DICKINSON LAW REVIEW
PUBLISHED SINCE 1897

Volume 129 | Issue 1

Fall 2024

The Outer Limits of Digital Privacy Protections: A Review of The Privacy Fallacy

Michael Conklin

Recommended Citation

Michael Conklin, *The Outer Limits of Digital Privacy Protections: A Review of The Privacy Fallacy*, 129 DICK. L. REV. 249 (2024).
Available at: https://ideas.dickinsonlaw.psu.edu/dlr/vol129/iss1/6

Book Reviews

The Outer Limits of Digital Privacy Protections: A Review of *The Privacy Fallacy*

Michael Conklin[*]

Table of Contents

[*] Assistant Professor of Business Law, Texas A&M University Central Texas; Lecturer, Texas A&M University School of Law. mconklin@tamuct.edu.

INTRODUCTION

This is a review of Ignacio Cofone's new book, *The Privacy Fallacy: Harm and Power in the Information Economy*.[1] The book argues for the provocative policy proposal of dramatically increasing legal liability for data breaches. While Cofone provides thought-provoking analysis for the rapidly evolving and highly relevant subject of data privacy, this review is primarily a critique of the proposal. Topics covered in this review include: the extreme nature of Cofone's proposed policy, an analysis of the evidence provided to support such a policy, a discussion of the existing incentive structure's adequacy, the issue of autonomy and choice, and potential unintended consequences. Finally, the conclusion of this review mentions the importance of having this discussion at such a pivotal point in time.

I. PROPOSED POLICY

The main thesis of the book is that privacy law is largely based on contract-like relationships that are not applicable to modern, digital practices.[2] Contract law is rooted in notions of voluntary agreements while digital privacy agreements are not truly voluntary because there is no chance to negotiate terms, the services offered are often necessary for operating in society, and consumers rarely read the terms and conditions they are agreeing to.[3] Therefore, Cofone argues that privacy law should instead be grounded in concepts of tort law, rather than contract law.[4]

Additionally, Cofone proposes that the notion of harm applicable to privacy violations should be greatly expanded. The existing standard, as set out by the Supreme Court in *TransUnion LLC v. Ramirez*,[5] is that plaintiffs need to show a "close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts" such as physical harm, monetary harm, or various intangible harms including reputational harm.[6] Cofone argues that the Court's current approach is not expansive enough as it does not include "privacy harm" in itself as a cognizable harm.[7] "Recognizing privacy harm is the logical consequence of recognizing that privacy has

[1] IGNACIO COFONE, THE PRIVACY FALLACY: HARM AND PROTECTION IN THE INFORMATION ECONOMY (2024).

[2] *Id.* at 3.

[3] *Id.* at 4.

[4] *Id.*

[5] Transunion LLC v. Ramirez, 593 U.S. 413 (2021).

[6] *Id.* at 425.

[7] COFONE, *supra* note 1, at 118.

intrinsic value—that it's worth protecting in and of itself," explains Cofone.[8]

To illustrate, Cofone provides the example of someone whose internet activity is tracked by Google.[9] By analyzing this history, Google can engage in more accurate targeted advertisements.[10] The more history Google gathers, the more accurate it can be with those targeted ads.[11] Cofone posits that this increasing accuracy produces a coreferential increase in privacy loss, or "loss of obscurity."[12] By engaging in this practice, Google has constituted "privacy harm independent of its material consequences."[13] Using the real-world context of the Grindr breach, Cofone claims that courts should recognize harm as how the breach "affected their intimacy, contravened social expectations, inhibited trust, and obstructed communications that LGBTQ people may want to have with each other."[14] According to Cofone, this expansive interpretation of harm would also encompass the real-life instance where users of the OKCupid dating app had their profile pictures used to train a facial recognition computer program.[15]

II. TRIVIAL COMPLAINTS AND DISANALOGOUS ANALOGIES

Many of the complaints voiced by Cofone appear trivial when compared to the extreme nature of his proposed solution. Cofone references "confirmshaming," which is described with the following example: "[w]hen we decline an email newsletter, some websites shame us into changing our choice with banners that read something along the lines of: 'Don't go! We'll miss you!'"[16] The practice of "digital manipulation" is also criticized by the author with very trivial examples, such as: "Think of websites that shame you for not providing your email for a discount, using pop-up messages that say: 'No thanks, I like paying full price.'"[17]

Cofone further alleges that "dark patterns" are the "ultimate form of design manipulation."[18] However, the examples provided cast serious doubt on this claim. Cofone explains that "if you try to

[8] *Id.* at 125.
[9] *Id.* at 120.
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.* at 126.
[14] *Id.* at 146.
[15] *See id.* at 46 (explaining why expecting individual agreements to protect privacy and reduce harm is a "dead end").
[16] *Id.* at 40.
[17] COFONE, *supra* note 1, at 67.
[18] *Id.* at 42.

cancel a subscription with the *Financial Times*, you'll find a preselected option to change the subscription to a different (sometimes more expensive) one; to find the 'cancel subscription' button you'd have to scroll to the bottom of the webpage and find it in smaller font."[19] Another example of this "ultimate form of design manipulation" is how "*The New Yorker* sends a pretend final demand letter that reads, 'statement of account: FINAL NOTICE,' but is just a request to renew the subscription, which would otherwise expire."[20]

Cofone writes as though the ability of businesses to target specific demographic groups with advertisements that they are more likely to be interested in is a great harm.[21] He claims that "[o]nline manipulation amounts to privacy harm when someone affects our decisions by using our personal data to target and exploit our vulnerabilities."[22] Cofone then laments, "[b]ut the information Facebook has about its users is so detailed and nuanced that [removing the "ethnic affinity" filter option] hardly made a difference. For example, advertisers can't filter by who's Latinx, but they can filter by who likes Telemundo."[23] It is unclear what exactly the alleged harm would be here, as the use of targeted advertising means that customers are more likely to see advertisements relevant to their interests. Is it also a great harm when salesmen in face-to-face settings alter their sales pitches based on the unique interests of the customer? Furthermore, the ability to engage in targeted advertisements provides an incredible benefit to small, minority-owned businesses who cater to underserved communities, as it allows them to reach their target audience more efficiently. Additionally, targeted advertising is a great way for activists with minority views to spread their message and create change.

Cofone's use of analogies is often peculiar given his proposed solution. Properly understood, these analogies often argue *against* his position rather than for it. For example, Cofone attempts to use the Ford Pinto products liability lawsuit to illustrate how victims of data harms "don't get the affordances that victims of other harms get."[24] It is true that, as Cofone points out, the law does not allow consumers to choose unsafe cars; rather, it mandates safe cars for all.[25]

[19] *Id.* (parenthesis in original).

[20] *Id.* at 42–43.

[21] *Id.* at 3.

[22] *Id.* at 125. Additionally, Cofone claims that, "When someone uses our personal information to our disadvantage by covertly manipulating us, that constitutes privacy harm independent of its material consequences." *Id.* at 126.

[23] *Id.* at 3.

[24] *Id.* at 88.

[25] *See id.* ("The law doesn't allow companies to ask consumers: 'do you accept the risk that your car engine may combust?' It just requires companies to sell safe engines.").

That said, it does not logically follow that consumers should therefore be unable to choose privacy policies, as the two are not analogous in any meaningful way. First, unsafe cars often lead to death while security breaches do not. Second, Facebook's privacy infrastructure is not defective by design. Of course, a company can always invest more time and money into protecting customer data, but no amount of investment can render data breaches impossible.[26] In the Ford Pinto products liability lawsuit, the product was dangerous as it left the dealership; it did not require an intentional, criminal act by a third party to cause the damage.[27] Finally, the judgment against Ford was only possible because of the presence of actual damages. If the design of the automobile never harmed anyone, there would have been no lawsuit as plaintiffs in products liability litigation generally cannot recover without demonstrating that they suffered harm.[28] A plaintiff merely positing that they were in fear of potentially being harmed is inadequate.[29] However, this is essentially the premise Cofone is arguing regarding the breach of privacy liability.

Some of the evidence Cofone presented bears little relation to issues of privacy. For example, he points out how Facebook "stoke[s] division," "weaken[s] our democracy," "exacerbate[s] body-image issues in teenage girls," and sometimes allows "hate speech."[30] While one or all of these general critiques may be independently true, they have nothing to do with privacy law. Cofone appears to be applying some type of argumentation whereby Facebook should face more stringent privacy standards because it engages in other practices that some people disagree with. This is a particularly weak argument in the context of advocating for stricter privacy laws. These are, of course, legitimate issues that should be addressed, but they are wholly separate from any privacy issues.

III. INCENTIVES

Cofone alleges that, under the current legal regime, businesses are inadequately incentivized to protect customer privacy. He uses

[26] *See infra* note 34.

[27] *See, e.g.*, Aaron Gold, *The History (and Tragedy) of the Ford Pinto: Everything You Need to Know*, MOTOR TREND (Apr. 4, 2024), https://tinyurl.com/3rh579ce [https://perma.cc/6PT6-Q4VU].

[28] *See, e.g.*, *Products Liability*, CORNELL L. SCH. LEGAL INFO. INST., https://tinyurl.com/bdekcckv [https://perma.cc/3NL8-RY8G] (last visited Mar. 31, 2024) (listing "[t]he plaintiff suffers an injury" as the third element in a *prima facie* case for products liability).

[29] *Id.*

[30] COFONE, *supra* note 1, at 89.

the 2019 Desjardins Canadian data breach to illustrate this.[31] There, a single employee engaged in criminal activity and exfiltrated sensitive customer data.[32] This led to Desjardins ultimately settling a class action lawsuit for $201 million.[33] Cofone finds this amount woefully inadequate.[34] While it is true that an even harsher punishment would naturally provide an even greater incentive for companies to protect customer privacy, there does reach a point of diminishing returns. And no amount of prevention would render a data breach impossible.[35]

When considering the issue of incentives, one must consider the entire cost to companies like Desjardins, not just the final settlement amount. For example, Desjardins faced reputational harm, attorney's fees, and mitigation costs (they partnered with Equifax to identify which customers' information was breached).[36] This total amount of harm would far exceed the $201 million from the lawsuit. With this more accurate understanding of the costs involved, it becomes clear that there already exists a substantial incentive to avoid data breaches.

Another argument against increasing companies' liability for data breaches is that of diminishing returns. Put simply, the more a business spends on data protection, the less benefit is gained on a per-dollar basis. This is because businesses will naturally invest in the most cost-effective measures first, leaving less and less cost-effective measures to be implemented with any increased spending.[37] Not only would these increased expenditures decrease the per-dollar effectiveness in privacy, but this is also money that could otherwise be spent on developing better products and services for the consumer.

[31] *The Desjardins Data Breach + What We Can Learn From It*, TITANFILE, https://tinyurl.com/3r6avc5c [https://perma.cc/C556-HHHH] (last visited Mar. 29, 2024).

[32] *Id.*

[33] COFONE, *supra* note 1, at 138.

[34] *Id.* at 138–39. Elsewhere, Cofone refers to a $425 million fine as leaving "the company underincentivized to avoid data breaches in the future." And remember, the $425 million is just the fine; there are many other costs incurred for a data breach. *Id.* at 139.

[35] As Cofone himself explains, "the question isn't who's going to be hacked; the question is when each company will get hacked." *Id.* at 150.

[36] Canadian Press, *Quebec Court Approves $200.9M Settlement Against Desjardins Over Data Breach*, CBC (June 17, 2022), https://tinyurl.com/yckfjxv5 [https://perma.cc/2NHY-QEG6].

[37] Much like if someone was to spend $10,000 on home security and then decide to spend an additional $10,000 on home security on top of that. This additional expenditure doubled the amount spent but is unlikely to reduce the probability of a theft by 50 percent. This is because the most cost-effective home security measures were likely implemented with the first $10,000 (the "low hanging fruit," if you will). The additional spending will provide more home security, but the per-dollar value obtained will decrease—thus the diminishing returns.

Cofone does not acknowledge this reality—rather, he appears to believe that this additional liability will somehow increase firm profitability. He alleges that dramatically increasing liability would not only "preserve the information economy" but that "[i]t would even improve it."[38] He continues, "It wouldn't halt innovation or the tech industry because it creates space for the industry to engage in any data practice that produces more profit than harm. Creating liability for the consequences of their data practices provides needed incentives to develop data practices that are high-profit and low-harm."[39] This is a highly peculiar claim, because if increased expenditures on data privacy would naturally result in increased profitability, then these profit-seeking firms would naturally increase these expenditures without the need of coercion.

The issue of incentives is not just limited to the incentives existing firms experience to keep user data private. Dramatically increasing firm liability regarding privacy practices would also function to disincentivize new firms from entering the industry, thereby ultimately decreasing consumer choice. The practice of onerous regulations pricing out competitors is a well-researched phenomenon referred to as regulatory capture.[40] Raising market entry prices would be especially harmful in the tech industry where rapid innovation from new companies is imperative.

IV. CHOICE

Somewhat paradoxically, Cofone alleges that "[p]rotecting people's autonomy means sheltering them from exploitation even when they would agree to it."[41] To support this position, Cofone states, "[c]hoice assumes knowledge and understanding of risks. It's impossible to make a real choice if you do not know what the real choice is and what its consequences can be—what risk you are taking on by agreeing."[42] However, this proposition ignores the reality that consumers often choose to be willfully ignorant regarding certain aspects of a given choice. And in this way, even if someone, say, does not read the terms and conditions they are agreeing to, they are still making a willful decision—the decision that accepting what is likely included in the terms and conditions is preferable to the alternative of conducting an investigation into the terms and perhaps then trying

[38] COFONE, *supra* note 1, at 171.

[39] *Id.*

[40] *See, e.g.*, Will Kenton, *Regulatory Capture Definition with Examples*, INVESTOPEDIA (Mar. 1, 2011), https://tinyurl.com/2nyzb4fc [https://perma.cc/K4XM-GFEY].

[41] COFONE, *supra* note 1, at 168.

[42] *Id.* at 17.

to find an alternative product with more acceptable terms and conditions. This is similar to the conscious ignorance doctrine in contract law.[43] And this willful ignorance is likely not irrational. There are legal limits as to what the terms and conditions can contain, there is nothing one can do to negotiate better terms, and the alternative route of not using the service altogether is not an attractive option.

On the topic of choice, it is somewhat ironic that Cofone is the one who is, properly understood, advocating for a significant reduction of consumer choice. Currently, consumers can choose to join Facebook, which entails agreeing to allow Facebook to track and sell their personal information along with numerous other terms such as a California forum selection clause.[44] In return, the consumer gains access to all that Facebook has to offer completely free. And indeed, hundreds of millions of consumers have made the decision for themselves that this is a favorable tradeoff.[45] But if Cofone's policies are implemented, it is unlikely that Facebook would be able to continue offering its product for free, thus depriving consumers of their current choice. The fact that no large-scale social media company has been successful running on a business model that charges the consumer in exchange for increased privacy protections is a strong indication of consumer preferences.[46]

Cofone correctly points out that behavioral economics has demonstrated that, in certain contexts, consumers do not act consistently with rational choice theory. For example, consumers are willing to stand in a long line to save $20 on a $50 purchase but not to save $20 on a $1,000 purchase.[47] However, using this notion as evidence that the government should bar consumers and businesses from entering into agreements that they each find agreeable, if consistently applied, would be untenable as it would extend to nearly every consumer transaction.

CONCLUSION

While this review is a critique which focuses on areas of disagreement, the book is certainly not without valid points. For example, Cofone addresses how easily anonymized data can sometimes

[43] *See, e.g.*, *Contract Law: Possible Applicability of the Conscious Ignorance Doctrine Precluded Summary Judgment in This Mutual Mistake Action*, N.Y. APP. DIG. (Feb. 23, 2017), https://tinyurl.com/4w73drkh [https://perma.cc/S7DF-AL5Y].

[44] COFONE, *supra* note 1, at 17–18.

[45] *Facebook Has 3 Billion Users. Many of Them Are Old*, CBS NEWS (May 8, 2023), https://tinyurl.com/bdhwnea8 [https://perma.cc/96TR-YTKA].

[46] Furthermore, studies routinely demonstrate that consumers put very low value on their privacy. COFONE, *supra* note 1, at 33–34.

[47] *Id.* at 29.

be deanonymized.[48] Even though Cofone's main points are rather extreme and would likely produce more harm than benefit, considering his position is beneficial to understanding various privacy-related issues. This is perhaps more important now than ever before as there is a confluence of contentious privacy-related legal issues such as facial recognition biometrics,[49] artificial intelligence in criminal trials,[50] record-high data breaches,[51] and the use of online artistic expressions posted on social media being used as evidence in criminal trials.[52]

[48] *Id.* at 52.

[49] *See generally* Michael Conklin & Brian Elzweig, *A Face Only an Attorney Could Love: Madison Square Garden's Use of Facial Recognition Technology to Ban Lawyers with Pending Litigation*, 83 MD. L. REV. 578 (2024).

[50] *See generally* Michael Conklin, *Justice by Algorithm: Are Artificial Intelligence Risk Assessment Tools Biased Against Minorities?*, 16 S. J. POL'Y & JUST. 2 (2022).

[51] *See generally* Justin Klawans, *Data Breaches Increases in 2023 and with Them, Internet Security Concerns*, THE WEEK (Mar. 7, 2024), https://tinyurl.com/yjmnupw7 [https://perma.cc/JWV6-8J8M].

[52] *See generally* Michael Conklin, *The Extremes of Rap on Trial: An Analysis of the Movement to Ban Rap Lyrics as Evidence*, 95 IND. L.J. SUPPLEMENT 50 (2019).

***