W.J., (2015), p. 207-208, Maxwell, W.J., (2015-2), p. 2.
[44] Maxwell, W.J., (2015), p. 210.

Chapter 3 Existing interpretations of negligence in Dutch and common law and the notions of conditional intent and gross negligence in Dutch tax- and criminal law

3.1 Introduction

This chapter discusses existing interpretations of and requirements for establishing negligence in Dutch and common law. After analyzing the requirements of negligence, the author discusses the notions of conditional intent and gross negligence as referred to in Dutch tax- and criminal law. The Dutch General law on state taxes[45] (Algemene Wet inzake Rijksbelastingen; hereinafter AWR) includes provisions which states that public authorities are competent to impose a civil penalty when specific requirements are met. One of the requirements that needs to sufficiently proven is either intent or gross negligence[46] which is attributable to the taxpayer (referred to in this chapter as "defendant"). The author aims to show that the requirements to establish both notions can help either establish a relevant level of culpability (serious) or negligence itself to further narrow down an interpretation of '*serious culpable negligence'*.

3.2 Negligence: existing interpretations in Dutch and common law

This paragraph analyzes the various requirements needed to establish (torts or actions of) negligence in the context of common law countries and Dutch law.

An action (torts) of negligence in common law countries requires the existence of a duty of care, a breach of this duty, where this breach must have caused legal injury (harm) to the plaintiff and it must be proven that the defendant's action or inaction was the proximate cause of said injury[47]. Negligence can be established through either an act or omission on part of the defendant[48] but depends also on whether the harm caused was reasonably foreseeable for the defendant[49].

The existence of a duty of care relies on a special existing relationship (relationship of proximity) between the parties involved at the time of the negligent act but it also depends on whether it is "just and fair" to impose a duty of care upon the defendant as there might be reasons to refuse to recognize a duty of care in some cases[50]. It is this relationship which determines whether a duty is care exists, which must have been breached, and where the breach subsequently resulted in the kind of (physical) injury or damage (harm) which is

[45] Algemene Wet inzake rijksbelastingen, Stb. 1959, 301.
[46] See also footnote 10.
[47] Christian, G.E., *A New Approach to Data Security Breaches*, Canadian Journal of Law and Technology, Vol. 7, No. 1, p. 149, 2009 (hereafter: Christian, G.E., (2009)), p. 19.
[48] Tjong Tjin Tai, T.F.E., et. al., (2015), p. 80.
[49] Chandler, J. A., *Negligence Liability for Breaches of Data Security*, Banking and Finance Law Review, Forthcoming (hereafter: Chandler, J.A., (Forthcoming)), p. 22.
[50] Chandler, J.A., (Forthcoming), p. 21.

recognized by law[51]. If necessary, a duty of care will be created by statute or by judges through the application of common law principles[52].

One way of describing negligence is as "the failure to live up to the standard of care". Regarding the 'standard of care', it is viewed as "care that would be exercised by a reasonable and prudent person under the same or similar circumstances to avoid or minimize risks or harm to others" by US courts. And in the US, "professionals" are "held to possess the skill and knowledge of others in good standing in their profession"[53].

Dutch Private law recognizes a tort of negligence in the form of a liability for faults of negligence ('onzorgvuldigheid') which stems from the French Civil Code. Under Dutch law, everyone has a 'zorgvuldigheidsplicht' ('duty of diligence): the carefulness or diligence which is required under ordinary social circumstances. 'Duty of care' is a relatively recent development within the Dutch legal system. This duty of care requires not only passive caution to avoid tortious action on the basis of negligence, but it might also require active behavior to protect others from harm, even if the primary cause lies elsewhere. Beyond Dutch tort law, 'duties of care' comprises also of the duty of contracting parties to observe the care of reasonable contracting parties. In this context, a 'duty of care' is described as: "a duty for a person to observe or provide care for another person or object", care which is usually defined as the care required under any particular given circumstances[54].

The concept of a duty of care is also part of a liability for an offence based on negligence in Dutch criminal law. For criminal liability to exist on the basis of negligence, intentional actions ('dolus') is required which includes the conscious acceptance of the considerable likelihood of the occurrence of a certain result (see also conditional intent, discussed below): this situation implies a duty to be aware of the consequences of one's actions and to take preventative measures to diminish the opportunities to commit crimes. Where intent does not exist but culpa ('schuld') does, negligence can be established by asking whether an organization has not acted as considerately as can be reasonably expected from the average person in a certain situation. Depending on the organization or profession involved (in a data breach for example), professionals will sometimes be held against higher standards of conduct than average users, which makes it easier to assume (serious culpable or gross) negligence, especially when they are specialists in the field of information security (such as a CISO)[55].

[51] Christian, G.E., (2009), p. 20-21 and Rhee, W. J., *The Tort Foundation of Duty of Care and Business Judgment* (2013), Notre Dame Law Review, Vol. 88, 2013, p. 1139+; U of Maryland Legal Studies Research Paper No. 2013-27, p. 1159-160 and Tjong Tjin Tai, T. F. E., Koops, E. J., Op Heij, D. J. B., E Silva, K. K., & Skorvánek, I. (2015), *Duties of care and diligence against cybercrime*, Tilburg University (hereafter: Tjong Tjin Tai, T.F.E., et. al., (2015)), p. 79.
[52] Chandler, J.A., (Forthcoming), p. 22.
[53] Tjong Tjin Tai, T.F.E., et. al., (2015), p. 80.
[54] Tjong Tjin Tai, T.F.E., et. al., (2015), p. 17-18
[55] Tjong Tjin Tai, T.F.E., et. al., (2015), p. 64 and 69.

In summary

- *Negligence in common law requirements: a duty of care, the breach of this duty, where the breach caused harm and where the practice (act or omission) was the proximate cause of the harm. A duty of care depends on whether it is 'just and fair' to impose such a duty on the defendant and on the relationship between parties at the time of the act. Negligence depends also on whether the harm caused was reasonably foreseeable for the defendant, and depends on a standard of care: "care that would be exercised by a reasonable and prudent person under the same or similar circumstances to avoid or minimize risks or harm to others".*

- *Negligence under Dutch private law is linked to a duty of diligence: the carefulness or diligence which is required under ordinary social circumstances where the duty of care requires both an act or an omission to avoid tortious action on the basis of negligence and to protect others from harm, even if the primary cause lies elsewhere. Liability for an offence based on negligence (criminal law) based on intent requires at least an intentional act and the conscious acceptance of the considerable likelihood that an effect (adverse) will ensue. Negligence offences based on culpa (lack of intent) are offences attributable to those who have been insufficiently careful which resulted in adverse effects to actually occur.*

3.3 Conditional intent and gross negligence in the Wetboek van Strafrecht and Algemene Wet inzake Rijksbelastingen

Intent or negligence attributable to the "defendant" are necessary components which need to be proven by the public authority if (s)he wants to penalize or fine a "defendant" under either the Dutch Penal Code (Wetboek van Strafrecht, hereafter: WvSR)[56] or the Dutch General law on state taxes (Algemene Wet inzake rijksbelastingen, hereafter: AWR)[57] for a violation of the law. Both articles 67e and 67f AWR for example, apply to the violation of specific provision as a result of intent or gross negligence attributable to the "defendant".[58][59]

In the following subparagraphs the author will discuss the requirements for establishing conditional intent and gross negligence, also noting that the interpretation and application of either of these terms by the tax authorities, is done in accordance with the interpretation of these terms in the regulatory field of Dutch law[60]. The author aims to show that the

[56] Wetboek van Strafrecht, Wet van 3 Maart 1881, *Stb*. 35. For example see articles 158 and 307 WvSr: "Hij aan wiens schuld brand, ontploffing of overstroming te wijten is…"; "Hij aan wiens schuld de dood van een ander te wijten is…".
[57] Algemene Wet inzake rijksbelastingen, Stb. 1959, 301, see articles 67d-67f AWR.
[58] Sitsen, J.M, *Comments on Artikel 67e AWR Aanslagenbelastingen; door opzet of grove schuld te weinig belasting geheven,* par. 2 and 4, via http://www.ndfr.nl/link/W0178-67e, consulted on July 11, 2016.
[59] Sitsen, J.M, *Comments on Artikel 67f AWR Aangifte belastingen; door opzet of grove schuld (gedeeltelijk) te weinig belasting betaald,* par. 6, via http://www.ndfr.nl/link/W0178-67f , consulted on July 11, 2016.
[60] Hoge Raad 29 mei 2015, V-N 2015/27.17, BNB 2015/146, NJB 2015/1268, par. 2.4.2., last sentence.

requirements establishing both notions can help narrow down an interpretation of '*serious culpable negligence'*.

3.3.1 Conditional Intent

In Dutch criminal law intent can be divided into various subcategories, the lowest category being conditional intent (*voorwaardelijk opzet*), a notion which does not exist in common law systems[61]. The requirements for establishing conditional intent, as can be read later, can function as the highest threshold where '*serious culpable negligence'* cannot be established anymore.

Conditional intent can be defined as the conscious acceptance of a possible risk and thus consists of these elements: there is a reasonable likelihood (risk) of a certain result, during the act (or omission) the defendant was aware of this reasonable likelihood and finally, the defendant consciously accepted the materialization of the reasonable likelihood of that particular result.[6263] Condition intent applies where the defendant has for example, knows about the risk (reasonable likelihood) which may materialize but acts (or omits) and thus takes the risk regardless.[64] In line with criminal law, the Decree on Administrative Fines of the Tax Authority (Besluit Bestuurlijke Boeten Belastingdienst, hereinafter: BBBB)[65] defines conditional intent as[66] willingly and knowingly accepting the reasonable chance that an act or omission leads the the payment or determination of too little taxes and/or the untimely or non-payment of taxes.

For the establishment of a reasonable likelihood, one needs to look at the surrounding circumstances, which includes the nature of the act or omission and on whether a chance is deemed reasonable under the general rules op experience ("algemene ervaringsregels"). Proving awareness of the reasonable likelihood and the conscious acceptance of the materialization of the reasonable likelihood in Dutch criminal law can make the difference between establishing either conditional intent or conscious negligence (*bewuste schuld*): knowing of but not accepting the materialization of the reasonable likelihood of a particular result, such as when the defendant thinks the adverse effects will not materialize (does not

[61] Keiler, J., Panzavolta, M., Roef, D., *Criminal Law*, Chapter 7 in Introduction to Law, Springer 2014 (hereafter: Keiler, J. (2014)), p. 137-138.
[62] Keiler, J. (2014), p. 137 and Hoekendijk, M.G.M, ZAKBOEK STRAFRECHT VOOR DE POLITIE 2015, Kluwer (hereafter: Hoekendijk, M.G.M., (2015), p. 23-24.
[63] In the *Aanmerkelijke Kans*-case, Hoge Raad 19 february 1985, NJ 1985, 633, defendant had been lent two suitcases by a man abroad, the suitcases had been packed with items from the foreigner and later also by defendant. When defendant arrived at Schiphol airport, the authorities found drugs in the double lid and bottom of both suitcases. The High Court noted that it is generally known that drugs are packed in the outer layers of suitcases and that defendant should have noticed that the lids and bottoms of the suitcases were thicker and heavier on average. Under these circumstances, the High Court concluded that by not inspecting the suitcases prior to flying, the defendant willingly and knowingly accepted the reasonable chance that there were drugs hidden in the suitcases, establishing conditional intent, and thus fulfilling the requirement of intent in this case.
[64] Keiler, J. (2014), p. 137.
[65] Besluit van 19 juni 2015, nr. BLKB2015/571M, Stcrt. 2015, nr. 17778 (Besluit Bestuurlijke Boeten Belastingdienst) (hereinafter: BBBB).
[66] Sitsen, J.M, *Comments on Artikel 67d AWR Aanslagenbelastingen; opzettelijk niet, onjuiste of onvolledige aangiften doen,*, par. 4(1) and (2), via http://www.ndfr.nl/link/W0178-67d, consulted on July 11, 2016.

take it for granted but believes in a positive outcome), may prove conscious negligence rather than conditional intent.[67] The Courts have emphasized the fact that where defendant should or could have known about the reasonable chance is insufficient to establish acceptance of a reasonable chance: for the establishment of conditional intent a conscious (subjective) acceptance needs to be proven[68].

An example of conditional intent can be shown through the Cake from Hoorn[69] case:

> Defendant intended to poison Mr. X by sending Mr. X a poisoned cake. Defendant knew Mr. X was married and lived with his spouse, so there was a reasonable chance that his wife would eat the cake as well (thus poisoning her (as well)). Mr. X's wife ate the cake and died as a result thereof. The court established and confirmed there was a reasonable chance the wife would eat the cake, that the defendant, while acting, had knowledge of this reasonable chance and consciously accepted the reasonable chance of the result to happen by sending the cake to Mr. X.

Another case where the High Court eventually decided there was no case of conditional intent is in the Porsche case[70]:

> The defendant caused a deadly car accident after driving while under influence of alcohol. The Court and Court of Appeals both established a case of conditional intent because: the defendant drove at an irresponsibly high speed while being under the influence of alcohol, drove through a red sign two times and made several dangerous attempts to bypass the car in front of him. The High Court considered that through the defendant's actions, he himself had a reasonable chance of dying. And that under the general rules of experience it is unlikely that the defendant took the reasonable chance of the deadly accident for granted. Evidence also showed that the defendant had halted several bypassing attempts to apparently avoid a collision: by not stopping the final attempt at bypassing the car in front of him, the defendant apparently was under the impression that the attempt would not lead to a collision (did not accept the risk nor did he take the risk for granted).

The establishment of reasonable chance was under discussion in a case where the High Court[71] concluded (from evidence) that having unprotect sexual relations with someone who is HIV-positive is hazardous, but could not conclude that (from evidence nor the general opinion) that this action (sexual relations with an HIV-positive person) can reasonably lead to being infected with HIV, unless special, risk-heightening circumstances apply. Conditional intent could not be proven in this case.

---

[67] Keiler, J. (2014), p. 139 and Hoekendijk, M.G.M., (2015), p. 24.
[68] Hoge Raad 3 december 2010, nr. 09/04514, NTFR 2010/2930 and Hoge Raad 20 september 2011, nr. 10/01297, NTFR 2011/2323 via Sitsen, J.M, *Comments on Artikel 67d AWR Aanslagenbelastingen; opzettelijk niet, onjuiste of onvolledige aangiften doen,*, par. 4(2), via http://www.ndfr.nl/link/W0178-67d, consulted on July 11, 2016.
[69] Hoge Raad 19 june 1911, W 9203.
[70] Hoge Raad 15 oktober 1996, NJ 1997, 199/Ars Aequi AA19970438.
[71] Hoge Raad 18 january 2005, LJN AR1860/NJ 2005, 154, and Hoge Raad 20 februari 2007, LJN AY9659.

3.3.2 Gross Negligence

This subparagraph discusses a particular form of negligence, namely 'gross negligence' because the requirements establishing this notion can help further narrow down an interpretation of '*serious culpable negligence'*. As established in par. 3.2, establishing negligence includes the violation of a duty of care under Dutch criminal law, a duty of care which requires a particular standard of care. Negligence under criminal law can be interpreted in various ways, such as considerable or gross negligence or considerable or gross carelessness (culpa 'lata'). It also includes recklessness and the use of terms such as 'lack of due care' or 'lack of reasonable care'.[72]

The BBBB defines gross negligence as an act or omission thus "unacceptable" it borders on intent[73], such as unacceptable carelessness or serious negligence. Under the AWR (gross) negligence applies when the defendant doesn't consciously violate the law nor does (s)he consciously take the risk of violating the law, but where (s)he should have been aware of the risk of the violation[74]. Also, the level in which additional facts and circumstances need to be accounted for in the establishment of gross negligence depends on several factors, such as the knowledge of the "defendant", the complexity of the case at hand and the level of exertion involved.[75]

- *(Gross or Considerable) Carelessness*

An example of where considerable carelessness (for the establishment of negligence) could not be established is the case *Of the Fatal Climb*[76]:
Defendant, a professional indoor climber, had to secure the victim, who was on the climbing wall when the fatal accident occurred. Victim was secured and connected by a rope with defendant, who was then on the ground. A friend of the defendant, together with another 'securer', climb the wall next to defendant. While defendant' friend returns to the ground and defendant talks to the other 'securer', defendant disconnects the rope connected to the victim while she is still on the wall. The victim fell and died later on as a result of her wounds. The Court of Amsterdam ruled that *unconscious negligence* (lack of attention) was attributable to the defendant, because according to the Court, defendant acted *considerably negligent* by not giving the expected attention to the victim and by unconsciously disconnecting the rope without verifying whether the victim had returned to the ground. The Court however acknowledged that the disconnect occurred while in "auto-pilot-mode" as defendant shifted his attention to his friend who had been rather hesitant of climbing as a result of several negative climbing experiences. The Court of Appeals in turn disagreed with the Court of Amsterdam,

[72] Hoge Raad 29 juni 2010, LJN BL5630; Hoge Raad 20 november 2010, LJN BN7726, Keiler, J. (2014), p. 138 and Hoekendijk, M.G.M., (2015), p. 36 and 37": "baldadig, driest, lichtvaardig, lichtzinnig/onberaden, onbesuisd, onbezonnen, vermetel/waaghalzig".
[73] Par. 25(2) BBBB, Hoge Raad 19 december 1990, nr. 25 301, BNB 1992/217, Hoge Raad 12 juni 1976, nr. 17 879, BNB 1976/199.
[74] A-G Groeneveld, FISCAAL BESTUURSRECHT; Boete. Begrip pleitbaar standpunt. Mate van verwijtbaarheid, V-N 2002/34.7, par. 4.3.
[75] Gerechtshof Arnhem 22 july 2004, V-N 2005/9.6, NTFR 2004, 1392, nr. 01/02257, par. 12.
[76] Hoge Raad 7 februari 2010, LJN BU2879.

stating that defendant had not been nonchalant or negligent when acting as he had been conscious about his duties as a 'securer' at all times. The Court of Appeal did not find gross or considerable negligence, and the death of the victim could not sufficiently be attributed to the act of the defendant. The Court of Appeals accounted for the fact that the defendant, as a professional in the field, disconnected his rope attached to the victim 'in auto-pilot-mode when his friend returned back to the ground. The High Court confirmed the decision of the Court of Appeals.

- *(Gross or Considerable) Carelessness II*

In this case the High Court agreed with the Court of Appeals[77] in the finding of a considerable degree of attributable carelessness (establishing negligence) with the defendant, which was deduced from evidence: defendant had made a unusual maneuver which contradicted traffic regulation as he speedily backed up a car at an intersection, resulting in defendant fatally hitting a cycler with his car.

- *(Gross or Considerable) Carelessness III*

Attributable negligence was also established in the *Machinist*-case[78]: the Court of Appeals found that defendant did not act responsible as required for a safe execution of his function as he had been highly careless and inattentive when he had failed to notice six warnings signs, was tardy in pumping the brakes and did not follow an instruction, which ultimately lead to the death of one victim and caused severe physical damage to another.

- *Recklessness*

In 2012 the High Court set aside a decision of the Court of Appeals[79] where the Court of Appeals found recklessness for the establishment of negligence: the Court of Appeals had defined recklessness as severe careless behavior where unacceptable risks are taken and continued by stating that recklessness requires a severe lack of carefulness. The level of negligence is determined by assessing the behavior of the defendant, the nature and severity of the act or omission and the surrounding circumstances of the case. The level of negligence cannot be deduced (merely) from the severity of the consequences. The High Court found that by proving severe, or rather considerable inattentiveness, carelessness and negligence are not sufficient for concluding recklessness for the establishment of negligence without further motivation.

3.4 Summary

In this chapter the author has discussed the notions of negligence, conditional intent and finally gross negligence. In summary:

- Negligence under Dutch and common law requires the existence of a duty of care, a breach of this duty of care, harm and the breach being the proximate cause of this harm. Negligence and the duty of care depend on various factors, such as the proximity

[77] Hoge Raad 17 september 2002, NJ 2002, 549.
[78] Gerechtshof Arnhem 12 juni 2009, LJN BI8313.
[79] Hoge Raad 22 mei 2012, LJN BU2012, NJ 2012, 488.

to the harm caused by the respondent/defendant, the special relationship between parties necessary for the establishment for a duty and standard of care, the question as to whether the harm was reasonably foreseeable for the respondent, whether due care was exercised by a reasonable and prudent person under the same or similar circumstances to avoid or minimize risk or harm to others and also whether it is 'just and fair' to attach a duty of care to the respondent;

- Gross negligence (*grove schuld*) may not be '*serious culpable negligence'* exactly, but establishing gross negligence could help determine a necessary level of culpability for the establishment of '*serious culpable negligence',* as negligence is defined as an act or omission thus "unacceptable" it borders on intent (hereby also emphasizing the fact that there is a thin line between conditional intent and gross negligence[80]); and
- Conditional intent is the lowest form of intent, thus does not apply in a case of '*serious culpable negligence*'. But the requirements establishing conditional intent can be valuable for the interpretation of the 'roof' for situations where one wants to establish '*serious culpable negligence'*. Conditional intent requires a considerable likelihood at a particular result, the conscious acceptance of the considerable likelihood of that result and where the considerable likelihood was known to defendant during an act or omission.

These notions will be applied in the conclusion (chapter 6) for an interpretation of '*serious culpable negligence'*, as to be applied by the AP.

[80] Schutte, N.J., *Fiscale Boetes bij fraude*, Dossier onderneming, Financiering en Recht, Vol. 45, 2001, p. 52 and Keiler, J. (2014), p. 139.

Chapter 4 Determining culpability through the application of the culpability score as laid down in Chapter Eight of the US Federal Sentencing Guidelines

4.1 Introduction

This chapter starts with a discussion on the FTC's manner of enforcement of consumer's privacy rights in the US, in particular the competency of the FTC to impose a fine on organizations for violating either a cease-and-desist or consent order[81] with the aid of a sentencing court. The sentencing court can consult Chapter Eight of the Federal Sentencing Guidelines (hereafter: FSG)[82] as it provides guidelines for the calculation of fines for organizations in violation of the law. The FSG includes three main methods for the calculation of fines[83]. The first method is linked to offenses of organizations who operate primarily for a criminal purpose or by criminal means. The second method applies to all organizations that do not operate primarily for a criminal purpose or by criminal means. The rules for calculating the fine range under this methodology (§§8C2.2 through 8C2.9 of the FSG) are limited however to offenses specifically-enumerated in §8C2.1(A) and (B) of the FSG, offenses which are all laid down in Chapter 2 of the FSG. The third and final method for determining a fine applies to counts not covered by the two aforementioned methods.

Most relevant for the interpretation and application of '*serious culpable negligence'* by the AP is the second fine determining method under the FSG: this method includes the seriousness of the offense and the result of a culpability score to determine the fine (range). The FSG, together with guidelines to the FSG, indicate which practices could be aggravating or mitigating factors for the establishment of either the level of seriousness of the offense, the culpability score and thus the fine to be levied. The aggravating or mitigating factors influencing the culpability score in particular could help establish a relevant level of culpability for the establishment of '*serious culpable negligence*'.

This chapter is outlined as follows: first the author will introduce the FTC and its competencies relevant to the enforcement of consumer's privacy rights, in particular the competency to indirectly impose a fine. Hereafter the author will discuss the guidelines for the calculation of fines relating to the second calculation method of the FSG, as laid down in §§8C2.1 through 8C2.9 of the FSG and conclude this chapter with what we might be able to deduct from the (guidelines to the) FSG when for the interpretation of '*serious culpable negligence'*.

[81] Federal Trade Commission Act 1914, hereafter: FTC Act, FTC Act, Sections 5(l) and 5(m).
[82] United States Sentencing Commission Guidelines Manual 2015, Chapter Eight – Sentencing of Organizations.
[83] See §8C1.1, §8C2.1 and §8.C2.10 of the FSG respectively.

4.2 When is the FTC competent to impose a fine for the enforcement of consumer's privacy rights?

The FTC involvement in consumer privacy issues started in 1995 after having been established in 1914 to ensure fair competition in commerce[84]. The expansion of the FTC's jurisdiction to prohibit "unfair or deceptive acts or practices" in addition to "unfair methods of competition" was completed after US Congress passed the Wheeler-Lea amendment to the FTC Act[85]. From the late 1990s, members in specific industries in possession of particularly sensitive information (such as health care providers and financial institutions) were obliged to safeguard consumer sensitive information as well, through Statutes such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Act of 1999 (GLBA) respectively[86].

Initially, the FTC promoted industry self-regulation to combat threats to consumer privacy (such as through the publication of privacy notices/policies on websites and via enforcement of those privacy policies[87]). After having assessed the effectiveness thereof, the FTC reported to Congress that said approach was not working. Since then, the FTC has applied Section 5 of the FTC Act to enforce consumer protection[88].

Section 5(a) of the FTC Act is the general statute for the enforcement of consumer protection, providing that "unfair or deceptive acts or practices in or affecting commerce…are…declared unlawful"[89]. As discussed prior in chapter 2 of this thesis, "unfair" practices are those acts or omissions that "cause or are likely to cause substantial injury to consumers (harm) which are not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"[90]. This definition of "unfair" practices is embedded in Section 5(n) of the FTC Act, after codification of the *1980 Unfairness Statement* by the FTC

[84] Hartzog, W., Solove, D.J., *The FTC and the New Common Law of Privacy* (August 15, 2013), 114 Columbia Law Review 583 (2014): GWU Legal Studies Research Paper No. 2013-120; GWU Law School Public Law Research Paper No. 2013-120 (hereafter: Hartzog, W., Solove, D.J., (2014)), p. 598, Hoofnagle, C.J., (2016-2), p. 3, Maher, A.V., Fair, L., *The FTC's Regulation of Advertising*, 65 Food and Drug Law and Regulation 589 (2010) (hereafter: Maher, A.V. (2010)), p. 590.

[85] Hartzog, W., Solove, D.J., (2014), p. 598, Hoofnagle, C.J., (2016-2), p. 35 and 37-38, Ohlhausen, M.K, (2015), p. 25.

[86] Zetoony, D.A., *The 10 Year Anniversary of the FTC's Data Security Program: Has the Commission Finally Gotten Too Big for Its Breaches*?, Stanford Technology Law Review, 2011, 12 (hereafter: Zetoony, D.A., (2011)), p. 2.

[87] "Industry favored a self-regulatory regime, which consisted largely of what has become known as "notice and choice". For the "notice" part, companies began to include privacy policies on their websites, especially commercial ones…For the "choice" part, users were given some kind of choice about how their data would be collected and used, most commonly in the form of an opt-out right, whereby companies could use data in the ways they described in the privacy policy unless users affirmatively indicated they did not consent to these uses." Via Hartzog, W., Solove, D.J., (2014), p. 592 and 598, and Scott, M.D., *The FTC, the Unfairness Doctrine and Data Security Litigation: Has the Commission Gone Too Far*? (August 21, 2007), p.4 and 6.

[88] Stevens, G.M., *Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority*, Library of Congress. Congressional Research Service, CRS Report for Congress, R43723 (hereafter: Stevens, G.M., R43723), summary.

[89] FTC Act Sec. 5(a), 15. U.S.C. Sec. 45(a)(1) via https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority, consulted on July 25th, 2016.

[90] FTC Act 15 U.S.C. Sec. 45(n) via via https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority, consulted on July 25th, 2016 and Stevens, G.M., R43723, p. 3.

therein[91]. The *1983 Deception Statement* provides guidance for determining a deceptive practice or act[92]: the Statement deems unlawful those representations, omissions or practices likely to mislead a reasonable consumer under the circumstances about a material fact[93].

The FTC expanded the concept of unfair and deceptive practices in consumer protection to include processing of personal data by organizations in ways that are incompatible with the reasonable expectations of consumers[94]. From 2002 onwards, the FTC has brought several enforcement actions against organizations for allegedly having insufficient data security practices through either a deception or unfairness claim[95]: the FTC claimed deception where organizations misrepresented the security level that had been applied to consumer data, the FTC claimed unfairness where a company had used inadequate security to protect consumer information regardless of a lack of representations concerning the security level applicable to consumer information[96] and it has brought cases against organizations for not honoring consumer privacy expectations[97].

4.2.1 The FTC's authority to enforce consumer's privacy rights

The FTC has various competencies to pursue organizations who (allegedly) violate consumer's privacy rights[98]. General competencies of the FTC include the authority to *prosecute* "any inquiry necessary to its duties in any part of the United States", the authority to "*gather and compile* information concerning" and the authority to "*investigate* from time to time the organization, business, conduct, practices and management of any person, partnership, or corporation engaged in or whose business affects commerce…"[99]. Once the FTC has conducted an investigation and insofar the FTC has "reason to believe" that the law is violated, the FTC could initiate an action to enforce consumer protection[100]. When the FTC enforces substantive requirements of consumer protection provisions it can do so through either an administrative or a judicial process in a federal district court[101].

---

[91] Frechette, P.S., *FTC v. LabMD: FTC Jurisdiction Over Information Privacy is 'Plausible', but how far can it go?* (May 9, 2013.), American University Law Review, Vol. 62, No 5, 2013, p. 105 and Scott, M.D., *The FTC, the Unfairness Doctrine and Data Security Litigation: Has the Commission Gone Too Far?* (August 21, 2007), p.16.

[92] Ohlhausen, M.K, Okoliar, A., *Competition, Consumer Protection, and the Right (Approach) to Privacy* (February 6, 2015), Antitrust Law Journal (hereafter: Ohlhausen, M.K, (2015)) , p. 31-32.

[93] Ohlhausen, M.K, (2015), p. 32, Hartzog, W., Solove, D.J., (2014), p. 628, Serwin, A.B., *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices – Version 2.0* (December 31, 2010) (hereafter: Serwin, A.B., (2010)), p. 11-14 and Hoofnagle, C.J., (2016-2), p. 123.

[94] Maxwell, W.J., (2014), p. 65.

[95] Zetoony, D.A., (2011), p. 2.

[96] Petco and BJ's Wholesale Club Inc. cases, via Zetoony, D.A., (2011), p. 2.

[97] Hoofnagle, C.J., *Assessing the Federal Trade Commission's Privacy Assessments*, 14(2) IEEE Security and Privacy 58-64, March-April 2016 (hereafter: Hoofnagle, C.J., (2016)), p.1.

[98] https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority, consulted on July 25th, 2016 and Maxwell, W.J., (2014), p. 68-69.

[99] Emphasis's added. FTC Act Sec 3, 15 U.S.C. Sec 53 and FTC Act Sec. 6(a), 15. U.S.C. Sec. 46(a) via https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority, consulted on July 25th, 2016, and Hoofnagle, C.J., (2016-2)), p. 102 and 333.

[100] https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority, consulted on July 25th, 2016.

[101] Binkley, J.W., *Fair Notice of Unfair Practices: Due process in FTC Data Security Enforcement after Wyndham* (April 26, 2016), 31 Berkeley Technology Law Journal, Vol. 31 (hereafter: Binkley, J.W., (2016)), p.8 and Stevens, G.M., R43723, p. 5 and Hoofnagle, C.J., (2016-2)), p. 109.

The administrative enforcement process can take place through either a rulemaking procedure[102] or an adjudicative procedure. The FTC will make a primary determination on whether a practice violates the law (allegedly) in both procedures. The adjudicative procedure is the relevant procedure in this case as it can lead to the competency of the FTC to impose a fine (civil penalty)[103], which will be further discussed below.

4.2.1.a The Adjudicative procedure: complaint

The FTC is allowed to challenge "unfair or deceptive act(s) or practice(s) through an administrative adjudication procedure. Where the FTC has "*reason to believe*" that a person or entity has engaged in an unfair or deceptive act or practice and insofar it seems that the proceedings would be in the public interest[104], the FTC can issue an administrative complaint (Section 5(b) of the FTC Act) wherein it lays forth its charges relating to the alleged violations[105]. After a complaint has been lodged the respondent can choose to contest the charges or to settle on the charges. The adjudicative procedure can result in a cease-and-desist order but also a consent order for the (alleged) infringement of consumer's privacy rights, which in turn, when violated, can give cause to the FTC's fulfillment of its competency to impose a fine (civil penalty)[106].

- *Contesting the allegations in the complaint: cease-and-desist order*

If the respondent opts to contest the charges alleging a violation of the law, an administrative trial will ensue[107]. The dispute will be brought in for a hearing before an administrative law judge (hereafter: ALJ) who will make an initial decision on the case and can recommend either entry of a cease-and-desist order or dismissal of the complaint. If a violation of the law is found, the FTC will issue a cease-and-desist order instructing the respondent to refrain from continuing to engage in the unlawful practice. The ALJ's decision for the imposition of a cease-and-desist order can be appealed to the full Commission, which may modify or set aside the order if it finds that either new conditions of fact or law or the public interest so requires[108]. Both parties then get an opportunity to submit their opinions and argue orally in front of the full Commission. The respondent may appeal the final decision of the Commission, where the appeals court has full jurisdiction to enter a decree affirming, modifying or setting aside the Commission's order. The Appeal's court's judgment is final and can only be reviewed by the Supreme Court.[109]

[102] The rulemaking procedure is out-of-scope for this thesis as it is irrelevant for the practice of the imposition of fines relating to a violation of consumer's privacy rights.
[103] https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority, consulted on July 25th, 2016.
[104] https://epic.org/privacy/internet/ftc/Authority.html, consulted on July 24th, 2016, Hoofnagle, C.J., (2016-2)), p. 139.
[105] Hoofnagle, C.J., (2016-2)), p. 98-99, Maher, A.V. (2010)), p. 592.
[106] Hoofnagle, C.J., (2016-2)), p. 110.
[107] Maher, A.V. (2010)), p. 593, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority, consulted on July 25th, 2016.
[108] https://epic.org/privacy/internet/ftc/Authority.html, consulted on July 24th, 2016.
[109] Binkley, J.W., (2016), p.9, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority, consulted on July 25th, 2016 and Stevens, G.M., R43723, p. 6, Hoofnagle, C.J., (2016-2), p. 24 and 111 and Maher, A.V. (2010)), p. 593.

- *Settling on the allegations in the complaint: consent order*

The respondent can also opt to settle on the charges, where it will eventually agree on a final consent order. The content of a consent order differs largely from the allegations embedded in a complaint: the complaint identifies specific data security failures that are allegedly a violation of Section 5 of the FTC Act. Consent orders on the other hand impose general requirements to prevent violations of consumer's privacy rights. Consent orders usually include provisions requiring both internal and external auditing procedures (by independent agencies), training programs, regular reporting (duties) to the FTC[110] but also the implementation of reasonable data security measures (programs)[111]. The requirements laid down in the consent orders can last up to a period of twenty years, allowing the FTC to co-regulate (major) organizations over a longer period of time[112]. Opting for this route also means that the respondent waives all rights to a judicial review[113]. The final consent order will be publicized once the FTC has accepted the proposed consent order[114]. The final consent order becomes binding for the respondent sixty days after it has been served (in principal). A consent order binds the organization to mitigate and/or tackle the alleged violations practices [115] and to provide reasonable security protection (procedural and structural safeguards) to prevent violations of consumer's privacy rights[116].

Examples of consent orders

Asus (2016)
The order, as agreed upon with Asus, required the establishment and maintenance of a comprehensive security program (which is subject to independent audits for the upcoming twenty years), the notification of consumers regarding software update or other steps to protect themselves from security flaws, including an option to register for direct security notices, and prohibits the organization from misleading consumers about the security of company's products[117].

Wyndham (2015)
Wyndham was one of the first organizations to directly challenge the FTC's enforcement of data security practices under Section 5 of the FTC Act but eventually agreed to a settlement on the FTC charges[118]. The consent order required for example the establishment of a comprehensive information security

[110] Binkley, J.W., (2016), p.12, Hoofnagle, C.J., (2016), p.2.and Maxwell, W.J., (2014), p. 69.
[111] Binkley, J.W., (2016), p.13.
[112] Maxwell, W.J., (2014), p. 69, Hanson, J.B., *Liability for Consumer Information Security Breaches: Deconstructing FTC Complaints and Settlements*, 4 Shidler J.L. Com. & Tech. 11 (5/23/2008), part <32>, Hoofnagle, C.J., (2016-2), p. 114-115 and 167.
[113] Binkley, J.W., (2016), p.8.
[114] FTC Act Section 5(b) via https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority, consulted on July 25th, 2016.
[115] Maxwell, W.J., (2014), p. 68-69.
[116] Stevens, G.M., R43723, p. 7 and Maxwell, W.J., (2014), p. 69.
[117] https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put and *Consent Order No. 142 3156 FTC in the matter of ASUSTeK Computer, Inc., a corporation*., consulted on July 24th, 2016.
[118] https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment, consulted on July 25th, 2016.

program designed to protect cardholder data, annual information security audits for the certification of the organization's security program and maintaining safeguards in connection to its franchisees' servers. The requirements under the consent order are active for a period of twenty years[119].

BJ's Wholesale Club (2005)
The consent order required the establishment and maintenance of a comprehensive information security program (which includes administrative, technical and physical safeguards), an audit from a qualified, independent, third-party professional determining that its security program meets the standards of the consent order (every other year for twenty years) and compliance with standard book- and record keeping provisions[120].

Eli Lilly (2002)
The agreed upon consent order required the establishment of a four-stage information security program designed to establish and maintain reasonable and appropriate administrative, technical and physical safeguards to protect consumer's personal information against reasonably anticipated threats or hazards to its security, confidentiality or integrity and to protect such information against unauthorized access, use or disclosure[121].

It is notable that where the FTC has claimed deception or unfairness of a practice in organizations leading to an alleged violation of consumer's privacy rights, the FTC has barely litigated a single case. In most cases the FTC has agreed on consent orders with the respondents, sometimes even before a complaint has been filed before a district court[122]. Respondents opt for settlements perhaps because they can avoid a court proceeding, avoid admission of liability and wrongdoing (as the merits of the complaints will have gone without an assessment[123]) and possibly avoid any additional costs related to reputational damages[124]. Another consideration for settling is that the expected costs of settling and fulfilling the

[119] https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment, consulted on July 25th, 2016.
[120] https://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges and *Agreement containing Consent Order No. 0423160 FTC in the matter of BJ'S WHOLESALE CLUB, INC., a corporation*, consulted on July 24th, 2016.
[121] https://www.ftc.gov/news-events/press-releases/2002/01/eli-lilly-settles-ftc-charges-concerning-security-breach, consulted on July 24th, 2016.
[122] Petco and BJ's Wholesale Club Inc. cases, via Zetoony, D.A., (2011), p. 3, Binkley, J.W., (2016), p.2, Stevens, G.M., R43723, p. 7, Hoofnagle, C.J., (2016-2)), p. 111 and Hartzog, W., Solove, D.J., (2014), p. 610-611: "The FTC negotiates and settles the majority of actions it initiates through prescribed consent order procedures" and "The FTC has issued over 170 privacy-related complaints against companies. Yet virtually every complaint has either been dropped or settled. Only one case has yielded a judicial opinion.".
[123] Binkley, J.W., (2016), p.14.
[124] Hartzog, W., Solove, D.J., (2014), p. 610 and 613, Hoofnagle, C.J., (2016-2)), p. 111: "It avoids an extended bout of publicity during the administrative process…" and p. 166.

requirements of the consent order may seem less costly than the cost of litigation (financially, time-wise and expectation of to be put in effort in litigating the case)[125].

- *Civil penalties for violating consent and cease-and-desist orders*

If a cease-and-desist order is imposed following from the determination that a practice is (either) unfair and/or deceptive, and if respondent knowingly violates the final cease-and-desist order, then the FTC is able to engage in a civil suit in a district court seeking either a monetary penalty or other equitable relief for said violation under Section 45(m)(1)(B) of the FTC Act[126]. This does put a burden of proof on the FTC, requiring it to prove that the respondent had "actual knowledge that such act or practice is unfair or deceptive (violating the cease-and-desist order) and thus unlawful" under Section 5(a)(1) of the FTC Act[127]. If respondent violates any of the requirements laid down in a final consent order, the FTC can bring a suit in a district court as well if it wants to enforce the consent order and impose a civil penalty per violation[128]. The FTC will then have to prove noncompliance with that order[129].

The civil penalty per violation of any requirements laid down in the final consent order and the cease-and-desist order is capped at 40.000 USD[130]. The cap of 40.000 USD is the result of a recent fare adjustment, which also covers Sections 5(l) and 5(m)(1)(A) and (B) of the FTC Act (unfair or deceptive acts or practices). The new maximum fines apply to civil penalties assessed after August 1, 2016 and covers violations predating the effective date[131]. The actual fine will still depend on a fact-specific analysis of each case. When determining the fine the sentencing district courts should look at the Federal Sentencing Guidelines 2015 for guidelines. The process of fine determination is further discussed in the following par. 3.3.

[125] Binkley, J.W., (2016), p.13 and Hartzog, W., Solove, D.J., (2014), p. 611-613: "Settling with the FTC also allows for companies to eliminate the uncertainty and expense of lengthy negotiation and pretrial preparation and litigation.".

[126] Binkley, J.W., (2016), p. 9, Hoofnagle, C.J., (2016-2)), p. 114: where the FTC seeks civil penalties, it has to give the US Department of Justice 45 days to bring suit. If the Department of Justice does not take action, the FTC can bring a suit in its own name to seek civil penalties, for example were the respondent violates a final FTC order, Maher, A.V. (2010)), p. 593 and https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority, consulted on July 25th, 2016.

[127] FTC Act, Section 5(m)(1)(B); 15. U.S.C. Sec. 45m(1)(B) via https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority, consulted on July 25th, 2016: "the Commission typically shows that it had provided the violator with a copy of the Commission determination in question, or a "synopsis" of that determination."

[128] FTC Act, Section 5(l), Bartnick, W., Stegmaier, G.M., *Physics, Russian Roulette, and Data Security: the FTC's Hidden Data Security Requirements* (May 9, 2013.), George Mason Law Review, Vol. 20, No. 3, 2013, p. 690-691: "And [e]ach separate violation …[is] a separate offense, except that in a case of violation through continuing failure to obey or neglect to obey a final order of the Commission, each day of continuance of such failure or neglect shall be deemed a separate offense.", Maher, A.V. (2010)), p. 593 and Stevens, G.M., R43723, p. 6.

[129] Hoofnagle, C.J., (2016), p.6.

[130] FTC Act Section 5(b) via https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority, https://www.ftc.gov/news-events/blogs/business-blog/2016/06/civil-penalties-undergo-inflation-recalculation and Federal Trade Commission, 16 CFR Part 1: Adjustment to Commission Civil Penalty Amounts to Reflect Inflation as Required by the Federal Civil Penalties Inflation Adjustment Act; Interim Final Rule, June 30, 2016 via https://www.ftc.gov/policy/federal-register-notices/16-cfr-part-1-adjustments-commission-civil-penalty-amounts-reflect-0, consulted on July 25th, 2016.

[131] Federal Trade Commission, 16 CFR Part 1: Adjustment to Commission Civil Penalty Amounts to Reflect Inflation as Required by the Federal Civil Penalties Inflation Adjustment Act; Interim Final Rule, June 30, 2016 via https://www.ftc.gov/policy/federal-register-notices/16-cfr-part-1-adjustments-commission-civil-penalty-amounts-reflect-0, consulted on July 24th, 2016.

4.3 Chapter Eight of the FSG – Sentencing of Organizations: determining the fine on the basis of the seriousness of the offense and culpability score of the organization

The Federal Sentencing Guidelines (hereafter: FSG) came into effect on November 1, 1991 and was developed by the US Sentencing Commission[132]. The FSG provides guidelines for sentencing courts to establish a fine. The main purposes of the FSG are to self-monitor and police, strongly deter unethical acts and punish members or stakeholders of organizations who engage in unethical behavior[133]. Chapter Eight of the FSG aims at establishing sanctions that provide "just punishment, adequate deterrence, and incentives for organizations[134] to maintain internal mechanisms for preventing, detecting, and reporting criminal conduct"[135]. Application of the FSG used to be mandatory. But after the US Supreme Court declared the document unconstitutional in early 2005 and ordered the removal of the provision prescribing its mandatory use, the Supreme Court declared the document to be advisory instead[136]. The Supreme Court still requires sentencing courts to consider the provisions of the FSG when determining a fine, but the courts have the additional option to take various other circumstances into consideration as well[137].

Chapter Eight is based on several general principles, one of which is that "the fine range for any other organization[138] should be based on the seriousness of the offense and the culpability of the organization", which is specifically outlined in §§8C2.2 through 8C2.9 of Chapter Eight. Establishing the range of the fine consist of three consecutive steps: first, establish the base fine (through determination of the offense level), second, determine the culpability multipliers (after determining the culpability score)[139] and finally, apply the culpability multipliers on the base fine[140]. The three steps will be dealt with in the following paragraphs.

4.3.1 Establishing the base fine (seriousness of the offense)

The base fine is generally made of the seriousness of the offense (offense level)[141]. Once the offense level has been established, the offense level will be compared to a table converting the offense level to USD[142], resulting in the base fine.

---

[132] Ferrel, O.C., LeClair, D.T., Ferrel, L., *The Federal Sentencing Guidelines for Organizations: A Framework for Ethical Compliance*, Journal of Business Ethics, 1998, Vol. 17 (hereafter: Ferrel, O.C., et. al., (1998)), p. 354.
[133] Ferrel, O.C., et. al., (1998), p. 355.
[134] United States Sentencing Commission Guidelines Manual 2015, Chapter Eight – Sentencing of Organizations, p. 499-500: "a person other than an individual".
[135] United States Sentencing Commission Guidelines Manual 2015, Chapter Eight – Sentencing of Organizations, p. 499.
[136] *United States v. Booker*, 123 S. Ct. 785 (2005) via Finder, L.D., Warnecke, A.M., *Overview of the Federal Sentencing Guidelines for Organizations and Corporate Compliance Programs*, August 2005 (hereafter: Finder, L.D., Warnecke, A.M., (2005)), p. 2.
[137] Finder, L.D., Warnecke, A.M., (2005), p. 2.
[138] Any other organization than those operating primarily for a criminal purpose or primarily by criminal means, see United States Sentencing Commission Guidelines Manual 2015, Chapter Eight – Sentencing of Organizations, p. 499.
[139] Ferrel, O.C., et. al., (1998), p. 358.
[140] Finder, L.D., Warnecke, A.M., (2005), p. 7-8.
[141] Ferrel, O.C., et. al., (1998), p. 358.
[142] Finder, L.D., Warnecke, A.M., (2005), p. 8.

The *Introductory Commentary* in Chapter Eight clarifies that the "seriousness of the offense" is generally reflected by the greatest of the pecuniary (monetary) gain by the organization, pecuniary loss suffered by the victims or the amount portrayed in USD in the *offense level fine table* in §8C2.4 of the FSG[143]. Pecuniary gain is the before-tax profit gained by the organization as result of the (alleged) offense, a pecuniary loss is the monetary loss caused by the knowing, intentional or reckless acts of the organization. Each federal offense has been assigned to a corresponding offense level[144] and the table in §8C2.4 of the FSG links an amount in USD to the corresponding offense level.

4.3.2 Determining the culpability multipliers

Before determining which multipliers have to be applied to the base fine, the culpability score needs to be established. §8C2.5 of the FSG specifies how of the culpability score is calculated.

Three rationales apply to the culpability score: the first being that culpability within an organization will be higher as a result of the organizations involvement in or tolerance of the unlawful conduct by high-level personnel or those with substantial authority, such as where high ranking individuals have participated, condoned or willfully ignored the unlawful conduct[145]. The second rationale is that where the respondent is a large organization, participation in misconduct by management is increasingly seen as a breach or trust or abuse of position as management is expected to act in a professional manner. And thirdly, the culpability score will be higher in larger organizations as the risk of unlawful conduct increases wherever management's tolerance of unlawful conduct is pervasive[146]. All three rationales are (to various extents) embedded in the six aggravating or mitigating factors affecting the culpability score as seen in §8C2.5(a) through (g) of the FSG:

- The four aggravating factors are: involvement in or tolerance of misconduct as measured by the organizations size and the seniority of the wrongdoers, prior history of misconduct by the organization, violations of existing court orders by the organization and obstruction of justice[147](§8C2.5(b) through (e)) of the FSG:
    - *Involvement in or tolerance of criminal activity*: the larger the organization, the more points to be awarded to the culpability score (5 points to organizations with over 4999 employees, 4 points to organizations with over 999 employees, etc.) insofar either high-level personnel participated in, condoned, or was willfully

[143] United States Sentencing Commission Guidelines Manual 2015, Chapter Eight – Sentencing of Organizations, p. 499.
[144] Ferrel, O.C., et. al., (1998), p. 357.
[145] Background to §8C2.5 of the FSG, p. 525 and Ferrel, O.C., et. al., (1998), Vol. 17, p. 357-358 and United States Sentencing Commission Guidelines Manual 2015, Chapter Eight – Sentencing of Organizations, p. 502-503: *"High-level personnel" refers to those who have substantial control over the organization or those who have a substantial role in the making of policy within the organization. Examples are the director and the executive officers. "Substantial authority" refers to those who within the scope of their authority exercise a substantial measure of discretion in acting on behalf of an organization and includes high-level personnel. Those "willfully ignorant" of an offense are individuals who did not investigate the possible occurrence of unlawful conduct despite knowledge of circumstances that would lead a reasonable person to investigate whether unlawful conduct had occurred."*
[146] Background to §8C2.5 of the FSG, p. 525 and Finder, L.D., Warnecke, A.M., (2005), p. 9.
[147] This includes toleration of misconduct by organizations, via Ferrel, O.C., et. al., (1998), Vol. 17, p. 355-356.

ignorant of the offense or if tolerance of the offense by substantial personnel was pervasive throughout the organization (§8C2.5(b));
- *Prior history*: if "similar misconduct" has either been committed, or where criminal adjudication based on "similar misconduct" or civil or administrative adjudications based on two or more "similar misconduct" has taken place in a shorter time span, the more points to be awarded to the culpability score (§8C2.5(c));
- *Violation of an order*: if the violation of the order occurred through "similar misconduct" as the initial offense, a higher culpability score should be awarded (§8C2.5(d));
- *Obstruction of justice*: points are awarded for the obstruction of justice insofar the organization willfully obstructed or impeded, attempted to obstruct or impede, aided, abetted or encouraged obstruction of justice during the investigation, prosecution or sentencing of the offense or, with knowledge thereof failed to take reasonable steps to prevent such obstruction or impedance or attempted obstruction or impedance (§8C2.5(e)).

- The two mitigating factors are: the existence of an effective compliance and ethics program and self-reporting, cooperation with the authorities and acceptance of responsibility[148](§8C2.5(f) and (g)):
  - *Effective compliance and ethics program*: points can be deducted to the culpability score if there is an effective compliance and ethics program in place. This is not the case if, after having become aware of an offense, the organization unreasonably delayed reporting of the offense to the authorities and if there were high level personnel or substantial authority personnel in place who participated in, condoned, or was willfully ignorant of the offense. The point deduction will still be granted regardless if those responsible for the operations of the compliance and ethics program have direct reporting obligations to the authority; the compliance and ethics program detected the offense prior to discovery outside of the organization or before discovery was reasonably likely; the organization had promptly reported the offense to the appropriate authorities and those responsible for the operations of the compliance and ethics program in no way participated, condoned or were willfully ignorant of the offense (§8C2.5(f));
  - *Self-reporting, cooperation and acceptance of responsibility*: between a clear (recognized and affirmed) acceptance of responsibility of the misconduct to reporting to the authorities (prior to imminent threat of disclosure or state investigation and within reasonable prompt time after becoming aware of the threat), full cooperation in the investigation and a clear (recognized and affirmed) acceptance of responsibility of the misconduct, the organization is able to get various points deducted from the culpability score (the more actions taken on the front of reporting, cooperating with the authorities and taking responsibility for the misconduct, the more point deductions are available to the organization)(§8C2.5(g)).

[148] United States Sentencing Commission Guidelines Manual 2015, Chapter Eight – Sentencing of Organizations, p. 499 and Ferrel, O.C., et. al., (1998), p. 358.

Once the culpability score has been established, it is compared to a table to determine the minimum and the maximum multipliers (ranging from 0.05 to 4.00, see §8C2.6 through §8C2.8 of the FSG).[149].

4.3.3 Applying the culpability multipliers to the base fine to establish the fine range

After the Court has determined the culpability multipliers it can apply them to the "base fine" to produce the applicable fine range[150]. However, if the courts find "that there exists an aggravating or mitigating circumstance of a kind, or to a degree, not adequately taken into consideration by the Sentencing Commission in formulating the guidelines that should result in a different sentence than what has been suggested by the FSG", the courts are still allowed the go below or above the established fine range[151]. The FSG includes examples of which circumstances justify an increase or decrease to the established fine range[152].

After determining the fine range, the maximum fine to be imposed per violation will still be capped at 40.000 USD however, as of August 1, 2016, for consumer-related civil penalties[153].

4.4 '*Serious culpable negligence*': what can we learn from the method of fine determination of Chapter Eight of the FSG?

The sentencing courts can look to Chapter Eight of the FSG for guidelines for the establishment of a fine, once the FTC has initiated a civil suit for the violation of either a cease-and-desist or consent order by organizations[154]. As discussed in previous par. 4.3, one of the methods for determining a fine is based on the seriousness of the offense and the culpability score of the respondent organization[155]. What could we learn and possibly deduct from these guidelines for the interpretation of '*serious culpable negligence'*, especially if we look at the underlying rationales and the aggravating and mitigating factors for the establishment of the culpability score laid down in §8C2.5 of the FSG?

4.4.1 Recap: the rationales underlying and the six factors influencing the culpability score

According to the *Background* of §8C2.5 of the FSG the culpability scores are based on three interrelated rationales[156]:

---

[149] Finder, L.D., Warnecke, A.M., (2005), p. 9.
[150] Finder, L.D., Warnecke, A.M., (2005), p. 11.
[151] Finder, L.D., Warnecke, A.M., (2005), p. 12-13.
[152] Finder, L.D., Warnecke, A.M., (2005), p. 13.
[153] https://www.ftc.gov/news-events/blogs/business-blog/2016/06/civil-penalties-undergo-inflation-recalculation and Federal Trade Commission, 16 CFR Part 1: Adjustment to Commission Civil Penalty Amounts to Reflect Inflation as Required by the Federal Civil Penalties Inflation Adjustment Act; Interim Final Rule, June 30, 2016 via https://www.ftc.gov/policy/federal-register-notices/16-cfr-part-1-adjustments-commission-civil-penalty-amounts-reflect-0, consulted on July 24th, 2016.
[154] FTC Act, Sections 5(l) and 5(m).
[155] §§8C2.2-8C2.9 of the FSG (Chapter Eight).
[156] United States Sentencing Commission Guidelines Manual 2015, Chapter Eight – Sentencing of Organizations, p. 499

1. an organization is more culpable when individuals who manage the organization or those who have substantial discretion in acting for the organization participate in, condone, or are willfully ignorant of criminal conduct (referring to "high-level personnel" or "substantial authority personnel" as defined in the *Commentary* of §8A1.2 via the *Commentary* of §8C2.5 of the FSG);
2. the larger an organization is and their management becomes more professional, participation in, the condoning or willful ignorance of unlawful conduct by said management is increasingly a breach of trust or abuse of position; and
3. the larger the organization gets, the risk of unlawful conduct beyond that which is reflected in the instant offense increases whenever management's tolerance of that offense is pervasive.

The three rationales have been embedded in the factors influencing the culpability score (§8C2.5 of the FSG). The four factors increasing the culpability score are: involvement in or tolerance of misconduct as measured by the organization's size and the seniority of the wrongdoers, prior history of misconduct by the organization, violations of existing court orders by the organization and obstruction of justice. The two mitigating factors are: the existence of an effective compliance and ethics program and self-reporting, cooperation with the authorities and acceptance of responsibility.

Before we continue onto the final part of this chapter, which analyses what we can deduct from the rationales and factors affecting the culpability score under the FSG in relation to the interpretation of '*serious culpable negligence'*, a final remark relating to the inclusion of mentioned rationales and factors in the Fining Policy of the AP. We have learned that the Fining Policy of the AP includes no guidance or explanation whatsoever to determine '*(serious culpable) negligence'* or culpability. It does contain factors encompassing, relating or similar to the rationales and factors affecting the culpability score embedded in the FSG. For example, recidivism can make up a part in 'prior history' (which affects the culpability score) and the role "high-level personnel" or "substantial authority personnel" have played in a violation or the size of the organization (under the FSG) could play a part under the heading of "the nature and the extent of the violation" to be accounted for by the AP when establishing a fine[157]. Still, neither recidivism nor "the nature and the extent of the violation" help establish (*serious culpable) negligence* or culpability under the Fining Policy as they only grant cause for the establishment of a (higher) fine. It is thus important that we attempt to assess what we can deduct from the rationales underlying and factors affecting the culpability score in relation to the interpretation of 'serious *culpable negligence'*, which we will in the following subparagraph.

4.4.2 What can we deduce from the rationales underlying and the factors affecting the culpability scores when it comes to the interpretation of '*serious culpable negligence*'?

From the rationales we can deduce a few pointers: the US Sentencing Commission finds a higher degree of culpability when the violation is attributable to large organizations (the larger

[157] Articles 6.1(a) and 9.1.(a) of the Fining Policy of the AP.

the organization, the higher the burden of responsibility for compliance with the law). The US Sentencing Commission also finds that the attitude (level of tolerance) by "higher management"[158] towards noncompliance with legal provisions could also affect the culpability level. Finally, several of the factors that either increase or decrease the culpability score are linked to "higher management" participating in, condoning or being willfully ignorant of a law violation. If it is included into a factor, it usually means the culpability score will be increased.

Similar to the rationales, the AP could also apply several of the factors aggravating or mitigating the culpability score to narrow down the interpretation of '*serious culpable negligence'*, particularly, by using it to establish the applicable level of culpability for the interpretation of '*serious culpable negligence'*.

The first aggravating factor regarding involvement or tolerance (condoning or being willfully ignorant) of misconduct is linked to the size of the organization and the role "higher management" has played in relation to the law violation. Prior history, the second aggravating factor, shows that where similar misconduct has taken place in a (shorter) timespan, organizations are held to a higher degree of responsibility to prevent the law violation from happening again, or are otherwise awarded more culpability points. Proving a prior history "supports" the establishment of condoning (tolerance) or willful ignorance of law violations as the organization knew or should have reasonably known in this case that the law violation will most probably happen again. The AP could use prior history to hold organizations to a higher degree of responsibility and establish '*serous culpable negligence*' sooner where the organization could and should have reasonably taken measures to prevent the risk of the law violation from occurring or to mitigate the adverse effects but hasn't. The third aggravating factor, violation of an order, could be used in the situation where an alleged violation of the Wbp has been found, and the AP has given Binding Instructions to the organization so it gets the opportunity to mitigate the alleged violation of the law. The AP can establish '*serious culpable negligence*' more easily in this case where the violation of the law persists or where the violation occurs again, even though the organization could and should have reasonably taken measures to negate the situation of the law violation and to prevent the violation from happening again. The fourth and final aggravating factor, obstruction of justice, can also be applied to by the AP, finding '*serious culpable negligence'* sooner when the organization has violated the Wbp and the organization (insofar possible) willfully obstructs, impedes or attempts to obstruct or impede, aided, abetted or encourages obstruction in the process of sanctioning during investigation or when imposing a fine or where the organization, with knowledge thereof, failed to take reasonable steps to prevent the obstruction or impedance or attempted obstruction of impedance.

The FSG includes two mitigating factors to the culpability score. Having an effective compliance and ethics program is the first. By analogy, where the AP establishes that the organization, even though they violated the law, had an effective compliance and ethics program in place, will less

[158] With "higher management" I am referring to the definitions of "high-level personnel" and "substantial authority personnel" as defined in the *Commentary* of §8A1.2 via the *Commentary* of §8C2.5 of the FSG

likely be deemed '*serious culpably negligent*'. However, if the organization has unreasonably delayed reporting of the offense to the AP once it became aware of the law violation and where "higher management" participated in, condoned, or was willfully ignorant of the law violation, the AP could find 'negligence' or '*serious culpable negligence'* nonetheless. For example, in a situation where a law violation has occurred and it concerns sensitive personal data, where the organization knew that timely notification of the law violation with the authorities and the data subjects could give them more time to take measures to mitigate and prevent any adverse consequences relating to the law violation, and the organization could have reasonably made a timely notification but didn't, the AP can more easily establish the organization was '*serious culpably negligent*'. The final mitigating factor could be applied in reverse to show '*serious culpable negligence'*: the AP can determine that, where a violation of the law occurred and the organization seems to take no clear responsibility for the violation (perhaps it continuously tolerates the risk of the law violation as it takes no reasonable measures to prevent the law violation or does not aid in mitigating the adverse consequences relating to the law violation), where it does not cooperate with the AP in the investigation process and where the organization does not report law violations to the AP where it could and should (have) in a timely manner (perhaps because it doesn't have an incident detection system in place where it reasonably should have), the AP could establish 'negligence' and perhaps even '*serious culpable negligence'* where circumstances allow it.

Chapter 5 What might the effect be of the application of '*serious culpable negligence*' of art. 66 Wbp on the organization of privacy compliance within organizations?

The connection between privacy and the organization of privacy compliance can be explained as: for privacy to exist, there has to be a sufficient level of security present within an organization[159]. And to be subjected to a direct and higher fine under art. 66 Wbp the respondent will need to be at least *seriously culpable*.

Existing laws and regulations include provisions on behalf of data subjects to guarantee a certain level of data security ("appropriate measures").[160] Having appropriate measures in place to establish a certain level of data security is a first step, but compliance also requires due diligence, meaning a "reasonable effort made to satisfy legal requirements or to discharge legal obligations".[161] This reasonable effort includes the organization of the manner in which organizations will adequately protect the personal data and the processing of personal data[162] and managing this entire process persistently throughout the entire life cycle of the personal data (from collection/creation to deletion/destruction). Laws and regulations seem to be the most important driver for (initial) compliance efforts.[163]

Law enforcement has also been a driver for compliance efforts, as shown in the US where the FTC's enforcement actions were critical for the promotion of privacy practices amongst private-sector organizations[164] and in the UK: a research conducted by the UK's data protection authority, the Information Commissioner's Office (hereafter: the ICO), on the impact of civil penalties (Civil Monetary Penalties, hereafter: CMPs) it issued on organizations for violating

[159] Maxwell, W.J., (2014), p. 67, Hiller, J.S., Baumer, D.L., Chumney, W.M., *Due Diligence on the Run: Business Lessons Derived from FTC Actions to Enforce Core Security Principles*, 45 Idaho Law Review 2009 (hereafter: Hiller, J.S. (2009)), p. 285.
[160] See for example: Article 13 Wbp: "passende technische en organisatorische maatregelen…", Recital 61 GDPR: "The protection of rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organizational measures are taken…", Recital 66 GDPR: "In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected.", Art. 22(1) GDPR: "The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this regulation.", Art. 26(1) GDPR: "…the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subjects…" and art. 30 GDPR: "The controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected…" and Hiller, J.S., (2009), p. 285.
[161] Breaux, T.D., Baumer, D.L., *Legally "reasonable" security requirements: a 10-year FTC retrospective*, Computers & Security 2011, p. 179.
[162] Terstegge, J., *Managen van Privacycompliance*, Privacy & Compliance 03/2013, p. 7.
[163] Ponemon Institute LLC, *The True Cost of Compliance: A Benchmark Study of Multinational Organizations*, January 2011, via http://www.tripwire.com/tripwire/assets/File/ponemon/True_Cost_of_Compliance_Report.pdf, p. 4 and Bamberger, K.A., (2010), p. 266.
[164] Hoofnagle, C.J., (2016), p.2.

provisions of the Data Protection Act 1998[165] shows on overall positive effect of CMPs on the the organization of privacy and data compliance.

The main purpose of the research conducted on the CMPs was to determine the extent to which the penalties influence or improve privacy and data protection compliance and practice by organizations.[166] The research findings strongly suggest that within organizations which were issued a fine, privacy and data protection duties were taken more seriously as they had effectively improved compliance with said duties. For example, they had revised their policies and practices, increased awareness on privacy and data protection amongst employees through training, and also, the interest for privacy and data protection increased with higher management.[167] The research also showed that within the group of "peer" organizations (who had not been issued a fine), the issuance of the CMPs worked as a deterrence with an added positive effect on privacy and data protection compliance within these organizations. For example, the issuance of civil penalties influenced the way the second group of organizations managed their duties under laws and regulations and it affected the importance it attached to privacy rights, such as by reviewing or altering their policies and practices.[168]

The question dealt with in this chapter is what the effect might be of the application of '*serious culpable negligence*' of art. 66 Wbp on the organization of privacy compliance within organizations. Unfortunately, the AP has yet to impose a fine based on art. 66 Wbp, let alone a fine which is (partially) based on '*serious culpable negligence'*, so the answer cannot be deduced from practical evidence. However, theoretically, the fact that the risk of a direct or a possibly higher fine as a result of established (gross/serious) negligence and serious culpability could incite organizations to organize (and/or manage) their privacy compliance. Why?

As discussed, the Wbp nor the Fining Policy of the AP provide a definition or guidelines for the establishment of '*serious culpable negligence*' or 'serious culpability'. And for the application of art. 66(4) Wbp the AP will need to establish both. Alternatively, we could apply the rationales underlying and factors influencing the culpability score as embedded in the US FSG to establish 'serious culpability', accounting for the role higher management has played in the condoning or being willfully ignorant of misconduct for example.

Even in cases where the AP can establish negligence and noncompliance with the Wbp, if the respondent has taken reasonable efforts to adequately protect personal data and the processing thereof and manages this process persistently throughout the life cycle of the personal data (has organized privacy compliance to a certain degree), the respondent can reduce the level of culpability attributable to the respondent, especially if higher management was involved in the implementation of these measures and the overall organization of effective privacy compliance. A reduced level of culpability can result in the avoidance of an immediate

[165] Information Commissioner's Office, *Review of the impact of ICO Civil Monetary Penalties*, 20140723 (hereafter: ICO Review CMPs 20140723).
[166] ICO Review CMPs 20140723, p. 1.
[167] ICO Review CMPs 20140723, p. 4 and 6.
[168] ICO Review CMPs 20140723, p. 4 and 7.

and a higher fine should the AP be unable to establish the minimum required level of culpability.

This thought aligns with the parliamentary history of why '*serious culpable negligence'* was added to art. 66 Wbp: to protect the private life when extraordinary situations require a punitive action because of the severity of the violation of the right to privacy life and the ease with which the violation could have been prevented (see chapter 2): if the respondent has taken (all) reasonable measures to adequately protect (the processing of) personal data and to prevent noncompliance with the law (by conducting privacy impact assessments, by training its employees on awareness of privacy and data protection, etc.) and noncompliance still occurs, the respondent should not be punished by being subjected to an immediate (and possibly higher) fine, but should be given the opportunity to negate the violation of the law (or to appeal the alleged violation) instead.

To conclude, theoretically, the inclusion of 'serious culpable' in '*serious culpable negligence*' could incite organizations to effectively organize (the management of) effective privacy compliance, as doing so might help them avoid an immediate and higher fine which they can be subjected to in accordance with art. 66 Wbp.

Chapter 6 Conclusion

This thesis aims to answer the following research question:

> What can we learn from the GDPR, Dutch tax- and criminal law and Chapter Eight of the US Sentencing Guidelines for Organizations for the interpretation and application of '*serious culpable negligence'* concerning the competency of the Dutch DPA to impose fines for the violation of provisions of the Dutch Data Protection Act? And what might the effect be of the application of 'serious culpable negligence' in this context on the organization of privacy compliance within organizations?

The research question will be answered in two parts:

- **The interpretation of application of '*serious culpable negligence'***

We have learnt that negligence stemming from Dutch and common law (chapter 3) requires the existence of a duty of care (which depends on whether it is 'just and fair' to impose a duty on the respondent), a breach of this duty of care (requiring the establishment of a standard of care), established harm and where the breach of the duty of care is the proximate cause of this harm. The standard of care applicable depends on whether the harm was reasonably foreseeable for the respondent and whether the respondent has exercised the same care as would have been exercised by a reasonable and prudent person under the same or similar circumstances to avoid or minimize risk or harm to others.

- Once the AP concludes noncompliance with the Wbp, the AP can start with its first assessment: whether there is a case of negligence through the application of these requirements. It will need to establish a duty of care, determine whether it is 'just and fair' to impose a duty of care, establish the applicable standard of care to establish a breach of the duty of care, establish harm and finally determine whether the breach of the duty of care was a proximate cause of said harm.

If the AP succeeds in its assessment and decides there is a case of negligence, it can continue with determining whether serious culpability is attributable to the respondent by applying the culpability score as laid down in Chapter Eight of the FSG (chapter 4).

- The AP could establish a similar method for calculating and establishing different levels of culpability which includes guidance as to which score(s) result in a high enough level of culpability to be deemed '*serious culpable'* in a case of noncompliance with the law. It its method it could look at the culpability score of the FSG and apply the same rationales and score aggravating or mitigating factors.

For further narrowing down either culpability or negligence, the AP could subject the case to a fairness test (chapter 2) to find further evidence for one of either notions: fair processing of personal data requires at least the provision of sufficient transparency (adequate information) towards data subjects so they can exercise their individual autonomy and to protect the legitimate interests of the data subject (EU) and also requires the assurance that consumers

have reasonable opportunity to make an informed decision so they might be able to avoid harm (US).

- The fulfillment of these requirements requires the organization and implementation of measures such as determining which data subjects it processes data from, determine the effective means to inform them adequately for sufficient transparency regarding the data processing and to actually effectively implement and execute these measures, part of a compliance program, which are required by law[169];
- Not having these effective measures in place will under the culpability score, as laid down in the FSG, not necessarily lead to a higher culpability score as having an effective compliance program can only lead to a lower culpability score. But where the AP establishes that the respondent has not taken any reasonable measures to protect the interests of the data subject, its personal data and the processing of personal data, the AP can conclude a breach of a duty of care (if the standard of care has been breached and insofar a duty of care exists and can be imposed), which is one step towards showing negligence.

To further narrow down an interpretation of '*serious culpable negligence'* the AP can also apply the underlying case to the requirements of conditional intent and gross negligence (*grove schuld*) stemming from Dutch tax- and criminal law (chapter 3): conditional intent requires a reasonable chance at a certain outcome, the conscious (subjective) acceptance of a reasonable chance of that outcome and where the reasonable chance was known to the respondent during the act or omission in question. Gross negligence is defined as the unacceptable act or omission bordering on intent (the lowest form in Dutch criminal law being conditional intent).

- Although gross negligence (*grove schuld*) does not necessarily equal '*serious culpable negligence*', the AP could apply both notions to the case, where establishing conditional intent does not change its competency to impose a fine as 'intent' leads to the application of art. 66(4) Wbp; but in the situation where conditional intent almost applies and the act fits in the description of gross negligence as well, it could point towards a level of negligence which borders intent, possibly supporting an assessment by the AP to possible hold the respondent to a more serious degree of culpability (and/or negligence).

This segment concludes the first part of the research question, showing that although the Wbp and the Fining Policy of the AP provide no guidance for the interpretation or establishment of serious culpable negligence, we could learn from the notions of negligence, conditional intent and gross negligence in Dutch and common law systems, Chapter Eight of the FSG and the principle of fair processing to narrow down an interpretation of '*serious culpable negligence'*.

[169] See for example the general obligation under art. 5(1)(a) GDPR: data processing shall be done in a transparent manner in relation to the data subject.

- **The application of 'serious culpable negligence' and effect on the organization of privacy compliance**

The second segment of this conclusions focusses on the second part of the research question, which questions whether '*serious culpable negligence'* as embedded in art. 66 Wbp has the capabilities to affect the organization of privacy compliance within organizations. The author has concluded that, although no practical evidence exists to support an answer, the inclusion the requirement of 'serious culpability' in '*serious culpable negligence'*, by organizing compliance management (namely taking reasonable measures to ensure the adequate protection of personal data, the processing of said personal data and the legitimate interests of the data subjects and where these measures are managed throughout the entire life cycle of the personal data, respondents should not be held to a degree of culpability high enough to establish '*serious culpable negligence'* when noncompliance with the law occurs. This thought is also supported by the Parliamentary history of the notion stating that it was included to protect the private life when extraordinary situations require a punitive action because of the severity of the violation of the right to privacy life and the ease with which the violation could have been prevented: respondent has taken all reasonable measures to adequately protect the legitimate interests of the data subject and should not be penalized for this noncompliance by being subjected to an immediate (and higher) fine. The inclusion of 'serious culpable' in this notion could thus be able to incite organizations to organize (and manage) their privacy compliance and it could help them avoid an immediate and higher fine as to be applied by the AP.

Bibliography

Books, articles, papers

Bamberger, K.A., Mulligan, D.K., *Privacy on the Books and on the Ground*, Stanford Law Review, Vol. 63, no. 247 (2010)

Bartnick, W., Stegmaier, G.M., *Physics, Russian Roulette, and Data Security: the FTC's Hidden Data Security Requirements* (May 9, 2013.), George Mason Law Review, Vol. 20, No. 3, 2013

Binkley, J.W., *Fair Notice of Unfair Practices: Due process in FTC Data Security Enforcement after Wyndham* (April 26, 2016), 31 Berkeley Technology Law Journal, Vol. 31

Breaux, T.D., Baumer, D.L., *Legally "reasonable" security requirements: a 10-year FTC retrospective*, Computers & Security 2011

Chandler, J. A., *Negligence Liability for Breaches of Data Security*, Banking and Finance Law Review, Forthcoming via http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998305

Christian, G.E., *A New Approach to Data Security Breaches*, Canadian Journal of Law and Technology, Vol. 7, No. 1, p. 149, 2009

Cuijpers, C., et al., *Een eerste verkenning van het Voorstel Verordening bescherming persoonsgegevens*, Computerrecht afl. 3 juni 2012

European Union Agency for Fundamental Rights, European Court of Human Rights, and Council of Europe, *Handbook on European Data Protection Legislation* (Publication Office of the European Union, Luxembourg, 2014)

Ferrel, O.C., LeClair, D.T., Ferrel, L., *The Federal Sentencing Guidelines for Organizations: A Framework for Ethical Compliance*, Journal of Business Ethics, Vol. 17, 1998

Finder, L.D., Warnecke, A.M., *Overview of the Federal Sentencing Guidelines for Organizations and Corporate Compliance Programs*, August 2005 via http://www.americanbar.org/content/dam/aba/publishing/criminal_justice_section_newsletter/crimjust_wcc_OVERVIEW_OF_THE_FEDERAL_SENTENCING_GUIDELINES_FOR_ORGANIZATIONS_AND_CORPORATE.authcheckdam.pdf

Frechette, P.S., *FTC v. LabMD: FTC Jurisdiction Over Information Privacy is 'Plausible', but how far can it go?* (May 9, 2013.), American University Law Review, Vol. 62, No 5, 2013

Hanson, J.B., *Liability for Consumer Information Security Breaches: Deconstructing FTC Complaints and Settlements*, 4 Shidler J.L. Com. & Tech. 11 (May 23, 2008), via

https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/412/vol4_no4_art11.pdf?sequence=1&isAllowed=y

Hartzog, W., Solove, D.J., *The FTC and the New Common Law of Privacy* (August 15, 2013), 114 Columbia Law Review 583 (2014): GWU Legal Studies Research Paper No. 2013-120; GWU Law School Public Law Research Paper No. 2013-120

Hiller, J.S., Baumer, D.L., Chumney, W.M., *Due Diligence on the Run: Business Lessons Derived from FTC Actions to Enforce Core Security Principles*, 45 Idaho Law Review 2009

Hoekendijk, M.G.M, *ZAKBOEK STRAFRECHT VOOR DE POLITIE 2015*, Kluwer

Hoofnagle, C.J., *Assessing the Federal Trade Commission's Privacy Assessments*, 14(2) IEEE Security and Privacy 58-64, March-April 2016

Hoofnagle, C.J., *Federal Trade Commission Privacy Law and Policy,* Cambridge University Press, 2016

Keiler, J., Panzavolta, M., Roef, D., *Criminal Law*, Introduction to Law, Springer 2014

Kuner, C., *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, Bloomberg BNA Privacy and Security Law Report (2012) February 6, 2012

Maher, A.V., Fair, L., *The FTC's Regulation of Advertising*, 65 Food and Drug Law and Regulation 589 (2010)

Maxwell, W. J., *Principles-based regulation of personal data: the case of 'fair processing'*, International Data Privacy Law, Vol. 5, No. 3, 2015

Maxwell, W.J., *Global Privacy Governance: A Comparison of Regulatory Models in the US and Europe, and the Emergence of Accountability as a Global Norm*, February 2014, via https://ec.europa.eu/digital-single-market/en/content/global-privacy-governance-comparison-regulatory-models-us-and-europe-and-emergence

Maxwell, W.J., *The notion of "fair processing" in data privacy law* (January 2, 2015), Quelle protection des données personnelles en Europe?, Céline Castets-Renard (ed.), University of Toulouse, Forthcoming, 2015

Meal, D.H., Cohen, D.T., *Privacy Data Security Breach Litigation in the United States*, in Privacy and Surveillance Legal Issues, Aspatore, p. 101-124, 2014

Ohlhausen, M.K, Okoliar, A., *Competition, Consumer Protection, and the Right (Approach) to Privacy*, February 6, 2015, Antitrust Law Journal, Forthcoming via http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2561563

Rhee, W. J., *The Tort Foundation of Duty of Care and Business Judgment* (2013). Notre Dame Law Review, Vol. 88, 2013, p. 1139+; U of Maryland Legal Studies Research Paper No. 2013-27

Schutte, N.J., *Fiscale Boetes bij fraude*, Dossier onderneming, Financiering en Recht, Vol. 45, 2001

Scott, M.D., *The FTC, the Unfairness Doctrine and Data Security Litigation: Has the Commission Gone Too Far?,* August 21, 2007

Serwin, A.B., *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices – Version 2.0*, December 31, 2010 via http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1733217

Sitsen, J.M, *Commentaar op Artikel 67d AWR Aanslagenbelastingen; opzettelijk niet, onjuiste of onvolledige aangiften doen* via http://www.ndfr.nl/link/W0178-67d

Sitsen, J.M, *Commentaar op Artikel 67e AWR Aanslagenbelastingen; door opzet of grove schuld te weinig belasting geheven* via http://www.ndfr.nl/link/W0178-67e

Sitsen, J.M, *Commentaar op Artikel 67f AWR Aangifte belastingen; door opzet of grove schuld (gedeeltelijk) te weinig belasting betaald* via http://www.ndfr.nl/link/W0178-67f

Stevens, G.M., *Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority*, Library of Congress. Congressional Research Service, CRS Report for Congress, R43723 via https://www.hsdl.org/?abstract&did=757894

Terstegge, J., *Managen van Privacycompliance*, Privacy & Compliance 03/2013

Tjong Tjin Tai, T. F. E., Koops, E. J., Op Heij, D. J. B., E Silva, K. K., & Skorvánek, I., *Duties of care and diligence against cybercrime*. Tilburg University, 2015

Zetoony, D.A., *The 10 Year Anniversary of the FTC's Data Security Program: Has the Commission Finally Gotten Too Big for Its Breaches?*, Stanford Technology Law Review, 2011

Other Materials

Information Commissioner's Office, *Review of the impact of ICO Civil Monetary Penalties*, 20140723 via https://ico.org.uk/media/about-the-ico/documents/1042346/review-of-the-impact-of-ico-civil-monetary-penalties.pdf

Ponemon Institute LLC, T*he True Cost of Compliance: A Benchmark Study of Multinational Organizations*, January 2011

Legislation and Related Texts

National Legislation

Algemene Wet inzake rijksbelastingen, *Stb*. 1959, 301

Beleidsregels van de Autoriteit Persoonsgegevens van 15 december 2015 met betrekking tot het opleggen van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2016), *Stcrt*. 2016, 2043

Besluit van 19 juni 2015, nr. BLKB2015/571M, *Stcrt*. 2015, nr. 17778 (Besluit Bestuurlijke Boeten Belastingdienst)

Besluit van 10 november 2015 tot wijziging van de bedragen van de categorieën, bedoeld in artikel 23, vierde lid, van het Wetboek van Strafrecht, *Stb*. 2015, 410

De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp): Beleidsregels voor toepassing van artikel 34a van de Wbp, van de Autoriteit Persoonsgegevens van 16 december 2015, *Stcrt*. 2015, 46128

Kamerstukken II 2014/15, 33662, nr. 13

Kamerstukken II 2014/15, 33662, nr. 15

Kamerstukken II 2014/15, 33662, nr. 16

Kamerstukken II 2014/15, 33662, nr. 22

Kamerstukken II 2014/15, 33662, nr. 24

Wet bescherming persoonsgegevens, *Stb*. 2000, 203

Wetboek van Strafrecht, Wet van 3 Maart 1881, *Stb*. 35

Wet van 4 juni 1992, houdende algemene regels van bestuursrecht (Algemene wet bestuursrecht), *Stb*. 315

Wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens en enig andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede de uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de

Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp), *Stb*. 2015, 230

European Legislation

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 and on the free movement of such data, Official Journal L 281, 23.11.1995

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 04.05.2016

Northern American Legislation

Federal Trade Commission Act 1914

Federal Trade Commission, 16 CFR Part 1: Adjustment to Commission Civil Penalty Amounts to Reflect Inflation as Required by the Federal Civil Penalties Inflation Adjustment Act; Interim Final Rule, June 30

United States Sentencing Commission Guidelines Manual 2015, Chapter Eight – Sentencing of Organizations

Case law and Related Texts

National case law

A-G Groeneveld, FISCAAL BESTUURSRECHT; Boete. Begrip pleitbaar standpunt. Mate van verwijtbaarheid, V-N 2002/34.7

Gerechtshof Arnhem 22 juli 2004, V-N 2005/9.6, NTFR 2004, 1392, nr. 01/02257

Gerechtshof Arnhem 12 juni 2009, LJN BI8313

Hoge Raad 19 februari 1985, NJ 1985, 633

Hoge Raad 19 juni 1911, W 9203

Hoge Raad 12 juni 1976, nr. 17 879, BNB 1976/199

Hoge Raad 19 december 1990, nr. 25 301, BNB 1992/217

Hoge Raad 15 oktober 1996, NJ 1997, 199/Ars Aequi AA19970438

Hoge Raad 17 september 2002, NJ 2002, 549

Hoge Raad 18 januari 2005, LJN AR1860/NJ 2005, 154

Hoge Raad 20 februari 2007, LJN AY9659

Hoge Raad 7 februari 2010, LJN BU2879

Hoge Raad 29 juni 2010, LJN BL5630

Hoge Raad 20 november 2010, LJN BN7726

Hoge Raad 3 december 2010, nr. 09/04514, NTFR 2010/2930

Hoge Raad 20 september 2011, nr. 10/01297, NTFR 2011/2323

Hoge Raad 22 mei 2012, LJN BU2012, NJ 2012, 488

Hoge Raad 29 mei 2015, V-N 2015/27.17, BNB 2015/146, NJB 2015/1268

Northern American case law

Agreement containing Consent Order No. 0423160 FTC in the matter of BJ'S WHOLESALE CLUB, INC. (2005)

Consent Order No. 142 3156 FTC in the matter of ASUSTeK Computer, Inc., a corporation (2016)

United States v. Booker, 123 S. Ct. 785 (2005)

Websites

http://www.americanbar.org/

https://autoriteitpersoonsgegevens.nl/

http://ec.europa.eu/

https://epic.org/

https://www.ftc.gov/

https://ico.org.uk/

http://www.ndfr.nl/

https://www.rijksoverheid.nl/

http://www.triplepundit.com/