

The power of civil liability to address harms in the information economy on the current weaknesses of digital constitutionalism

Il potere della responsabilità civile per affrontare i danni nella società dell'informazione nelle debolezze del costituzionalismo digitale

[PAULINE TROUILLARD](#) 

Fellow in Public Law, CNRS Université Paris Nanterre
Associate Fellow, Information Society Project, Yale Law School

Abstract

The wave of different regulations adopted by the European Union and aiming at regulating platforms' power have been coined by some authors as "digital constitutionalism". In this article, I argue that Cofone's book highlights the limits of digital constitutionalism, understood both descriptively and prescriptively. Descriptively, Cofone's book highlights the fact that consent is not a constitutional tool, even if accompanied by tools reminiscent of the rule of law. It also shows that these procedural tools are not sufficient to limit platforms' power, as a Constitution should limit the State's power. Prescriptively, Cofone's book shows that civil liability is better equipped to protect users' interests, by taking into account the difference of power between users and platforms. Finally, I argue that constitutionalism can be a useful tool if it helps ensuring democratic choices in the digital sector, through a democratic governance framework.



Abstract

L'ondata di normative adottate dall'Unione Europea e volte a regolare il potere delle piattaforme è stata definita da alcuni autori "costituzionalismo digitale". In questo articolo, sostengo che il libro di Cofone evidenzia i limiti del costituzionalismo digitale, inteso sia in senso descrittivo che prescrittivo. Dal punto di vista descrittivo, il libro di Cofone evidenzia il fatto che il consenso non è uno strumento costituzionale, sebbene sia accompagnato da strumenti che ricordano lo Stato di diritto. Mostra anche che questi strumenti procedurali non sono sufficienti a limitare il potere delle piattaforme, poiché una Costituzione dovrebbe limitare il potere dello Stato. Dal punto di vista prescrittivo, il libro di Cofone mostra che la responsabilità civile è più adatta a proteggere gli interessi degli utenti, tenendo conto della differenza di potere tra utenti e piattaforme. Infine, sostengo che il costituzionalismo può essere uno strumento utile se contribuisce a garantire scelte democratiche nel settore digitale, attraverso un quadro di governance democratica.

Keywords: Digital constitutionalism; Consent; Material constitutionalism; GDPR

Summary: [1. Introduction.](#) – [2. Consent is not a constitutional tool – and is not adapted to privacy law either.](#) – [3. Procedural rights are not sufficient to limit platforms' power in a sphere dominated by private law.](#) – [4. The limits of digital constitutionalism as a prescriptive claim.](#)

1. Introduction.

The General Data Protection Regulation (GDPR) has been adopted in the European Union in 2016 with great enthusiasm, especially from EU legal scholars. It was meant to regulate what Shoshana Zuboff has coined "surveillance capitalism"¹ - the harvesting of our personal data through the use of cookies by platforms in order to offer feed their algorithms and offer targeted ads to their users. The GDPR was the first omnibus text (applying to all sectors) aimed at regulating the collection and processing of data. It was also the first step of the development, in the EU, of legislative approaches for the regulation of the digital economy, that has been described by some authors as "European digital constitutionalism". Aimed at developing the fundamental right to the protection of personal data enshrined in the European Charter of Fundamental Right, the GDPR offers a set of obligations for the data collectors, and a set of rights for the users against certain uses. These uses include as use without consent, use that goes beyond the purposes originally given, or use once consent has been withdrawn. Despite this great enthusiasm, little or nothing changed in the early days, except maybe our experience as internet users, as cookie banners started to invade our screen. As the GDPR entered into force in 2018, Meta switched the legal basis from processing users' data to consent to contractual necessity.² It defined, in its terms of services, the

¹ S Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (2019)

² L Zard, 'Five Years of Illegitimacy of Surveillance Advertising', in RÁ Costello and M Leiser (eds.), *Critical Reflections on the EU's data protection* (2024)

provision of personal advertisement and targeted content as part in the performance of the contract, thus establishing data processing as a contractual necessity. In that sense, the GDPR was a legitimizing text, as it legitimized the collection and processing of our data by companies as soon as they could for one legal basis.³ The intervention of the European Commission and the ECJ in 2023, who reduced the use of the “performance of the contract” as a legal basis in *Meta v. Bundeskartellamt*⁴ has been beneficial.⁵ The ECJ limited the possibility for Meta to include the provision of personal advertisement as a contractual obligation, since Meta could provide its service without this personal advertisement. The ECJ also denied Meta the possibility to rely on the “legitimate interest” to collect and process its users’ data, thus forcing Meta to use the “explicit consent” to process them. In doing so, the ECJ implemented the GDPR’s initial ambition to detach consent from contract: it forced companies to offer a real alternative to users in their condition of use of the service. Meta responded by providing a new alternative to its users: either accept the collection and processing of data, or paying a price in order to use the service. But is this really an alternative? This cat-and-mouse game between the Commission, the ECJ and powerful platforms highlights the limits of the European regulation as it is designed nowadays.

In this context, Ignacio Cofone’s book, *The Privacy Fallacy: Harm and Power in the Information Economy* is an indispensable read to understand why consent and obligations of due process are not the appropriate legal framework to tackle data collection and secure the rights of the users. The book provides an alternative theoretical and practical framework that allows us to think about privacy protection in a more efficient way.

To qualify the new legislative developments expected to frame the power of private platforms, many authors employ the term “digital constitutionalism”.⁶ Digital constitutionalism is both descriptive and prescriptive.⁷ Descriptively, it attempts to bring together the various texts adopted by the European Union within a common label to give them meaning. Prescriptively, it calls for the use of conceptual tools linked to classical constitutionalism - the rule of law and fundamental rights - to analyze how these texts constrain the power of private platforms. Authors call for the concept of constitutionalism to be detached from its purely statist dimension, in order to appreciate the emergence of the powers of private actors and subject them to the law.⁸

In this brief comment, I would like to focus on the relationship between the critical legal framework that Cofone develops and digital constitutionalism. I would also like to show how Cofone’s normative proposition regarding the regulation of data could be transposed to all areas of digital law, and in

³ O Lynskey, *The foundations of EU Data Protection Law* (Oxford University Press 2015)

⁴ Judgment of 4 July 2023, *Meta vs Bundeskartellamt*, Case C-252/21, EU:C:2023:537.

⁵ N Guggenberger, 'Consent as Friction', (2025) 66 Boston College Law Review 353-421

⁶ E Celeste, 'Digital Constitutionalism: A New Systematic Theorisation', (2019) 33 International Review of Law, Computers & Technology; G De Gregorio, *Digital Constitutionalism in Europe: Reframing rights and powers in the algorithmic society* (Cambridge University Press 2022), A Iliopolou-Penot, *La Constitution Numérique Européenne*, [2021] *Revue Française de Droit Administratif*

⁷ De Gregorio, *Digital Constitutionalism in Europe*, 25.

⁸ The Rise of European Digital Constitutionalism, *supra* nt 6.

particular the use of Artificial Intelligence, content moderation and content amplification.

In the first two parts of this article, I will talk about digital constitutionalism's descriptive ambition. In the first part, I will talk about consent. The limits of consent as highlighted by Cofone in the first part of the book shows that consent is anything but a constitutional tool. In the second part, I will show that, as highlighted by Cofone, procedural rights are not enough to limit platforms' power in a sphere dominated by private law. In the third part, I will focus on digital constitutionalism's normative ambition. Cofone's normative proposition show that liberal constitutionalism might not be the appropriate framework to tackle the difference of power in the marketplace of ideas that the harvesting of our personal data by private companies has created.

2. Consent is not a constitutional tool – and is not adapted to privacy law.

In a descriptive way, European digital constitutionalism refers to the different regulations that have been adopted by the European Union in order to respond to the (supposed) "lawlessness" that was characterizing the action of private platforms at the beginning of the 21st century.

The partisan of "digital constitutionalism" are right to state that these regulations resemble the rule of law. As recalled by Nicolas Suzor, the first requirement of the rule of law is that decisions be made according to a set of rules, and not in a way that is arbitrary or capricious. And in fact, article 6 of the GDPR forces platforms to collect data following one of the six legal bases provided by the article. The second requirement is that rules shall be clear, well understood and relatively stable. Article 13 and 14 GDPR in fact force platforms to provide information regarding the "purpose of the processing", the third party to which the data might be transferred and the period of time for which the data will be stored, and article 15 provides a right of access by the data subject to his collected data. Another requirement of the rule of law is that there must be « adequate due process safeguards, including an explanation of why a particular decision was made and some form of an appeals process that allows for the independent review and fair resolution of disputes".⁹ In fact, the GDPR provides due process safeguards for the users such as a right of rectification (Article 16) and a right to erasure (article 17) and the right to lodge a complaint with a supervisory authority (article 77). The GDPR is certainly a step forward, and yet the procedural rights that it grants to the users are not enough to characterize a constitutional framework. This is because the GDPR bases the relationship between platforms and their users in a contractual relationship¹⁰ and make the collection and process of data dependent on consent.

Many authors have already shown why consent in the consumer privacy

⁹ N Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms', (2018) 4 Social Media + Society

¹⁰ RÁ Costello, 'Faux Ami? Interrogating the Normative Coherence of 'Digital Constitutionalism '(2023) 12 Global Constitutionalism 326.

context is often pathological¹¹ and these critics, that apply to the European context, are perfectly summarized by Cofone. The first shortcoming of this approach is what Cofone calls “information overload”. Even if we assume that platforms are, as required by Article 13 and 14 GDPR, effectively exposing their privacy policies in an understandable way for the users, our ability to understand these policies is undermined by the number of privacy policy we go through each day. We have to process so many information that our decision-making activity is negatively impacted.¹² The design used by the websites to collect our consent, as well as its diversity between websites, reinforces this information overload. Who has never click on “accept all” by error, instead of “continue without accepting” because as a user, we need to localize in each website the “continue without accepting” intentionally reduced in size compared to “accept all”? This is why Neil Richards and Woodrow Hartzog wisely offer to make the validity of consent depend on the infrequency of the request.¹³

But Cofone’s contribution to the theory of consent in the digital world goes further. He explains why digital consent to data collection, even if used infrequently, is a fallacy. The so-called “meeting of the minds” – the mutual understanding and agreement regarding a transaction - can hardly exist in privacy law.¹⁴ This is first because privacy is not a yes/no concept: it is only context-dependent. You can choose to share a picture of you with your relatives, but this does not mean you have lost your right to privacy on that picture or that you have agreed to let your relatives share this picture with tabloids.¹⁵ The context-dependent nature of consent in privacy can hardly be reconciled with the way platforms who collect our data monetize them with other parties called “third parties”. Because privacy is not a yes/no concept, we cannot lose our right on our personal data as we lost our right on some trousers we have sold on Vinted. Yet, the way our personal data are processed in the market does not take into account this contextual consent. Most websites use “Real-Time-Bidding”, an auction system that allows to determine in real time which piece of advertisement will best suit a given slot of advertising offered by a website in the webpage consulted for a given users. Michael Veale and Frederik Zuiderveen Borgesius have argued, based on a precise knowledge of the functioning of this RTB system, that RTB could hardly be compatible with the GDPR.¹⁶ The theory of consent put forward by Cofone helps to explain why. Following the entry in vigor of the GDPR, to be able to share the data they’ve collected from their users in the Real-Time-Bidding Auction, websites have started using Consent Management Platforms (CMP). CMP allows a high number of third-parties operating on the Real-Time-Bidding Auction to collect the users’ consent in one click. The number of third-parties is usually extremely

¹¹ N Richards and W Hartzog, 'The Pathologies of Digital Consent', (2019) 96 Washington University Law Review; E Bietti, 'Consent as a Free Pass: Platform Power and the Limits of the Informational Turn', (2020) 40 Pace Law Review 310.

¹² | Cofone, *The Privacy Fallacy: Harm and Power in the Information Economy* (Cambridge University Press 2023)

¹³ Richards and Hartzog (n 11).

¹⁴ Cofone, *The Privacy Fallacy*, n° 12, 21

¹⁵ Cofone, *The Privacy Fallacy*, n° 12, 21

¹⁶ M Veale and F Zuiderveen Borgesius, 'Adtech and Real-Time Bidding under European Data Protection Law', (2022) 23 German Law Journal.

high – a median of 315 vendors,¹⁷ making the informed nature of the consent impossible to meet. Furthermore, during the RTB process, the vendors winning the auction (the vendor who will be presenting her advertising on the website) also gain knowledge of all the personal data of the user who will see her ad on the website. As it is impossible to know in advance who will win the auction, it is impossible for the website to inform users about who will collect data about them, and therefore, for users to give an informed consent¹⁸.

This brings us to Cofone's second important contribution regarding consent weaknesses in privacy law. Privacy law based on consent is grounded on classic and neoclassical economic paradigms, which assume that people always make rational choices on their own based on available information to maximize their utility. According to the neoclassical economic paradigms, we consent to share our data instead of paying Facebook a monthly fee because we have anticipated and measured the consequences of sharing our information with Facebook and the risks this may entail. However, data sharing risks on the internet are unpredictable.¹⁹ This is because people consent before they can even imagine the consequences of giving up their information. Websites who use RTB do not know in advance with whom they will share our personal data, so how could we know the risks that this data sharing could entail? Risks unpredictability is reinforced by unpredictable aggregation of information gathered by data brokers.²⁰ It is also reinforced by the opacity resulting from firm strategies, which creates a "moral hazard" situation created by information asymmetry.²¹ Moral hazard, Cofone explains, happens when one party (the user) has no control over what the other (the platform or website) does, but continues to be affected by what the other party does. Corporations have incentives to collect our data and to create inferences as much as possible, and since users have no control over this process, they can do so extensively. In this context, the fact that websites are only allowed to collect our data following one of the six legal bases provided by Article 6, that includes consent, is not enough to limit platforms' power.

3. Procedural rights are not sufficient to limit platforms' power in a sphere dominated by private law.

The GDPR provides many consent-independent rules, and Cofone argues that these rules are key to the protection of personal data. However, when reduced to compliance obligations, this framework is likely to prove counterproductive. This is because, as explained by Cofone, these consent-independent rules are procedural rather than substantive.²² These rules establish procedures that companies must follow before collecting or sharing

¹⁷ M Nouwens, I Liccardi, M Veale, D Karger, and L Kagal, 'Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence', ACM CONF. ON HUMAN FACTORS IN COMPUTING SYS. 5 (Apr. 2020).

¹⁸ Veale and Zuiderveen Borgesius (n 16).

¹⁹ Cofone, *The privacy Fallacy*, (n° 12)

²⁰ *Id.* 47.

²¹ *Id.* at 60.

²² *Id.* at 98.

their users' information but they do not define privacy harm. In this context, companies can be held liable for the damages their use of data has created for the user only if they have failed to respect some obligations provided by the text. In other words, as soon as they have checked the box, they cannot be held liable.²³ Despite (or maybe thanks to) the procedural compliance, companies keep on externalizing risks, since they cannot be held liable for any wrong their activity has caused to individuals or groups as long as they gone through the required privacy impact assessment. Cofone exemplifies what he means with the case of Grindr selling the personal data of its users, including their sexual orientation and HIV status. Grindr was inflicted a fine by the Norwegian authority that considered that Grindr didn't collect the consent of its users properly, because of the take-it or leave-it option in Grindr's privacy policy. But had Grindr collected the consent of its users, it wouldn't have been sanctioned even though it sold extremely sensitive information²⁴ knowing that they could deeply harm its users.

Furthermore, compliance rules are not adapted to the information economy because in the information economy, conditions are doomed to change rapidly. Thus, compliance rules do not cover all the potential harms that are likely to happen. They only provide legal certainty to firms. Overall, Cofone's demonstration highlights the limits of a "rule-of-lawish" framework applied to private parties. If the proposition to use the rule of law to evaluate the legitimacy of platforms governance²⁵ secures legal certainty for the firms, it fails to protect users' fundamental rights efficiently. It also fails to check private powers, and both affirmations are quite problematic for digital constitutionalism's internal coherence and normative appeal.²⁶ Two factors can explain why this is the case. First, in constitutional law, the power of the State is limited by the fact that the State must always act according to a rule. For each of their action, government must be able to specify a law that authorizes it.²⁷ Because the constitution institutes the government, and because the government possesses only the power recognized in the constitution,²⁸ citizens can attack a measure that wouldn't have been taken according to a text through judicial review. This is not the case with private actions. In private law, it is the contrary: what is not forbidden is allowed. And platforms have used this paradigm extensively: driven by technological changes, keep introducing new inference activities that the EU legislator didn't allow explicitly.²⁹ Their action is not properly illegal because the legislators didn't forbid it. This allows private platforms, as soon as they have collected users' consent, to engage in risky behaviors that they know is not covered by the rules. European digital texts, as exhaustive as they could be, cannot be called "constitutional" because they do not institutionalize platforms as a constitution legally institutionalize the State.³⁰ Platforms legally existed before these texts. They have also

²³ *Id.* at 100.

²⁴ *Id.* at 59.

²⁵ Suzor (n 9).

²⁶ Costello (n 10).

²⁷ M Loughlin, *Foundations of Public Law* (Oxford University Press 2012) 333.

²⁸ *ibid* 333.

²⁹ Cofone, *The Privacy fallacy*.

³⁰ Loughlin (n 27) 336.

extensively used intellectual property law to extend their power.³¹ Second, digital constitutionalism as a descriptive claim fails, at least for the GDPR, because it does not address data protection as a constitutional principle recognized by Article 8 of the European Charter of Human Rights effectively. The text of the GDPR does not allow the Commission or the ECJ to develop a substantive conception of data protection that would be decorrelated from the procedural obligations to process data according to a legal basis. Neither does it allow the controller to develop a substantive definition of harms for the purpose of Article 8 ECHR.

The Digital Services Act,³² that aims to regulate the way platforms moderate and amplify contents of their users, is much more ambitious in that respect. Article 34 refers directly to “negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter, to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter, to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter, to non-discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter and to a high-level of consumer protection enshrined in Article 38 of the Charter”. Platforms must identify systemic risks stemming from their services with regard to these rights and take appropriate measures to “mitigate” these risks. The chosen wording “take appropriate measures to mitigate” could be assimilated to a proportionality test, frequently used by constitutional or European courts when two fundamental rights are in conflict, or when the public interest enters in conflict with a fundamental right. The DSA has also introduced more procedures likely to create substantive and evolving rules. Through Article 34 and 35, that forces platforms to identify and mitigate annually systemic risks stemming from the designing of their platforms, the DSA takes into account some risks that were not known when the text entered in vigor. Article 53 gives recipient of the service or any organization mandated the power to lodge a complaint against providers alleging an infringement of the text. These provisions allow organization or association to litigate, through public enforcement, over practices they have identified as harming users' fundamental rights. As a result, they will also allow the European Commission and the Court to develop a substantive conception of users' fundamental rights in the information economy. But the DSA cannot be said to embrace this constitutional road because it keeps on establishing the basis for liability on the contractual relationship between platforms and its users.³³ Article 54 indeed provides that “recipients of the service shall have the right to seek, in accordance with Union and national law, compensation from providers of intermediary services, in respect of any damage or loss suffered due to an infringement by those providers of their obligations under this Regulation”.

³¹ A Kacpzyński, 'The Law of informational Capitalism' (2020) 129 Yale Law Journal 1460

³² Parliament and Council Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.

³³ B Darmais, 'Raviver la force obligatoire du contrat d'utilisation pour une meilleure protection des acteurs économiques dans l'écosystème des plateformes – À propos de la promesse de réparation figurant à l'article 54 du *Digital Services Act* (DSA), (2025, forthcoming) Dalloz IP/IT.

This provision first excludes non-users from the possibility to seek compensation, and thus potential harms created by platforms' moderation or amplification on non-users.³⁴ Second, this provision excludes the possibility to seek compensation for harms suffered by users if the providers have respected their obligations under the Act. Combined with the wording of Articles 35, which provides that platforms should mitigate (and not suppress) the risks they have identified, this reduces the number of cases in which platforms can be held liable. It means that users who have suffered a damage as a result of a systemic risks will be able to seek remedy only if platforms had failed to identify a risk they knew about and had not taken adequate measures to mitigate the risk. This is equivalent to establishing negligence as the basis for contractual liability.

Cofone's normative proposition, however, shows that even if it is normatively appealing,³⁵ the constitutional framework is not necessary to strengthen users' right and to hold platforms accountable. Constitutionalism indeed often fails to address economic inequalities between parties. This is why digital constitutionalism as a prescriptive claim can also prove problematic. The solution provided by Cofone, based on private enforcement rather than public enforcement seems like a more efficient way to address this economic power differences.

4. The limits of digital constitutionalism as a prescriptive claim.

In one chapter of her important book *Between Truth and Power*³⁶, Julie Cohen uses as an incipit a quotation from John Locke in his *Two Treatises of Government*: "In the beginning, all the world was America".

Locke uses America as a metaphor to describe for a place where land is abundant and not yet divided into private property. "In the beginning, all the world was America" means that at the beginning, all lands were wasted because they were not appropriated. In the Lockean state of nature, people start appropriating the fruits of the earth in order to secure basic means of subsistence. Through that process, they acquire property on things. Only the social contract can secure the right of property that allow people to live peacefully between each other. By using this quotation as an incipit, Cohen means that "in the beginning", personal data, as America in the 17th century, were considered as a "terra nullius", that is belonging to no one, free for appropriation and usable to make profits. During the "state of nature" companies started to appropriate these "free" data through the use of intellectual property law, and they did so in order to secure their means of subsistence, that is revenue from advertisement.

The comparison Julie Cohen makes between data and America is extremely thoughtful. America was far from being a "terra nullius" in 1690. It was populated by native tribes who were denied a property on the land they

³⁴ Id

³⁵ Costello (n 10) 333.

³⁶ J Cohen, *Between Truth and Power: the legal construction of informational capitalism* (Oxford University Press 2019) 48-74.

inhabited because their tradition of ownership and use were different from the colonizers' one. The same could be said of personal data before companies started extracting and processing them through the use of cookies and data-brokers. Data were not "terra nullius", because they were used and shared by the people they were related to, with the people they agreed to share them with. These data were not responding to the notion of ownership as understood in property law: they were not usually sold (even if they could be, think about someone participating in a psychology study for 50\$), but it didn't mean they were not appropriated. The comparison between America in Locke's theory and data extends to the legal framework. For Locke, the social contract must serve the purpose of ensuring the most effective enforcement of natural law and the better protection of our natural rights³⁷, the most important of these rights being property. In that sense, the Lockean social contract legally institutes and secures the relationship of power and dominion that had been established in the state of nature. This is part of the critics made by Rousseau to Locke when he states, in "Discourse on the Origin and Foundations of Inequality among Men" that "society turned a clever usurpation into an irrevocable right, and for the profit of a few ambitious men from that time on subjected all the human race to labour, servitude, and misery."³⁸ Thus, for Locke property is something natural, present in the state of nature, while for Rousseau, property is a construct from the society. The Lockean conception of rights and property has greatly influenced liberal constitutionalism and it is no coincidence if the partisans of the "digital constitutionalism theory" often make reference to the existence of a "digital social contract"³⁹. Liberal constitutionalism characterizes life under legal systems as egalitarian. It fails to see or acknowledge that "the legal system consists of rules that allow people to harm others"⁴⁰. The GDPR legally legitimizes a state of affairs that was created through exploitation but it does not acknowledge this exploitation nor the power that it confers to platforms by allowing them to collect and process users' data. The different procedural right that it creates does not really address the power differential, because it does not force platforms to internalize the risks their new exploitative activity creates. Neither does it allow to address the question of valuation of harm caused by data exploitation, because fines that are inflicted to platforms are decorrelated from this harm.

Cofone offers an alternative normative framework to address this power differential. This normative framework is based on private rather than public law and more precisely on tort rather than on contractual law. Cofone makes the case, convincingly, that civil liability law would lead to more accountability for the harms under information economy. By making corporations liable *ex-post* for the harms they've created, and thus by forcing corporations to share the burden of privacy harms, privacy liability would lead to risk reduction. It would incentivize corporations to act *before the fact* to minimize the likelihood

³⁷ M Loughlin, *Against constitutionalism* (Harvard University Press 2022) 92.

³⁸ JJ Rousseau, 'Discourse on the Origin and Foundations of Inequality among Men', in V Gourevitch (ed.), *The Discourses and Other Early Political Writings* (Cambridge University Press 1997), 111–222, 173.

³⁹ G De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022) 25.

⁴⁰ J W Singer, 'The Legal Rights Debate in Analytical Jurisprudence from Bentham to Hohfeld', (1982) *Wisconsin Law Review* 975.

of the users being harmed. Privacy liability, the book argues, also has the considerable advantage to remedy information asymmetries in the information economy, because it puts the burden on those who are better positioned to understand the harms they create, thus by-passing the cognitive biases currently used by corporations. This proposition builds on the legal realist tradition. Cofone sees rights as relational. He acknowledges that when the States confers to websites or platforms the right to process our data, it creates simultaneously a vulnerability for its users.

The second step of his normative contribution is thus to define this vulnerability. This requires, importantly, a strong conceptualization of privacy harm, conceptualization that is currently lacking in the majority of legal systems. Most of the courts fail to acknowledge privacy harms that aren't material. One of the strength of the book is to offer this conceptualization, by distinguishing three important concepts: privacy loss, consequential harms, and privacy harms. Privacy loss corresponds to the loss of control over your data resulting from data collection, interference, data sharing or leak. It's impossible to have a privacy or consequential harm without a privacy loss, but one can suffer from a privacy loss without suffering from a privacy harm. Consequential harms are these harms happening because of privacy loss, and that are easily identifiable and measurable. That is the case for financial harms resulting from data loss, physical harms or loss of chances. Privacy harms, on the contrary, are mainly immaterial. They can be identified by relying on privacy's long recognized social values - the reason why we protect privacy in the first place. US-based legal scholars have long debated over the different values privacy protects (mainly autonomy and intimacy), and Cofone's strength is to use these debates at the moment of defining remedies. One of the GDPR's weaknesses is indeed the complete mismatch between the values it intends to protect and the remedies it puts in place (because it sees right and obligations as self-existing). Using harm conceptualization at the moment of defining each remedy rather than in the regulation's preamble (as generally done in EU legislations) can help making sure these remedies will actually be adapted to the harms they intend to counter.

This does not mean that constitutional law has nothing to do with data, but maybe not in the way digital constitutionalists currently present it. Some authors have offered alternative legal framework that would involve constitutional law. Cofone defines rights and harms as relational and uses tort law to link the harm suffered by users and the behaviors of the firms. Even if Cofone convincingly argues that victims should rely on class action to reduce the legal cost of the lawsuit for each individual, the harms he's talking about are mainly suffered by individuals on the basis of their identity.

Salome Viljoen offers an analytical framework where data are relational, but mainly horizontally. As she explains, the main purpose of data collection and production is to relate people to one another on the basis of relevant shared population features.⁴¹ The horizontal relationship is created in the following way: a group is composed by different individuals who share a relevant feature. The group is used act on group members according to this grouping. It serves

⁴¹ S Viljoen, 'A relational theory of data governance' (2021) 131 Yale Law Journal, 578.

to make predictions for one group member based on other group members' characteristics. In Viljoen's account, data losses are not necessary to create data harms, because one member of the group can suffer a harm based on a data shared willingly by another member of the group.⁴² This horizontal relationship can also create socially beneficial effects that the law should also take into account and promote. This is the case, for example, of population-level health data when they are used in cancer studies. Horizontal data relationships cannot be seized through individual rights or individual remedies, because they aim at derivating population-level insights that have an impact on countless individuals. Viljoen argues that only a democratic governance framework can manage data's relationality social effects.⁴³ Her project is thus constitutional, because it highlights the importance of a set of institutions that aims at ensuring democratic control over datas. By taking into account the political economy of data relations to design a framework of governance that would represent everyone's interests, Viljoen offers a constitutional framework far from liberal constitutional and closer to material constitutionalism.⁴⁴ Viljoen and Cofone's view are not unreconcilable, on the contrary. While one addresses individual and identifiable harms through private law, the other addresses collective harms and social benefits through public law. They both highlight the limits of digital constitutionalism as it is thought today.

⁴² *Id.*

⁴³ *Id.*, 638.

⁴⁴ M Goldoni and MA Wilkinson, 'The Material Constitution' (2018) 81 *The Modern Law Review*, 567.