Texas Law Review Online

Volume 100

Response

Storming Zuckerberg's Castle

Anupam Chander†

Introduction

A company's server is its castle, Richard Epstein once declared.[1] Because of this, anyone sending an email to that server needs permission to enter. Within its own logic, this seems incontrovertible, but it depends on a few logical steps worth unpacking. It begins with the premise that a man's home is his castle. (The masculine pronoun in the early formulation seems relevant.) Let us accept that premise for the purpose of argument. Combining this premise with the investiture of legal personhood on a corporation, we might then deduce that a *company*'s home must be its castle. Finally, combining that claim with the assertion that a server is like one's home, we might conclude that a company's server is like its castle. Each of the moves above is subject to dispute, as is the premise itself. But the end goal is clear: sole and despotic dominion, now over the metaverse.

Thomas Kadri begins his excellent *Texas Law Review* article, *Digital Gatekeepers*, with the evocative image of Facebook as Mark Zuckerberg's

† Scott K. Ginsburg Professor of Law and Technology, Georgetown University; A.B. Harvard University; J.D. Yale Law School. I am grateful to librarian Heather Casey for helpful research, Daphne Keller for superb comments, and the *Texas Law Review Online* staff, including Rachel Stephenson and Patrick Wroe, for excellent editing.

1. Richard Epstein did not in fact use these precise words. This was the characterization offered by the California Supreme Court majority of his submission in a case. Intel Corp. v. Hamidi, 71 P.3d 296, 309 (2003) ("In effect, Professor Epstein suggests that a company's server should be its castle, upon which any unauthorized intrusion, however harmless, is a trespass.").

castle.[2] But rather than imagining lords watching over their rightful domains like Epstein, Kadri sees digital enterprises as trolls guarding a bridge. Yet, these digital trolls are not exacting fees from those who hope to cross, but rather are seeking to prevent anyone else from benefiting from the lands that lie across the bridge. Kadri hopes to build ladders to scale the ramparts or battering rams to break down the gates.

Permitting third-party access to enormous datasets, such as the ones held by Facebook, raises concerns about privacy, as Kadri recognizes. In this essay, I suggest that this concern about user privacy finds a real-life example in the case of Cambridge Analytica, which exploited user data gleaned via a Facebook app. I review various legislative solutions to this problem of data-sharing across private parties. Further complicating this problem is the fact that, especially because of the internet, datasets held by today's companies often include information on individuals from multiple countries. This brings to bear multiple data privacy laws to the question of information sharing. Even if granting access is permitted (or required) under one law, granting such access may still violate another law if that second country's users are in the database. Companies that have not collected information about a user's country may now need to do so to ensure that the right set of laws are applied to that data.

This essay proceeds as follows. Part I sets out the digital gatekeeping function of the common law doctrine of trespass to chattels and the federal Computer Fraud and Abuse Act. It observes that defining the extent of gatekeeping power—the precise line-drawing between permissible and impermissible breaches—remains a complicated task. Part II focuses on Facebook's Cambridge Analytica scandal, which lives on as a warning about giving third parties access to personal data. Parts III then reviews proposals for changes to digital gatekeeping laws in the United States, the EU, and India, respectively.

I. Digital Gatekeeping Laws: From Trespass to Computer Fraud and Abuse

The doctrinal battleground for Kadri is the Computer Fraud and Abuse Act (CFAA), which dates from 1984 or 1986, depending on how one counts.[3] For Epstein, the doctrinal focus was the much older common law rule against trespass, applied now to the virtual world.[4]

2. Thomas E. Kadri, *Digital Gatekeepers*, 99 TEXAS L. REV. 951, 951 (2021).

3. *See generally* Kadri, *supra* note 2. *CFAA Background*, NAT'L ASS'N OF CRIM. DEF. LAWS. (Mar. 10, 2020), https://www.nacdl.org/Content/CFAABackground [https://perma.cc/MZ22-Y9YL] (pointing out that the CFAA, which passed in 1986, is technically an amendment to the Comprehensive Crime Control Act, which was passed in 1984).

4. *Hamidi*, 71 P.3d at 309.

The California Supreme Court, in its role as enunciator of the common law, rejected Epstein's maximalist vision. In *Intel Corp. v. Hamidi*,[5] it permitted an unhappy former employee to send emails to current employees using the company's computer network, much to the annoyance of their employer.[6]

The U.S. Supreme Court, in its role as interpreter of federal statutes, agreed with the narrower view that Kadri (and others) have offered of the Computer Fraud and Abuse Act, at least in significant part. In *Van Buren v. United States*,[7] it held that a Georgia police sergeant, who ran a search in a government license plate database in exchange for money, had not clearly violated the Computer Fraud and Abuse Act because he had authorization to access that database (though not for this illicit purpose).[8] In other words, both the California Supreme Court and the U.S. Supreme Court have, in recent cases, adopted views that reduced the power of digital gatekeepers.

These may appear to be esoteric questions of legal doctrine, such as the charming question of how to apply law developed for horses to cyberspace.[9] But they impact real-world questions of competition, privacy, surveillance, and even artificial intelligence learning. Take a few examples. Should Facebook be able to control its platform to prevent users from turning over their accounts to a competitor social network, which then wants to advertise to those users' friends? Should a company be able to train its AI on LinkedIn's public network?

The dispute between Epstein and Kadri might be characterized as one of the *extent of digital gatekeeper power*—where exactly should we draw the line between what a company can and cannot do, with respect to how others can use its digital platform? Epstein's maximalist approach seems problematic even on its own terms because it relies on the emergence of a market for access rights, which would in fact drown in the transaction costs of endless negotiations with every party you transacted with online. But where exactly we should delimit digital gatekeeping power is a complicated question. Drawing the line is difficult.

Kadri suggests that line should be drawn, at least with respect to the CFAA, on the basis of whether a website is publicly accessible.[10] But even here, questions of line drawing remain, whether they be questions of the CFAA or of other law.

---

5. 71 P.3d 296 (2003).

6. *See id.* at 299–300.

7. 141 S. Ct. 1648 (2021).

8. *See id.* at 1652.

9. Who said there wasn't a law of the horse? *See, e.g.*, Fouldes v. Willoughby (1841) 151 Eng. Rep. 1153, 1153, 1155 (holding that it was not conversion for a ferryman to move horses off a ferry, but it could possibly be trespass to chattels).

10. Kadri, *supra* note 2, at 988.

Take the case of *Facebook v. Power Ventures*.[11] Power Ventures sought to create a social media one-stop shop, taking all of your feeds from your various accounts and consolidating it on its page.[12] Essentially, users could authorize Power Ventures to log into those accounts on their behalf.[13] Power Ventures solicited users by offering a prize of $100 if they signed up 100 friends for Power Ventures' service.[14] Power Ventures would use its access to the users' Facebook accounts to send messages to their friends, including emails, like the following: "I am competing for the $100 prize in the 100x100x100 promotion and recommend you to participate too!"[15] Facebook sued Power Ventures, arguing, among other things, that Power Ventures violated the CFAA through such messages.[16] The Ninth Circuit agreed. It reasoned that even if users arguably gave Power Ventures authorization to send messages using their Facebook accounts, Facebook clearly revoked that access through a cease-and-desist letter to Power Ventures.[17]

A world of 50 Facebooks that some seek[18] would clearly bring with it promotions and other stunts to try to attract users to one platform rather than the others. That seems like the kind of competition we may wish for in a free market economy—at least someone is paying you for using their service. But the Ninth Circuit's determination that a competitor cannot exploit the app to send messages to a user's friends is a stark reminder that drawing the line between permissible and impermissible uses of a platform available to the public will prove controversial.

Particularly complicating that line drawing is concern over user privacy, including preventing data breaches. A repeated refrain from Facebook, when rejecting data-gathering efforts of researchers and others, is the protection of user privacy.[19] Certainly, these protests often serve corporate goals of avoiding negative scrutiny, but there is an additional reason for Facebook's caution: the cautionary tale of Cambridge Analytica.

---

11. 844 F.3d 1058 (9th Cir. 2016).

12. *Id.* at 1062.

13. *See id.* at 1067 (noting that certain user actions in a Power Ventures promotional campaign were "akin to allowing a friend to use a computer or to log on to an e-mail account").

14. *Id.* at 1063.

15. Brief of Plaintiff-Appellee Facebook, Inc. at 12, Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016) (No. 17-16161).

16. *Facebook*, 844 F.3d at 1063.

17. *Id.* at 1067 ("Here, initially, Power users arguably gave Power permission to use Facebook's computers to disseminate messages. . . . But Facebook expressly rescinded that permission when Facebook issued its written cease and desist letter.").

18. *See generally* Przemyslaw Palka, *The World of Fifty (Interoperable) Facebooks*, 51 SETON HALL L. Rev. 1193 (2021).

19. *See, e.g.*, Gilad Edelman, *Facebook's Reason for Banning Researchers Doesn't Hold Up*, WIRED (Aug. 4, 2021, 8:00 PM), https://www.wired.com/story/facebooks-reason-banning-researchers-doesnt-hold-up/ [https://perma.cc/8UMH-QVT7].

II. The Long Shadow of Cambridge Analytica

The Cambridge Analytica scandal casts a long shadow over data sharing by internet companies. It is useful to recall the details of that scandal. Aleksandr Kogan, an American citizen, was, at least at the time, a Senior Research Associate and Lecturer at the Department of Psychology at the University of Cambridge, where he established and led the Cambridge Prosociality and Well-Being Lab.[20] In 2014, through his UK company Global Science Research, Ltd. ("GSR"), he offered an app called thisisyourdigitallife via Facebook.[21] Some 250,000 to 270,000 Facebook users directly interacted with the app.[22] Kogan used the app to gather information, not only from the users who had downloaded the app, but also their Facebook friends.[23] He then shared that information with SCL Elections, Ltd., a U.K. corporation, which had an ownership interest in Cambridge Analytica, a Delaware corporation based in New York City (which had an affiliated company, Cambridge Analytica, (UK) Limited).[24] Cambridge Analytica then used the data to try to target individuals for advertising in the 2016 presidential elections,[25] though it seems likely that Cambridge Analytica was selling "snake oil"—that its "psychometric" profiling of users based on their "likes" was shoddy science both in the accuracy of its profile and in its ability to sway.[26] Ted Cruz, we might recall, also spent heavily on Cambridge Analytica in the 2016 presidential campaign only to find disappointment.[27] (Facebook's own ad targeting tools are likely better.[28])

---

20. Complaint at *2, *In re* Cambridge Analytica, LLC, No. 9383, 2019 WL 3451728 (F.T.C. July 22, 2019) [hereinafter F.T.C. Complaint].

21. *Id.* at *1–4.

22. *Id.* at *1.

23. *Id.*

24. *Id.* at *1–4. INFO. COMM'R'S OFF., INVESTIGATION INTO THE USE OF DATA ANALYTICS IN POLITICAL CAMPAIGNS: A REPORT TO PARLIAMENT 26 (Nov. 6, 2018) https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf [https://perma.cc/P5M9-DKD].

25. *See* Scott Detrow, *What Did Cambridge Analytica Do During the 2016 Election?*, NPR (Mar. 20, 2018, 7:22 PM), https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election [https://perma.cc/44T2-8USB].

26. Siva Vaidhyanathan, *Facebook Was Letting Down Users Years Before Cambridge Analytica*, SLATE (Mar. 20, 2018, 7:00 PM), https://slate.com/technology/2018/03/facebooks-data-practices-were-letting-down-users-years-before-cambridge-analytica.html [https://perma.cc/2XH3-DHQY].

27. Patrick Svitek & Haley Samsel, *Ted Cruz Says Cambridge Analytica Told His Presidential Campaign Its Data Use Was Legal*, Texas Tribune (Mar. 20, 2018), https://www.texastribune.org/2018/03/20/ted-cruz-campaign-cambridge-analytica/ [https://perma.cc/L8BG-M4H4].

28. Siva Vaidhyanathan, *Facebook's Privacy Meltdown after Cambridge Analytica is Far From Over* (Mar. 18, 2019, 6:00 AM), https://www.theguardian.com/uk-news/commentisfree/2019/mar/18/cambridge-analytica-chernobyl-privacy, [https://perma.cc/52R5-5SJ7] ("The

The transfer of data by Kogan violated Facebook's terms of use, which prohibited data from being sold or transferred "to any ad network, data broker or other advertising or monetization-related service."[29] But Facebook failed to police that policy. In 2015, reports began appearing about Cambridge Analytica's use of data harvested from Facebook.[30] Facebook then "demanded that Kogan, Cambridge Analytica, and its SCL affiliates delete all Facebook data in their possession."[31] But, "[w]hile Kogan and SCL Elections certified to Facebook that they had deleted the data obtained through the GSRApp, individuals or other entities still possess this data and/or data models based on this data."[32] Facebook's failure to police that use or to recognize the enormous harvesting of information that Kogan was undertaking would cost it dearly. It was only in March 2018 that Facebook suspended Cambridge Analytica and SCL Group from its platform.[33] It paid $5 billion in a settlement to the U.S. Federal Trade Commission,[34] $100 million in a settlement with the U.S. Securities and Exchange Commission,[35] and £500,000 in a settlement with the UK Information Commissioner's Office.[36]

The Cambridge Analytica debacle casts a long shadow. Table I below shows the number of articles mentioning Facebook and Cambridge Analytica since the scandal was exposed in 2018.

---

fact is that if you want to target political advertisements precisely to move voters who have expressed interest in particular issues or share certain interests, there is an ideal tool to use that does not rely on pseudoscience. It's called Facebook.").

29. Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html [https://perma.cc/7MQQ-VP2D].

30. *See, e.g.*, Harry Davies, *Ted Cruz Using Firm That Harvested Data on Millions of Unwitting Facebook Users*, THE GUARDIAN (Dec. 11, 2015, 5:22 PM), https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data [https://perma.cc/BE7G-2DBJ]

31. F.T.C. Complaint, *supra* note 20, at *6.

32. *Id.*

33. Paul Grewal, *Suspending Cambridge Analytica and SCL Group From Facebook*, FACEBOOK (Mar. 16, 2018), https://about.fb.com/news/2018/03/suspending-cambridge-analytica/ [https://perma.cc/L6RS-GX4N].

34. Lesley Fair, *FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making*, F.T.C. (July 24, 2019, 8:52 AM), https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history [https://perma.cc/73U7-NGMB].

35. Press Release, SEC, Facebook to Pay $100 Million for Misleading Invs. About the Risks It Faced from Misuse of User Data (July 24, 2019), https://www.sec.gov/news/press-release/2019-140 [https://perma.cc/Z9EJ-W5E4].

36. *Facebook Reaches Settlement with ICO Over £500,000 Data Protection Fine*, HUNTON ANDREWS KURTH: PRIV. & INFO. SEC. L. BLOG (Nov. 5, 2019), huntonprivacyblog.com/2019/11/05/uk-ico-imposes-maximum-fine-on-facebook-for-compromising-user-data/ [https://perma.cc/NAR4-RWR4]; *Statement on an Agreement Reached Between Facebook and the ICO*, INFO. COMM'R'S OFF. (Oct. 30, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/10/statement-on-an-agreement-reached-between-facebook-and-the-ico/ [https://perma.cc/6QJS-2AFZ].

Table 1. The Long Shadow of Cambridge Analytica: Newspaper articles mentioning both Facebook and Cambridge Analytica.[37]

Year	Number of articles
2018	15,123
2019	3,962
2020	1,185
2021	651 (through Oct. 17, 2021)

While the intense scrutiny of Facebook's relationship with Cambridge Analytica has ebbed from its enormous heights in 2018, it is very much a part of the ongoing debate on Facebook's data management.

III. Breaking Down Barriers to Access: Data Sharing Proposals in the U.S., EU, and India

Facebook has continued sharing data with researchers, but many complain that the terms, the kinds of data shared, and its quality are unreasonable.[38]

A. U.S. Law Proposal: Platform Transparency and Accountability Act

Stanford law professor Nathaniel Persily has suggested a U.S. law that would mandate data sharing by large social media platforms with vetted researchers.[39] His proposed "Platform Transparency and Accountability Act" would require large social media platforms (defined as ones with 40 million or more monthly active users) to follow FTC rules (promulgated pursuant to the Act) on sharing data with qualified researchers.[40] Persily would seek to escape the shadow of Cambridge Analytica by compelling the sharing, but

37. Search Query, PROQUEST NEWS & NEWSPAPERS (Nov. 1, 2021) (search "Facebook" and "Cambridge Analytica").

38. *See, e.g.*, Lauren Edelson & Damon McCoy, *We Research Misinformation on Facebook. It Just Disabled Our Accounts.*, N.Y. TIMES (Aug. 10, 2021), https://www.nytimes.com/2021/08/10/opinion/facebook-misinformation.html [https://perma.cc/M2YU-RPK3].

39. Nathaniel Persily, *Facebook Hides Data Showing It Harms Users. Outside Scholars Need Access.*, WASH. POST (Oct. 5, 2021, 7:20 AM), https://www.washingtonpost.com/outlook/2021/10/05/facebook-research-data-haugen-congress-regulation/ [https://perma.cc/E2LZ-XJZV].

40. *Id.*

also by immunizing the platform for any wrongs resulting from the release of that data pursuant to the rules.[41] His bill provides:

> No cause of action under state or federal law relating to or arising solely from the release of data to Qualified Researchers may be brought against any Qualified Platform that complies with this Act and the privacy and cybersecurity provisions described herein.[42]

There are likely some who will recoil at the prospect of offering immunities to a big technology enterprise. After all, shouldn't they be subject to the general liability laws? But it would seem unfair to require them to turn over data to researchers, and then hold them liable for sharing that data or for any misuse that might occur after they share the data. An immunity provision would save them from having to win on the merits of the claim, though there would still be a challenge to whether the social media enterprise qualified for the immunity on the ground that the enterprise failed to meet the FTC-mandated terms for information sharing.

However, because Facebook's networks almost inevitably cross borders, some of the information that may be required to be shared might well be from outside the United States. A U.S. immunity law would not protect Facebook from claims brought outside the U.S. under foreign law. This brings us to foreign law, to which we now turn.

B. EU Law Proposal: Data Governance Act

One concern for Facebook and other platforms in engaging in such sharing is the European Union's General Data Protection Regulation (GDPR). While the GDPR explicitly acknowledges the importance of research, its extensive obligations generally follow the data, with only limited variation for research. For example, the GDPR's Recital 33 recognizes that researchers may not be able to anticipate how exactly the data will be used: "It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection."[43] Recital 33 continues:

---

41. Nathaniel Persily, *A Proposal for Researcher Access to Platform Data: The Platform Transparency and Accountability Act*, J. ONLINE TRUST & SAFETY, Oct. 2021, at 1, 5.

42. Justin Hendrix, *Stanford Professor Proposes "Platform Transparency and Accountability Act,"* TECH POL'Y PRESS (Oct. 5, 2021), https://techpolicy.press/stanford-professor-proposes-platform-transparency-and-accountability-act/ [https://perma.cc/24DJ-DYZA].

43. Commission Regulation 2016/679 of Apr. 27, 2016, General Data Protection Regulation, 2016 O.J. (L 119) 1, 6.

> Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.[44]

The easing of purpose specification suggested here is not entirely clear. Indeed, it is not even clear what "scientific research" is. Article 89 uses the terms "scientific or historical research purposes or statistical purposes," though those terms do not define themselves.[45] The expectation seems to be that national laws will clarify the scope of the rules for research. Recital 156 makes that clear:

> Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[46]

Relying upon Member State laws increases the burden of conducting cross-border research that may involve individuals from across the twenty-seven member bloc and increases the possibility that certain research applications may not be legal in one of those states.

This is not a theoretical possibility. One private observer group reports that "organisations often report reticence and caution when embarking on data-sharing projects, for fear of breaching applicable data protection laws or due to a lack of clarity on what regulators and the public may expect."[47] The European Commission has itself observed the problem of fragmentation

44. *Id.*

45. *Id.* at 84–85.

46. *Id.* at 29.

47. *Centre for Information Policy Leadership's Response to the EU Commission's Consultation on a European Strategy for Data*, (Ctr. for Info. Pol'y Leadership) May 29, 2020, at 7, https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/06/cipl_response_to_the_eu_commissions_consultation_on_a_european_strategy_for_data__29_may_2020_.pdf [https://perma.cc/JN9Z-SRFY].

between Member States, including adaptations (such as the Finnish law on secondary use of health and social data, creating a data permit authority) for scientific research.[48]

The European Union's proposed Data Governance Act[49] may offer some hope for researchers. It promises public sector data for research and other purposes and also allows the private sector to donate data to a new type of not-for-profit, a "data altruism organisation."[50] It would also establish a European Data Innovation Board.[51]

But what if something goes wrong at the data intermediary or the data altruism organization, despite certifications and other safeguards? It is not fanciful to imagine a data breach from a rogue employee or an external hacker utilizing an unknown software defect. Unlike Persily's proposed bill, the Data Governance Act does not immunize the data provider for any harms that might flow from such a breach. Furthermore, the relationship between the Data Governance Act and the GDPR is not clear, so even if a data supplier is following the safeguards built into the Data Governance Act, that supplier could still be in violation of the GDPR based on the transfer of data. The Council of the European Union would make it clear that the Data Governance Act would not establish a basis for processing of personal data.[52]

C. Indian Law Proposal: Non-Personal Data Framework

In a vision that seems consistent with Kadri's concern to break down barriers to competition, India initially proposed a law, the Non-Personal Data Governance Framework, that would require big technology companies to share data with smaller firms.[53] This seemed designed to promote local businesses at the expense of mostly American multinationals. As Amba Kak and Samm Sacks observe, this led to a firestorm of criticism—not only from domestic and foreign businesses that complained "that coercive data sharing would impinge on intellectual property rights and commercial interests in datasets," but also from civil-society advocates who cited "data privacy and

48. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data*, at 6, COM (2020) 66 final (Feb. 19, 2020).

49. *Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)*, COM (2020) 767 final (Nov. 25, 2020).

50. *Id.*

51. *Id.*

52. Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act), No. 2020/0340 (COD) of Sept. 24, 2021, 3.

53. AMBA KAK & SAMM SACKS, SHIFTING NARRATIVES AND EMERGENT TRENDS IN DATA-GOVERNANCE POLICY: DEVELOPMENTS IN CHINA, INDIA, AND THE EU 5–6 (2021).

security concerns."[54] The Indian government relented, removing the compelled data sharing between two private firms from the latest draft.[55] The current version of the draft focuses largely on the creation of anonymized "high-value datasets" that are based on private sector data, but managed by data trustees and available to researchers and startups, alike.[56]

Conclusion

Return to Epstein's server as the castle of the contemporary corporation. That argument proves unpersuasive for a number of reasons. First, property rights over real property were never absolute, but subject to incursions for various purposes. Second, even if a corporation has legal personality, we may conclude that certain sticks in the bundle of rights employed by an individual should not follow. Third, a server is not a castle—the number of ordinary, welcome visitors is multiple magnitudes higher. The complexity of managing those contractual negotiations would overwhelm many mutually beneficial exchanges. Finally, as the California Supreme Court argued, Epstein's argument would transform trespass to chattels into trespass to real property.[57] Trespass to chattels by electronic means, the Court declared, must either "damage[] the recipient computer system [or] impair[] its functioning."[58]

In a recent case, the Ninth Circuit seemed to adopt a more Epstein-like approach than the California Supreme Court, permitting a claim of trespass to chattels to go forward on the basis of Facebook embedding code in third-party websites (presumably with permission from the websites) that tracks users visiting those sites.[59] Here, it is not Facebook that is the digital gatekeeper seeking to keep others out, but the individual web user, whose internet

54. *Id.*

55. Anupriya Dhonchak, *Revised Non-Personal Data Governance Framework and Intellectual Property Implications – Part I*, SPICY IP (Feb. 9, 2021), https://spicyip.com/2021/02/revised-non-personal-data-governance-framework-and-intellectual-property-implications-part-i.html [https://perma.cc/FDL3-NQYF] ("Data sharing between two or more for-profit private entities has been done away with under the new report.").

56. MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA, REPORT BY THE COMMITTEE OF EXPERTS ON NON-PERSONAL DATA GOVERNANCE FRAMEWORK (Dec. 16, 2020), https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf [https://perma.cc/NZD2-RD3A].

.

57. Intel Corp. v. Hamidi, 71 P.3d 296, 309 (2003).

58. *Id.* at 300.

59. *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 596 (9th Cir. 2020) ("Facebook facilitated this practice by embedding third-party plug-ins on third-party web pages. The plug-ins, such as Facebook's 'Like' button, contain bits of Facebook code. When a user visits a page that includes these plug-ins, this code is able to replicate and send the user data to Facebook through a separate, but simultaneous, channel in a manner undetectable by the user."), *cert. denied sub nom.* Facebook, Inc. v. Davis, 141 S. Ct. 1684 (2021).

has been allegedly trespassed by Facebook's invisible code found on third-party websites that the user visits. This scenario inverts Kadri's framing, and the court reaches a result that seems to magnify gatekeeper power. The Ninth Circuit interpreted the California Supreme Court's ruling in *Hamidi* as follows: "To prevail on a claim for trespass to chattels, Plaintiffs must demonstrate that some actual injury may have occurred and that the owner of the property at issue may only recover the actual damages suffered as a result of the defendant's actions."[60] The Ninth Circuit did not seem to ask whether the user's chattel (here, a computer) was in fact plausibly trespassed when the user visited a website with Facebook code.

Kadri offers a much more persuasive argument that would control the extent of gatekeeper power. But setting the exact limits of gatekeeper power will prove a complex undertaking, requiring more work from superb scholars like Kadri.[61]

60. *Id.* at 599 n.4 (citing *Hamidi*, 71 P.3d at 39–40).

61. *See, e.g.*, Thomas Kadri, *Platforms as Blackacres*, 68 UCLA L. REV. (forthcoming Nov. 2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3742086.