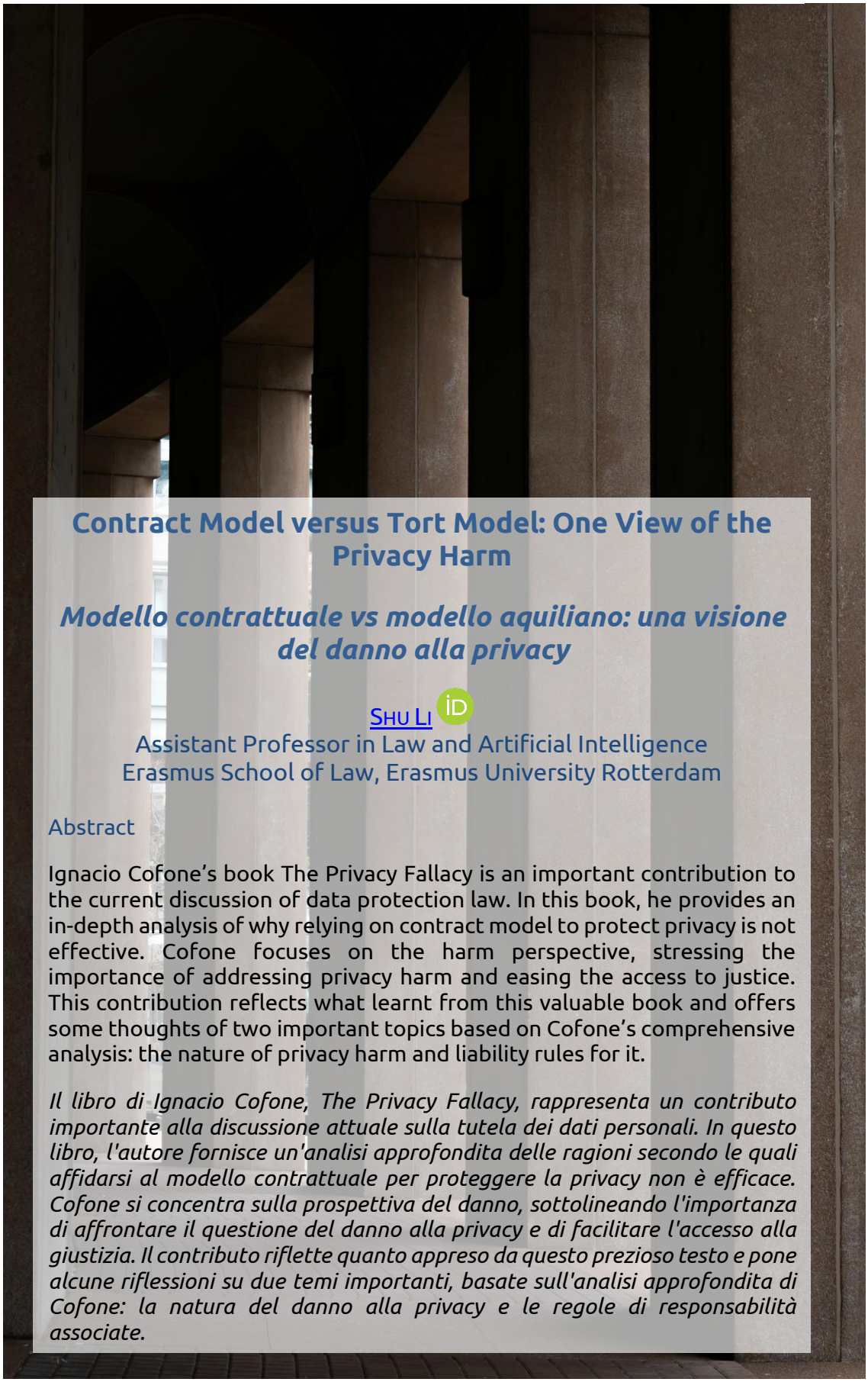
Li S, 'Contract Model versus Tort Model: One View of the Privacy Harm' (2025) 1 Special Issue EJPLT.
DOI: https://doi.org/10.57230/EJPLT251SL

EJPLT
ISSN 2704-8012



Contract Model versus Tort Model: One View of the Privacy Harm

Modello contrattuale vs modello aquiliano: una visione del danno alla privacy

Shu Li
Assistant Professor in Law and Artificial Intelligence
Erasmus School of Law, Erasmus University Rotterdam

Abstract

Ignacio Cofone's book The Privacy Fallacy is an important contribution to the current discussion of data protection law. In this book, he provides an in-depth analysis of why relying on contract model to protect privacy is not effective. Cofone focuses on the harm perspective, stressing the importance of addressing privacy harm and easing the access to justice. This contribution reflects what learnt from this valuable book and offers some thoughts of two important topics based on Cofone's comprehensive analysis: the nature of privacy harm and liability rules for it.

Il libro di Ignacio Cofone, The Privacy Fallacy, rappresenta un contributo importante alla discussione attuale sulla tutela dei dati personali. In questo libro, l'autore fornisce un'analisi approfondita delle ragioni secondo le quali affidarsi al modello contrattuale per proteggere la privacy non è efficace. Cofone si concentra sulla prospettiva del danno, sottolineando l'importanza di affrontare il questione del danno alla privacy e di facilitare l'accesso alla giustizia. Il contributo riflette quanto appreso da questo prezioso testo e pone alcune riflessioni su due temi importanti, basate sull'analisi approfondita di Cofone: la natura del danno alla privacy e le regole di responsabilità associate.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Privacy harm; tort liability; strict liability; full and effective compensation

Summary: 1. The problem of relying on contract model to protect privacy. – 2. The nature of privacy harm. – 3. Privacy harm: a descriptive or normative concept? – 4. Strict liability as a panacea of privacy harm? – 5. The future of privacy harm in the EU. – 6. Conclusion.

1. The problem of relying on contract model to protect privacy.

The story of *The Privacy Fallacy* starts from an important observation made by Cofone, which is 'data protection law became too focused on individual control and individual rights to exert control'.[1] While this contract-based model appears to respect personal option and autonomy regarding privacy in the first place, it results in opposite consequences in practice. The huge power and information asymmetry between service providers and users makes it extremely difficult, if not impossible, for the latter to make the choice that is free from harm.

In reality, the decision made by individuals is largely restrained by a person's knowledge and understanding of a risk.[2] 'One can only assume a risk when they actually understand the risk involved and can make choices that meaningfully change the risk levels'. [3] Cofone clarifies that such knowledge and understanding could be very few when the subject matter is privacy. There are multiple factors leading to this problem, ranging from the context where a privacy-related decision is made to the capability of estimating data's value as well as the risks and uncertainties around privacy.[4]

What is worse, the increasing adoption of deceptive design, or dark patterns, such as nagging and confirmshaming, makes it more difficult for individuals to make informed decisions regarding privacy. The situation becomes even worse, if we differentiate the users of online services. For example, children are more vulnerable under the contract model, as their knowledge of risk is fewer and they are more likely to be manipulated by deceptive design. Although dark patterns issues are more or less covered by data protection law (e.g., GDPR) and intermediaries regulation (e.g., DSA), their effectiveness has been questioned.[5] As Cofone rightly summarises, 'dark patterns aren't the disease'. Instead, 'they're a symptom of law's focus on individual control'.[6]

Cofone further identifies that the uncertainty of data processing adds another brick into the failure of merely relying on contract model to protect privacy. Individuals are unaware what happens after a click of consent and how

[1] I Cofone, The Privacy Fallacy: Harm and Power in the Information Economy (CUP 2023) 88
[2] Ibid 17.
[3] Ibid 32.
[4] Ibid 30-32.
[5] C Santos, V Morozovaite and SD Conca, 'No Harm No Foul: How Harms Caused by Dark Patterns Are Conceptualised and Tackled under EU Data Protection, Consumer and Competition Laws' (2025) 34(3) ICT Law, 1.
[6] Cofone (n 1) 44.

different options could improve the outcome. As a result, 'when people learn they can't manage their privacy effectively no matter how hard they try, they often stop trying'. [7] As Cofone precisely concludes, such a reaction of individuals does not represent that they do not care about their privacy at all. Nevertheless, a real consequence is that by clicking the 'consent' button, they meanwhile agree that they will bear the potential harm that they will otherwise avoid.

One specific case that Igancio uses to explain the failure of contract model is relational data. 'Information is relational in that it often describes interactions between people more than it describes discrete individuals'.[8] The relational nature of personal data also indicates the difficulty in using contract model to protect privacy. This nature has been observed in various types of personal data (e.g., biometric data) and its challenge to informed consent has been widely discussed in recent literature.[9] The question here is: How can a person consent the use of personal data that may infer and exploit the vulnerability of others? Individuals, however well they identify the risk when they click the 'consent' button, they are very unlikely to precisely estimate the potential externalities it may cause to other related individuals.[10]

Admittedly, the research on transparency and by design may improve the chance that an individual makes a desirable choice. The reality is that, despite how meaningful a mechanism is designed, it still relies on the assumption that individuals are able make the right choice about their privacy based on the improved mechanism. Therefore, I agree with Cofone's argument that merely focusing on giving individuals enough information and options may not address the problem rooted within the consent mechanism. Contract model will not guarantee that all of the costs that are externalised in the process of data processing will be fully internalised by the party that created the risk in the first place.

Two measures may help to correct the deterrence effect: one is exposing data controllers and process to high compliance costs and penalties; the second one is shaping their incentives by introducing proper liability rules. Data protection law, like GDPR, has been criticised for its anti-competition effect.[11] Recent years also witnessed a huge increase of fines for companies that failed to comply with data protection laws. The problem of penalty is that it highly relies on the assumption that authorities are able to identify the non-compliance incidents timely and to decide the amount of fines accurately. In reality, however, there are two essential problems if we simply rest on penalties. First, big companies may choose to harm, if the fines are substantially lower than the cost of adopting precautionary measures. Second, penalty only takes a role in deterrence, but it does not address the harmful consequences that have already occurred to impacted individuals. Therefore, understanding and addressing the actual privacy harm is of great importance.

[7] Ibid 35.
[8] Ibid 50.
[9] S Viljoen, 'A relational theory of data governance' (2021) 131(2) Yale L. J. 573-654.
[10] NA Smuha, 'Beyond the individual: governing AI's societal harm' (2021) 10(3) IPR 1-32.
[11] MS Gal and O Aviv, 'The competitive effects of the GDPR' (2020) 16(3) JCLE 349-391.

2. The nature of privacy harm.

When individuals click on the button of 'consent', they actually don't fully understand the consequence of doing so. This means that individuals may not take the harm into account and as a result, they may make excessive consents than they should have done. Meanwhile, service providers receive a signal that their activities will not be punished, as the harm is ultimately borne by impacted individuals. To correct this misallocation, it is crucial to identify and measure the privacy harm.

In private enforcement, a victim is normally tasked with the burden of proving the harm that they suffered. Unlike traditional accidents, such as car accidents, where harm is mainly in the form of personal injuries or property losses, identifying the concrete form of privacy harm is not easy. The direct result of data breach is that individuals *lose the control* of their privacy. If an individual cannot clearly claim the harm that they suffered at the moment of data breach, they may redress their harm, only at a later moment when the consequential harm of data breach becomes visible. In this sense, a successful claim is achieved, only if a financial loss or psychological consequence is evident. For example, third parties may misuse the leaked credit card information and steal money from data subjects. In this case, the harm is established and measurable with an objective price.

Against this background, one question that is not clearly addressed in theory and in practice is: Is the loss of controlling privacy or personal data *per se* recognised as harm? Literature has argued that risk and anxiety are eligible privacy harm. In a famous paper, Citron and Solove provide some meaning justification of why risk *per se* can and shall be recognised as harm.[12] As they argued, while harm is not materialised at the moment of data breach, the opportunity cost (e.g., such as the time and efforts that one monitors their account) is real.[13] In addition, data breach *per se* indicates a harm that 'involves a chilling of a person's ability to engage in life's important activities'. [14] Recognising risk as harm, however, is a huge step. This will not only generate profound influence on the conceptual system of tort law, blurring the distinction between risk and harm but also pose substantial challenges to downstream sectors, such as insurance industry. In addition, after recognising risk as harm, we may further ask: is the problem solved? That is, are individuals better compensated by recognising risk as harm? It is not clear how to measure the risk as harm at this stage. In the meantime, regarding risk as harm does not prevent subsequent harmful consequences at all. Individuals might suffer subsequent harm, when other misuse the leaked personal information.

The story for anxiety is different. Unlike risk, there is little controversy that anxiety falls under the scope of harm. It is by nature a kind of non-material harm, as it cannot be linked to an objective market value as medical bills or loss of salary. As non-material harm, the challenge for remedying anxiety is how to quantify it.

[12] DJ Solove and DK Citron, 'Risk and anxiety: A theory of data-breach harms' (2017) 96 Tex. L. Rev. 737-786.
[13] Ibid 758.
[14] Ibid 759.

3. Privacy harm: a descriptive or normative concept?

An important work accomplished by Cofone is that he further clarified the distinction between privacy loss and privacy harm. The loss of control of privacy immediately leads to privacy loss. In order to successfully claim such a loss, an individual needs to claim that this privacy loss is harmful.[15] This gap actually reflects the reasoning why judges from different jurisdictions, such as in the US and EU, are reluctant to recognise privacy harm merely based on the loss of control. Cofone further points out that this gap cannot be easily addressed, unless a clear understanding of what value Is reduced from a privacy loss Is achieved. According to Cofone, privacy harm is a normative term, which refers to 'the wrong of informational exploitation – profiting from someone's data while disregarding their wellbeing when in a position of power toward them'.[16] Cofone therefore concludes that the reason why privacy harm is underestimated in private enforcement is that judges fail to distinguish harmful loss of control from mere loss of control.

This distinction made by Cofone reminds me another important dichotomy in tort law: harm and damage. In tort law, harm refers to the disadvantage to individuals in nature, while damage refers to the harm in the eyes of law.[17] In this regard, there is also a normative evaluation in order to shift harm to compensable damage. In tort law, *protected interests* serve as the key factor of this transition. In theory, there is no doubt that certain interests deserve a high priority of protection. Such interests determine the quality of personal life (e.g., bodily integrity and property) and dignity (e.g., personality rights). In contrast, the protection of certain interests through tort law is not evident. One is economic benefits that individuals suffered due to a broken social or contractual relationship. Tort liability is normally reluctant to protect such interests, because there is a remote causal link between the harm and relationship. More importantly, the fact that tortfeasors can hardly estimate the existence of such a relationship makes it impossible for them to take measures to reduce the relevant costs.

Therefore, while Cofone takes a valuable step to penetrate the black box of harm by distinguishing mere loss of control and harmful loss of control, tort law scholars like me may wonder whether this distinction could to some extent covered by or separated from the dichotomy of harm and damage. If we admit the value of distinguishing descriptive loss and normative loss, then two normative assessments have to be embedded into tort theory. This may generate some confusion for judges and make the access to justice even more complex for individuals.

When it comes to the loss of controlling privacy or personal data, the majority of the literature accommodates it under the perspective of conceptualising harm. The key question is restricted to whether the loss of control or non-compliance of law can be recognised as harm? In my opinion, loss of control and non-compliance respectively touch upon different issues. The discussion on loss of control represents a matter of fact or, as Cofone mentions,

[15] Cofone (n 1) 125.
[16] Cofone (n 1) 123.
[17] F Busnelli, et al, *Principles of European Tort Law : Text and Commentary* (Springer 2005) 23.

a descriptive status. Therefore, its existence is independent of whether non-compliance happens. The core issue regarding loss of control relates to the determination of harm. In contrast, although non-compliance may result in loss of control, which further leads to harm, non-compliance *per se* has nothing to do with harm issue. Rather, non-compliance is a signal of fault of service providers. The link between non-compliance and fault, however, is also problematic. I will explain why in Section 5.

4. Strict liability as a panacea of privacy harm?

Different from the contractual approach, where the accident cost is allocated through the agreement among contractual parties, tort liability directly allocate the cost by law. One expectation under tort liability is that even if an individual suffered information asymmetry and they are unable to estimate the potential harm caused to them, liability rules could provide tortfeasors with an incentive to behave properly. If we suppose that the recognition of privacy harm is settled and agree that tort liability may play a crucial role in addressing privacy harm, the following issue to be addressed is: Which liability rule should be introduced to protect privacy?

Cofone applies his extraordinary law and economics knowledge to analyse this issue. According to tort law and economics, the choice between strict liability and fault liability can be roughly decided through two factors: the level of care and level of activity.[18] In the digital context, the level of care can be understood as the efforts that relevant parties take to reduce data breach and potential harm. In comparison, the level of activity can be understood as the amount of data collection or frequency of such activities. In a specific context, whether strict liability or fault-based liability shall apply is normally determined by the answer to which party's level of care and level of activity shall be optimised. For this issue, Cofone has an explicit preference for strict liability, as 'victims can't prevent them from happening by taking precautions'.[19] In law and economics theory, one factor that makes strict liability preferrable lies in its potential to resolve information asymmetry.[20] In this sense, considering the power and information advantage of service providers, holding them liable will incentivise them to take every possible method to minimise the accident cost. since it will be the residual risk bearer, it will also be incentivised to alleviate such the accident cost even if the law does not mandate them to do so.

When proposing a paradigm shift from contract model to tort liability model, Cofone also points out the potential four objections. If we further focus on applying strict liability to privacy harm, additional four problems and objections deserve to be considered.

First of all, strict liability mainly aims to correct deterrence rather than guarantee compensation. In this sense, service providers, especially those small ones, may suffer the insolvency problem. In law and economics, this is also

[18] S Shavell, *Economic analysis of accident law* (Harvard University Press 1987).
[19] Cofone (n 1) 148.
[20] AM Polinsky and S Shavell 'The uneasy case for product liability' (2009) 123(6) Harv. L. Rev. 1437-1492.

called the 'judgment proof problem'.[21] When this problem happens, there is a risk that victims cannot be fully compensated. To address this matter, some mandatory financial security would be helpful. Traditionally, mandatory financial security is required in scenarios where mass harm occurs, such as natural disaster and environmental harm.[22] In the digital age, especially in privacy harm, there is little discussion. If we consider privacy harm as mass harm and intend to have relational harm and social harm compensated in tort law, we may consider the necessity and form of mandatory financial securities.

Secondly, insurability issue may incur, if we extend the scope of damage under strict liability. Under strict liability, damage will be ultimately borne by the tortfeasor. In the context of data privacy, if we extend the scope of harm (e.g., by recognising loss of control as harm) and damage (e.g., admitting relational harm as damage), service providers may take a risk of bearing a larger scale of uninsurable risks. A risk becomes less insurable under certain conditions. One typical example is that law is not clear about liability, i.e. concepts like damage and causal link are not explicitly determined by law or courts.[23] In this circumstance, insurers are reluctant to provide coverage (i.e., liability insurance). Therefore, when defining privacy harm, it is necessary to take its influence on risk-shifting into account as well. A smart move will be developing multiple risk-shifting mechanisms to allow service providers to shift their risk.

Thirdly, under strict liability, the cost of privacy harm may be further transferred back to impacted persons via price mechanisms. Once service providers purchased the coverage, they intend to further distribute the expense among users.[24] A typical example is that service providers include such costs directly into the subscription fee. Alternatively, a price mechanism could also work indirectly, such as by exposing users to more advertisements. As a result, digital service becomes more expensive, making it unaffordable to certain users. This unaffordability is not only due to the different financial situations among users but can also be understood as their different levels of tolerance of online advertisements and manipulation. In this sense, certain people bear the shifted costs by paying extra subscriptions, while others may choose to stay away. The increasing cost of digital services may thereby generate discriminatory effects among users, as their capacity to access services is different.

Fourthly, strict liability may not address the problem of relational harm. Contract model is criticised for its failure to obtain the consent from all impacted persons. Liability is considered to have the potential of correcting this problem by requiring service providers to internalise the cost caused to all impacted persons via strict liability. As aforementioned, the first obstacle lies in the concept of harm, i.e., whether relational harm could be defined as tort damage. This is a normative issue, which requires an extension of tort damage. In addition to the perspective of damage, there is a crucial assumption that is

[21] S Shavell 'The judgment proof problem' (1986) 6(1) Int. Rev. Law Econ. 45-58.
[22] T Arons and R Rijnhout, *Mass Harm in Europe: Compensation and Civil Procedures* (Intersentia 2023).
[23] MG Faure 'The limits to insurability from a law and economics perspective' (1995) 20(77) GENEVA PAP R I-ISS P 454-462.
[24] S Li and MG M Faure 'The Revised Product Liability Directive: A Law and Economics Analysis' (2024) 15(2) JETL 140-171.

not evidently established. That is, whether the relational harm could be accurately assessed. In other words, if service providers are not the least cost avoider to reduce such costs, the deterrence provided by strict liability to them will be inefficient. People may still argue that service providers may still be an appropriate party to bear the risk as they are the best party to shift the risk (e.g., through liability insurance). Then, a distribution problem may come to the scene, as the cost will be redistributed to users through price mechanisms. If the cost is determined on average and equally distributed to all users, certain users whose processed data are less relational may have to pay a higher price than they actually should do.

5. The future of privacy harm in the EU.

Rightly after the book was published, a number of judgments relating to redressing the privacy harm were delivered by the Court of Justice in the European Union (CJEU). This simply indicates what Cofone discusses is a highly timely and relevant work that the legal community should address sooner than later.

The recent cases referred to the CJEU centre on the interpretation of Article 82 GDPR, which specifically addresses the right to compensation and liability. According to this article, 'Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered'. In this case, Article 82 provides data subjects with an approach to claim their damage resulting from data processing activities. However, it remains unclear in several key issues, such as the definition and scope of damage and the liability rules used for redressing the damage.

Regarding the concept and scope of compensable damage, the CJEU in *Österreichische Post* explicitly interpreted that merely violating GDPR rules or misuse of personal data is not considered as harm, so it does not give rise to a right to compensation as Article 82 defines.[25] A person must claim the concrete material or non-material damage. One harm that was recognised by the CJEU is the *fear* of the misuse of personal data.[26] When harm is established, the CJEU clarified that the severity of harm does not matter. In other words, the Member States shall not set up threshold for the compensability of harm, no matter how trivial it is.[27] The CJEU also requires the Member States to ensure the compensation is full and effective. Nevertheless, instead of setting up a ground that all Member States are obliged to follow, the CJEU allowed all Member States to consider their own situation to achieve this objective.

Another important development of the CJEU cases is clarifying the liability rules for privacy harm. For a long time, there were disputes regarding whether Article 82 is based on strict liability or fault liability.[28] This question was

[25] C-300/21 *Österreichische Post* [2023] ECLI:EU:C:2023:370.
[26] C-340/21 *Natsionalna agentsia za prihodite* [2023] ECLI:EU:C:2023:986.
[27] C-687/21 *MediaMarktSaturn* [2024] ECLI:EU:C:2024:72.
[28] See for example, R Strugala 'Art. 82 GDPR: Strict liability or liability based on fault?' (2020) Special Issue EJPLT, 71-79; J Knetsch 'The compensation of non-pecuniary loss in GDPR infringement cases' (2022) 13(2) JETL,132-153.

referred to the CJEU in *Krankenversicherung Nordrhein*.[29] In the final judgment, the CJEU interpreted that 'Article 82 of the GDPR must be interpreted as meaning that, first, the establishment of liability on the part of the controller is subject to the existence of a fault committed by the controller, which is presumed unless the controller proves that the event giving rise to the damage is in no way attributable to it and, secondly, Article 82 of the GDPR does not require the degree of seriousness of that fault to be taken into account when determining the amount of damages awarded as compensation for non-material damage on the basis of that provision.'[30] In this regard, the CJEU made it clear that the claim for privacy harm must be based on fault liability, while the defendant has the burden to prove that the damage was not caused by their fault. The CJEU reasoned that strict liability is not suitable, as it will not attain the legal certainty pursued by the GDPR.[31]

The recent development in the EU seems to show a quite different picture that Cofone has suggested in his book. On the one hand, the CJEU made it clear that the loss of control *per se* is recognised as harm. A claimant needs to further prove the existence of actual harm, such as the fear that their personal data will be misused. On the other hand, the CJEU specified that a claimant shall rely on fault liability rather than strict liability to compensate their harm. However, it must be noted that the CJEU cases also showed a careful balance toward the aforementioned two issues. First, treating the fear of data misuse as harm is a relatively low bar for conceptualising harm. Second, the fact that the defendant takes the burden to prove that the damage was not caused by their fault indicates that the CJEU may also not believe that a pure fault-based liability is the future of liability rules for privacy harm.

Relying on a pure fault liability to compensate privacy harm may generate two problems. First, how to define the duty of care in privacy law? One way is equalising duty of care with regulatory compliance, meaning that if a service provider meets all relevant rules and principles laid down in the data protection law, it has no fault. This approach is highly problematic. By doing so, the incentive of internalising accident cost by a service provider is essentially determined by the issue of whether regulators are able set up the due care level at the optimal level and whether courts can accurately assess the actual care level taken by the service provider. In data society, compared with service providers, regulators and judges obviously suffer a higher level of information asymmetry. Secondly, under fault liability, data subjects as the residual risk bearer should have the incentive to take measures to prevent harmful consequences. However, whether they have the incentive or capability to take relevant measures is questionable. This problem is also identified by Cofone, who argued that individuals may not even realise the necessity of taking relevant preventive measures, such as privacy-enhancing precautions.[32]

[29] C-667/21 Krankenversicherung Nordrhein [2023] ECLI:EU:C:2023:1022.
[30] Ibid para103.
[31] Ibid para100.
[32] Cofone (n 1) 32.

6. Conclusion.

The Privacy Fallacy is the first book that systematically analysed the approach to address privacy harm. This is not an easy topic, as it has to touch upon a number of fundamental issues beyond the area of privacy law, such as whether an increase of risk *per se* can/should be considered as harm and whether strict liability or fault liability should apply. Cofone in this book provides insightful idea on these fundamental questions in the context of privacy law. He not only sets up the scene of different standpoints and approaches but also gives an all-round evaluation of them. This book provides enough food for scholars and practitioners who follow the recent legal development and aware the same questions. The work done by Cofone is fundamental. Now when people stand in front of privacy context, we may hear a voice: Hey, there are two visions of the same thing! Therefore, I highly appreciate the hardwork and in-depth analysis carried out by Cofone and highly recommend The Privacy Fallacy to all!