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

Ignacio Cofone's *The Privacy Fallacy* not only addresses the political economy of informational capitalism, but also demonstrates the vital importance of a Law and Political Economy (LPE) perspective in data protection research. His work both reflects and contributes to a growing awareness of the role of corporate power in perpetuating unfair exploitation of data. This sensitivity to economic context allows *The Privacy Fallacy* to offer a realistic vision for better vindicating privacy rights now, while modeling methodological sophistication for future work in the area.

Cofone begins *The Privacy Fallacy* by critiquing overreliance on contract law in the governance of data in the United States and argues for using tort principles to compensate for (and deter) privacy harms. To broaden the scope for privacy protection, Cofone proposes a private right of action (PRA) in privacy laws, broader and more forceful than extant PRAs in US federal and state statutes and those in the General Data Protection Regulation of the European Union. He also wants to ensure that the right to sue survives exculpatory clauses sure to be included in online terms of service.

The Privacy Fallacy lays the foundation for an expansive future research agenda by examining notable concrete cases of privacy harms. Consider the dating app Grindr's sale of "its users' personal information to third parties, which included sexual orientation and HIV status" (145). Cofone mentions that Grindr faced a historic fine imposed by the Norwegian Data Protection Authority (DPA) for its misdeeds: €9.6 million, or 10 percent of its global revenue in 2020. Drawing on this case, Cofone recommends dual remedial regimes, where victims of illegal data practices can sue in courts, while regulators pursue parallel administrative proceedings.

Such cases raise two sets of questions of particular interest to LPE scholars. First, what methods of valuation might best ensure just remedies for wronged data subjects? Second, how should courts and regulators coordinate to rationally divide the labor of privacy protection?

As for the first question on valuation, the determination of proper levels of compensation offers difficult challenges for judges, policymakers, and scholars. After an HIV-related privacy breach, Aetna (a US insurer) settled a case involving the illegal revelation of about twelve thousand persons' HIV status for $17 million—roughly $1,400 per person had it been distributed equally.[1] This figure is the same order of magnitude as the £3,500 and £5,000 privacy damages awards in Britain mentioned in a 2017 article on the tort of misuse of private information.[2] The £3,500 case involved a famous model who was photographed leaving a drug rehabilitation clinic and who recovered damages for misuse of private information.[3] The small award does not seem like adequate recompense for the anguish the model suffered. Nor does it seem likely to deter major media firms from engaging in similarly invasive conduct in the future. But Britain is a loser-pays legal system, and presumably the model incurred high attorneys fees to press her case.

[1] Settlement Agreement, Beckett v. Aetna Inc., No. 2:17-cv-03864-JS (E.D. Pa. Jan. 16, 2018). This case was not discussed in Cofone's book, but I bring it up as a way of benchmarking the valuation of certain mass privacy torts.
[2] Jojo Y.C. Mo. "Misuse of Private Information as a Tort: The Implications of Google v Judith Vidal-Hall." 33 *Computer Law & Security Review* 87 (2017).
[3] Campbell v. MGN Ltd. [2004] 2 A.C. 457 (UK).

The specific facts of the case may also create opportunities for equitable attention to divergent effects of privacy violations. The Aetna breach occurred because "the fact that [affected data subjects] had been taking HIV drugs was revealed through the clear window of the envelope" sent to them, which contained a letter regarding a prior Aetna privacy violation.[4] Some of these envelopes may have resulted in devastating revelations to family members or others privy to the victim's mailbox; others may have only been seen by a postal worker, or not even noticed. To respond to such diverse harms, the settlement established a two-tier remedy framework, where $500 was to be distributed to each of about twelve thousand persons who may have received the letter and another fund was designated for those who "experienced additional financial or emotional distress," with potential payouts up to $20,000.[5]

On one level, this seems like a sensible outcome. Some claimants may not have had any impact from the visibility of the HIV-related information. The $500 award to them simply serves to deter misconduct, rather than to recompense harm. However, on the opposite end of the scale, the $20,000 figure seems inadequate to truly recompense plausible "worst case scenarios," given the potential for stigma documented in the complaint in the case.

It is relatively easy to imagine tragic sequelae of a privacy violation for particular victims. But this raises other difficult questions. For example, when should class action settlements be shared equally by members of the class, and when should those who are particularly harmed receive more? Fuller consideration of these issues would enrich future discussions of the privacy class actions that Cofone endorses.

A second question that arose after reading *The Privacy Fallacy* was the proper coordination of nonmonetary judicial remedies with regulators' demands. Plaintiffs who demand equitable remedies are in a sense acting as private attorneys general (in US parlance). To offer a concrete example: Private rights of action filed pursuant to the California Consumer Privacy Act (CCPA) may give rise to equitable remedies that duplicate, exceed, or fall short of relevant regulatory requirements crafted by the California Privacy Protection Agency (CPPA). It would seem advisable for courts to at least consult these regulatory requirements as they determine standards of care.[6] And when courts prescribe equitable remedies whose demands exceed what regulators presently demand, that should be an opportunity for the CPPA to reexamine whether its own regulations are too lax.

It is to Cofone's great credit that *The Privacy Fallacy* raises such intriguing questions about the future of data protection. The book clearly advances our understanding of the difficult challenges ahead in balancing the rights of businesses and consumers, as well as the responsibilities of supranational, national, and subnational regulators. I look forward to Cofone's further work in the area, as his remarkably cosmopolitan perspective and passion for social justice greatly enriches contemporary privacy law discourse.

Frank Pasquale
Cornell Law School and Cornell Tech
fp269@cornell.edu

[4] Elana Gordon. "Aetna Agrees to Pay $17 Million in HIV Privacy Breach." *NPR*, January 17, 2018. https://www.npr.org/sections/health-shots/2018/01/17/572312972/aetna-agrees-to-pay-17-million-in-hiv-privacy-breach.
[5] Ibid.
[6] Frank Pasquale. "Data-Informed Duties in AI Development." 119 *Columbia Law Review* 1917 (2019).