# JUDICIAL INDEPENDENCE AND THE CORPORATE 'CUSTODIANS' OF DIGITAL TOOLS:[1] A CALL TO SCRUTINIZE RELIANCE ON PRIVATE PLATFORMS AS 'ESSENTIAL INFRASTRUCTURE'

Karen ELTIS
*Full Professor*
*Civil Law Faculty, University of Ottawa*

"In a lot of ways, Facebook is more like a government than a traditional company."[2]

Mark Zuckerberg

## Introduction

Digital technologies – and their corollary misuse (or even weaponization)[3] – are briskly transforming democratic institutions generally, and altering how "law is disseminated throughout and used by the…public,"[4] more specifically. The eco-system in which courts operate has shifted – a shift sharpened abruptly by the pandemic, as justice precipitously migrated to private platforms and private technology.[5] The COVID-19 pandemic precipitated and spurred judicial digitization "on a scale and at a pace that our court system

1. T. Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media*, New Haven, Yale University Press, 2018.

2. D. Kirkpatrick, "The Facebook Defect," 12 April 2018, available at www.time.com/5237458/the-facebook-defect/. See also H. Whitney, "Search Engines, Social Media, and the Editorial Analogy," 27 February 2018, *Knight First Amendment Institute at Columbia University*, fn 187, available at www.knightcolumbia.org/content/search-engines-social-media-and-editorial-analogy.

3. CybeRighTech, "Prof Irwin Cotler – A Must-Watch Speech on Technology, Regulation and Human Rights," 1 November 2020, at 00h:01m:57s, online (video): *YouTube* www.youtube.com/watch?v=PnMc1CJdqR4.

4. N. Feigenson and C. Spiesel, *Law on Display: The Digital Transformation of Legal Persuasion and Judgment*, New York, New York University Press, 2009.

5. A term broadly and generically used here.



406540FKH_AILAW_livre.indb 153 10/05/2023 14:16:27

would never have contemplated just a few months ago,"[6] visibly culminating in a number of scourts worldwide conducting proceedings on Zoom and the like.[7] This de facto marriage'of convenience' may best be characterized as an *ad hoc*, unstructured partnership prematurely born out of necessity. For instance, Zoom, simply described as "a multi-faceted cloud communications platform for video, voice, content sharing, and chat,"[8] faced several class action lawsuits for alleged privacy violations, a mere few months into the "cyberpandemic."[9] At writing, not unlike other similar platforms, Zoom, not unlike Microsoft Teams stores data (including but not limited to that of courts) onto the Cloud.[10]

While it exceeds the narrow scope of this present endeavor to delve further into this most pressing issue, storage of sensitive litigant data invites further reflection, as does the issue of Predictive analytics are similarly seeping into a justice system that inadvertantly privatizes its datas.

In effect, a "new normal" defined by a general and abrupt dependance on "a few dominant internet intermediaries act[ing] as gatekeepers in the curation, distribution and monetization of information"[11] is ripe for rigorous scrutiny. A great deal is at stake when intermediaries "[o]ffering services 'for free'…profit from profiling and commercializing the public sphere"[12] more generally. This is exponentially true, few would query, in the judicial context.

Mindful of this gargantuan communications and infrastructure reallocation, the following posits that judicial independence must now be understood in the context of platform-dependent modern communications in the digital realm. What previously struck most as incredulous let alone unfeasible is

6. The Every Lawyer, "Digitalizing Our Courts," 24 June 2020, *Canadian Bar Association*, at 00 h m30s, online (podcast): www.cba.org/Publications-Resources/Podcasts/All.

7. See *ibid.*; "Covid-19 Forces Courts to Hold Proceedings Online," 14 June 2020, *Economist*, available at www.economist.com/international/2020/06/14/covid-19-forces-courts-to-hold-proceedings-online.

8. Onna Technologies, "The Beginner's Guide to Zoom eDiscovery," 1 October 2020, *JDSupra*, available at www.jdsupra.com/legalnews/the-beginner-s-guide-to-zoom-ediscovery-42363/.

9. See Y. UNNA, "How Zoom Colonized Our Lives," 25 June 2019, Cyberweek, Blavatnik ICRC Tel Aviv University. See also M. STUBBS, "Zoom Faces Multiple Class Action Lawsuits Over Privacy Complaints," last updated on 25 June 2020, available at *Expert Institute* www.expertinstitute.com/resources/insights/zoom-video-faces-multiple-class-action-suits-over-privacy-complaints/.

10. More generally, see L. DIGNAN, "Zoom Aims to Meld Remote, In-Office Collaboration to Prep for Hybrid Workplaces," 3 February 2021, *ZDNet*, available at www.zdnet.com/article/zoom-aims-to-meld-remote-in-office-collaboration-to-prep-for-hybrid-workplaces/.

11. J. HAAS, "Freedom of the Media and Artificial Intelligence," 16 November 2020, Office of the OSCE, Government of Canada, p. 1, online (pdf): www.international.gc.ca/campaign-campagne/assets/pdfs/media_freedom-liberte_presse-2020/policy_paper-documents_orientation-ai-ia-en.pdf.

12. J. HAAS, "Freedom of the Media and Artificial Intelligence," *op. cit.*, p. 2.



406540FKH_AILAW_livre.indb 154 10/05/2023 14:16:27

now commonplace in justice systems across jurisdictions globally.[13] Whereas innovation tailored to palliate the disquieting backlog that has haunted courts and tribunals for years is best greeted with openness – if not enthusiasm, – recognizing the necessity of digitizing, this article endeavors to shed light on the perils to judicial independence inherent to unbridled dependence on foreign commercial platforms. While these concerns are largely obscured by both the urgency and convenience of hastily transitioning online during the persisting pandemic, the long-term impact of this partnership is ripe for sober scrutiny. Thus, underscoring the risk of compromising the foundational principle of judicial independence in the age of default platform infrastructure, the following calls for mechanisms tailored to ensure that intermediary partnerships are mindful and structured ('*balisé*'), rather than dangerously and anachronistically ad hoc.

## I. INADVERTENTLY TRANSPOSING OPACITY AND THE 'SURVEILLANCE CAPITALISM'[14] MODEL TO JUSTICE?

As the below discussion reveals, public use of private infrastructure and its increasingly essential character is an ambiguous relationship at best. Such partnerships are of particular concern for courts: safeguarding judicial independence and insulating courts from unmitigated (or any real or perceived) dependence on private commercial actors is of paramount importance. If nothing else, this article seeks to highlight the conspicuous and insidious absence of verifiable parameters for these delicate collaborations.

Accordingly, adequately framing this private-public relationship and abating creeping judicial dependence on commercial platforms is of the essence. Recognizing the need for courts to maintain control and curtail reliance on private intermediaries, the following is a first attempt to grapple with the challenges that mirror the opportunities of the digital age. As a starting point to ultimately engendering reflection beyond this piece, we suggest that the German concept of Drittwirkung[15] is helpful in the quest to frame these (at least temporarily necessary) alliances. As has been submitted elsewhere, and in order to respect constitutional values in the digital age, enshrined constitutional rights may be upheld not only against the state but "against

13. CBA COVID TASKFORCE Report, https://www.cba.org/CBAMediaLibrary/cba_na/PDFs/Publications%20And%20Resources/2021/CBATaskForce.pdf.

14. Sh. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, PublicAffairs, 2019.

15. A German legal doctrine meaning "third party effect" and used to transpose fundamental rights onto private law relations, see E. ENGLE, "Third Party Effect of Fundamental Rights (*Drittwirkung*)," 2009 *Hanse L. Rev.* 5:2, p. 165.



406540FKH_AILAW_livre.indb 155 10/05/2023 14:16:27

any group in society that is sufficiently powerful to functionally substitute for the state."[16] In other words, there may be an affirmative constitutional responsibility to interpret law in a way that protects citizens against the actions of private groups who exercise what Lapidoth, in a different context called "functional sovereignty."[17]

## II. In the Interim – Drittwirkung and Considering Fiduciary Duties

In addition to Drittwirkung, the concept of fiduciary duties, explored in great detail elsewhere,[18] similarly finds relevance in this context as we devise more robust solutions. While we do not seek to address this exhaustively, it suffices to raise the concept for further deliberation. In a word, "[t]he information-fiduciary model is an instance of a larger trend in theories of digital privacy – a movement to viewing privacy in relational terms of trust and trustworthiness."[19]

Plainly put, information fiduciaries have three basic kinds of duties toward their end users: a duty of confidentiality, a duty of care, and a duty of loyalty. These fiduciary duties must also "run with the data:" digital companies must ensure that anyone who shares or uses the data is equally trustworthy and is legally bound by the same legal requirements of confidentiality, care, and loyalty as they are.[20]

Although beyond the scope of this modest exposition, this model has been proffered by leading Internet governance scholars, such as Jack Balkin, as a sine qua non or first (although, we submit, not necessarily sufficient) standard for ensuring that platforms and other transnational data-collecting cyberactors meet a basic standard of legality in engaging with the public in the justice arena;[21] that is, as we await more robust governance frameworks.

16. CA 6024/97 *Shavit v Rishon Lezion Jewish Burial Society*, [1999] IsrSC 53(3) 600, [1998-9] IsrLR 259 (Israel) (for an ostensibly private body providing public functions and therefore subject to the constitutional normative framework such as protecting human dignity).

17. R. Lapidoth, "Sovereignty in Transition," 1992 *J. Intl Affairs* 45:2, p. 333. See also K. Eltis and I. Siatitsa, "Realigning the Law to Better Uphold the State's Duty to Protect Human Rights: Towards an Interoperable Model for Addressing Racism and Strengthening Democratic Legitimacy," in Y. Shany (ed.), *Reducing Online Hate Speech: Recommendations for Social Media Companies and Internet Intermediaries*, Jerusalem, The Israel Democracy Institute, 2020, 187.

18. J.M. Balkin, "The Fiduciary Model of Privacy," 2020 *Harv L. Rev.* 134:1, p. 11; P. Trudel on Civil Law perspective as term is used differently.

19. J.M. Balkin, "The Fiduciary Model of Privacy," *op. cit.*, pp. 15-16.

20. J.M. Balkin, "The Fiduciary Model of Privacy," *op. cit.*, pp. 14, 17.

21. J.M. Balkin, "The Fiduciary Model of Privacy," *op. cit.* See also J.M. Balkin, "Information Fiduciaries and the First Amendment," 2016 *UC Davis L. Rev.* 49:4, p. 1183.



406540FKH_AILAW_livre.indb 156 10/05/2023 14:16:27

## III. CONTEXT: A FEW WORDS ON JUDICIAL INDEPENDENCE

The effectiveness and legitimacy of the judiciary is largely rooted in its independence. The public is more likely to trust the judiciary if it renders decisions "impartially and disinterestedly, shielded from inappropriate external influences and political pressures."[22] Accordingly, judges should be insulated from politicization and improper influence.[23]

These, of course, take the forms of the Constitution and legislation, but also conventions and unwritten principles, with judicial independence having three components and two dimensions. The three components are, of course, security of tenure, financial security and administrative autonomy. The dimensions – and this is important – are both individual and collective.

Of the three main elements inherent to judicial independence, administrative independence, and its perception, appears most jeopardized under the circumstances discussed here. Increased dependence on platforms like Zoom and Microsoft Teams inter alia imperils the very foundation of these principles by potentially introducing the apprehension of external pressures (or the perception thereof).[24]

So too, a significant component of judicial independence is transparency, accountability, and control. As Professor Farrow observed in a different context: "From the early days of the Magna Carta, all the way up to the current judgments of the Supreme Court of Canada, it is key to Canada's functioning democracy that we are ruled by laws, not humans. That is a core element of our democratic system."[25] For our purposes then, reliance and – a fortiori – over-reliance on private platforms and the like threatens to supplant laws and institutions with foreign commercial intermediaries and the opaque algorithms that they mysteriously deploy for profit; so, the influences that judicial independence is meant to shield judges from operating, as Peter Russell has said, "at a level more subtle than the threat of

22. K. ELTIS and F. GÉLINAS, "Judicial Independence and the Politics of Depoliticization," 23 March 2009, 1 at 1, online (pdf): *SSRN* papers.ssrn.com/sol3/papers.cfm?abstract_id=1366242. See also K. BENYEKHLEF, N. VERMEYS and S. MIZRAHI, "Zooming in on the Importance of Upholding Legal Values in Virtual Trials," 18 June 2020, online (blog): *Slaw* www.slaw.ca/2020/06/18/zooming-in-on-the-importance-of-upholding-legal-values-in-virtual-trials/.

23. K. ELTIS and F. GÉLINAS, "Judicial Independence and the Politics of Depoliticization," *op. cit.*

24. See also *Basic Principles on the Independence of the Judiciary, Adopted by the Seventh United Nations Congress on the Prevention of Crime and the Treatment of Offenders held at Milan from 26 August to 6 September 1985*, GA Res 40/32 and 40/146 29, UNGAOR, 1985.

25. "Bill C-58, An Act to amend the Access to Information Act and the Privacy Act and to make consequential amendments to other Acts," Senate, Standing Committee on Legal and Constitutional Affairs, 20 February 2019 *Evidence*, 42-1, No. 55, at 16:15 (Trevor CW Farrow).



406540FKH_AILAW_livre.indb 157 10/05/2023 14:16:27

removal."[26] This is where the digital age component becomes especially salient to the reflection process on these said "subtle influences" on judicial independence.[27]

## IV. JUDICIAL INDEPENDENCE WITH ZOOM ET AL. AS 'CRITICAL INFRASTRUCTURE'

In light of the above, what is the place of courts within this architecture of "planetary-scale computation…[that] distorts and reforms modern jurisdiction and political geography and produces new forms of these in its own image?"[28] The concern, as previously noted, is what "we don't know we don't know."[29] Who is to say what these platforms will eventually do (even inadvertently) with a treasure trove of judicial process data?[30]

In this delicate context, it stands to reason that seemingly innocuous dependence on commercial actors risks bringing individual justices and themselves into disrepute.[31] The conundrum, briefly summarized, is as follows: As many courts, to our collective chagrin, are under-resourced, keeping up with Silicon Valley – or at the very least entrusting private platforms with supporting digital Justice – is understandably tempting.[32] All the more so as these pre-existing difficulties and inadequacies are compounded by an unforeseen and seemingly protracted pandemic.[33]

More broadly, this expedient yet thoroughly spontaneous and amorphous marriage of necessity between courts and platforms (and other intermediaries), is part and parcel of a broader far-reaching phenomenon, beyond the scope of this endeavor. A reality in which, as noted elsewhere, "constitutional rights that democratic nations have toiled to enshrine and interpret are relegated to the largely side-lined brick and mortar world and can be

26. P. RUSSELL, *The Judiciary in Canada: The Third Branch of Government*, Toronto, McGraw-Hill Ryerson, 1987, p. 82.

27. P. RUSSELL, *The Judiciary in Canada: The Third Branch of Government*. See also K. ELTIS and F. GÉLINAS, "Judicial Independence and the Politics of Depoliticization," *op. cit.*, p. 15.

28. B.H. BRATTON, *The Stack: On Software and Sovereignty*, Cambridge, MIT Press, 2015, p. 6.

29. Originally spoken by former US Secretary of Defense, Donald Rumsfeld, during a news briefing, *Known and Unknown: A Memoir*, New York, Sentinel, 2011, p. xiii.

30. See K. ELTIS, *Courts, Litigants, and the Digital Age: Law, Ethics, and Practice*, Toronto, Irwin Law, 2016, ch. 3; K. ELTIS, "Courts in the Digital Age: 'Adaptive Leadership' for Harnessing Technology and Enhancing Access to Justice," in C. HUNT and R. DIAB (eds), *Digital Privacy and the Charter*, Thompson Reuters, 2021, https://store.thomsonreuters.ca/en-ca/products/the-last-frontier-digital-privacy-and-the-charter-softbound-book-42962345.

31. *Ibid.* As noted elsewhere, because of the digital age, commonly available information has been taken out of context and made more accessible, and as a result, the quality of the information decreases.

32. E. DOUEK generally: https://tsjournal.org/index.php/jots/article/view/17.

33. K. ELTIS, "Digitizing Courts," 2020; CBA COVID TASKFORCE Report, *op. cit.*



406540FKH_AILAW_livre.indb 158 10/05/2023 14:16:27

effectively bypassed in the online realm."[34] A space that defies territory that defines most legal concepts,[35] one where courts too are constrained to rapidly migrate to private platforms and their offerings (from banal cloud to assisted AI decision-making).[36]

While the difficulties of transposing and enforcing domestic and international human rights norms to the borderless digital realm are by no means limited to online courts,[37] and by far precede the COVID-19 crisis,[38] the pandemic and its desperate scramble[39] have rendered judicial reliance on platforms as infrastructure seemingly all the more inevitable (or even unavoidable).

As former Chief Justice Beverley McLachlin stated long before the pandemic, access to justice is a question of democracy.[40] Although seemingly obvious it is worth repeating in context. Private alternatives may have their place in the above-highlighted triage but, due to the carefully nurtured imperatives of cherished Constitutional values, they cannot supersede or supplant the public system and courts' institutional authority. Nor can inordinate dependance upon them be permitted or allowed to compromise judicial independence.

Indeed, as a matter of institutional and judicial independence above all, irrespective of immediate convenience, courts must not abdicate their public dispute-resolution function – particularly in light of the broader privatization of constitutional rights adjudication alluded to above.[41]

Consequently, Justice must be zealously selective and overly-cautious when exceptionally (rather than routinely) succumbing to the understandable temptation to defer to private actors as a matter of proximate need and efficiency. This is all the more poignant in the absence of a governing framework.

34. K. ELTIS, "Digitizing Courts," *op. cit.*

35. *Google Inc v Equustek Solutions Inc*, 2017 SCC 34 (which emphasizes the inability of the state to successfully regulate conduct in cyberspace).

36. K. ELTIS, "Extra-Territorial Jurisdiction in the Internet Age: Reflecting on the Effective Emasculation of Domestic Courts on the Heels of Equustek v Google," 26 November 2017, available at *The Federmann Cyber Security Research Center*, www.csrcl.huji.ac.il/people/extra-territoial-jurisdiction-internet-age-reflecting-effective-emasculation-domestic.

37. K. ELTIS, "Extra-Territorial Jurisdiction in the Internet Age: Reflecting on the Effective Emasculation of Domestic Courts on the Heels of Equustek v Google," *op. cit.*

38. K. ELTIS, "Extra-Territorial Jurisdiction in the Internet Age: Reflecting on the Effective Emasculation of Domestic Courts on the Heels of Equustek v Google," *op. cit.*

39. As disputes multiply has amplified the backlog. See CBA Report *supra.*

40. The Right Honourable Beverley McLachlin, "The Decline of Democracy and the Rule of Law: How to Preserve the Rule of Law and Judicial Independence?," remarks at Saskatchewan and Manitoba Courts of Appeal Joint Meeting, 28 September 2017, available at scc-csc.ca/judges-juges/spe-dis/bm-2017-09-28-eng.aspx.

41. This issue is beyond the scope of this discussion.



406540FKH_AILAW_livre.indb 159 10/05/2023 14:16:27

As one of the few scholars to delve into this important matter more generally and beyond the justice context, Rikka Kolu dolefully cautioned that "[t]he increase in private enforcement confounds legal structures and challenges the nation state's monopoly on violence. [T]he technology-driven privatisation of enforcement – from direct enforcement of e-commerce platforms to self-executing smart contracts in the blockchain – brings the ethics of law's coercive nature into the open."[42]

Judith Resnick also observed (in the context of privately supported ODR) that:

> "The foundation of the authority of judges is that their power to impose judgment comes from the structure of adjudication, its constraints, and its public character. If the task of adjudication is replaced with that of shepherding parties toward private conciliation, the independence of judges becomes a goal without a purpose or a constraint. The result is the decline of adjudication's potential to serve and to support democracies."[43]

## V. TORONTO QUAYSIDE PROJECT/SIDEWALK LABS: A CAUTIONARY TALE

One resonant example of these novel, exponentially multiplying, and ungoverned public-private partnerships is the now defunct Sidewalk Labs project in Toronto.[44] The failed Quayside Project epitomizes what Zuboff labeled "the commodification of behavior"[45] from a democratic legitimacy perspective.[46] Although the Project comes from without the justice system, its demise is instructive for our purposes.

Briefly summarized, the defunct Quayside Project was marketed by Google's Sister company, Sidewalk Labs, as a "sustainable and affordable community resulting from innovations in technology and urban design"[47] in an era of "constrained" government resources. It is the epitome of former

42. RIIKKA KOULU, *Law, Technology and Dispute Resolution: Privatisation of Coercion*, New York, Routledge, 2018, available at helda.helsinki.fi//bitstream/handle/10138/311733/Law_Technology_and_Dispute_Resolution.pdf?sequence=1.

43. J. RESNICK, "The Contingency of Openness in Courts: Changing the Experiences and Logistics of the Public's Role in Court-Based ADR," 2015 *Nev. L. J.* 15:1631, p. 1687, available at scholars.law.unlv.edu/cgi/viewcontent.cgi?article=1648&context=nlj.

44. "Toronto Tomorrow," last updated May 2020, available at sidewalktoronto.ca/.

45. Sh. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, *op. cit.*, note 14.

46. P. CONSTANTINIDES, O. HENFRIDSSON and G.G. PARKER, "Platforms and Infrastructures in the Digital Age," 2018, articles in *Advance*, online (pdf): *Informs Pubs Online* ide.mit.edu/sites/default/files/publications/ISR%202018%20Constantinides%20Henfridsson%20Parker%20Editorial.pdf.

47. D.L. DOCTOROFF, "Why We're No Longer Pursuing the Quayside Project – And What's Next for Sidewalk Labs," 7 May 2020, *Medium*, available at medium.com/sidewalk-talk/why-were-no-longer-pursuing-the-quayside-project-and-what-s-next-for-sidewalk-labs-9a61de3fee3a.



406540FKH_AILAW_livre.indb 160 10/05/2023 14:16:27

Google CEO Eric Schmitt's vision of private immixion in the public domain and may be summarized thusly in his own parlance: "give us a city and put us in charge."[48]

Quayside, labeled "Google's Guinea Pig"[49] by critics, was billed to develop a "smart city" on Toronto's waterfront. As the Canadian Civil Liberties Association's director remarked after Sidewalk announced that it was abandoning its project:

> "It is a frightening thought that Toronto may be the testing ground for products designed to leverage data and monitor or ultimately influence human behavior, porting an internet model of surveillance capitalism from our computers to our city streets. What is happening in Toronto is the tip of the iceberg when it comes to erosion of privacy rights in projects that pitch the ability to monitor, count, sort, and track people as a feature, not a flaw. But is this really "smart"? What is at stake is the fundamental human dignity and personal autonomy owed to people who live and move about in our Canadian communities."[50]

For our purposes, courts too, particularly during a global pandemic, are surely no strangers to limited public funds, thereby creating understandable temptation for unconventional partners who may be "put in charge" of the backlog. What seems equally resonant in any opaque public/private marriage of innovative expediency is "[we] know enough about the agreement that [we] think you [the public] would like to know more about the agreement."[51] Further, while cooperation with the private sector is certainly desirable and proper on some fronts, ad hoc private governance of an institution as central to democracy as Justice no less is of utmost trepidation if not alarm.

Governance, it is essential to recall in this vein, includes both "formal and informal control mechanisms."[52] These mechanisms – such as gatekeeping, performance metrics, and relational control tasks – are employed by platform owners (in relation to app developers) to reward and punish behavior, and to establish platform best practices.[53] It stands to reason that this type

48. Sh. DINGMAN, "With Toronto, Alphabet Looks to Revolutionize City-Building," 17 October 2017, *The Globe and Mail*, available at theglobeandmail.com/report-on-business/with-toronto-alphabet-looks-to-revolutionize-city-building/article36634779/.

49. M. SAUTER, "Google's Guinea-Pig City," 13 February 2018, *The Atlantic*, available at theatlantic.com/technology/archive/2018/02/googles-guinea-pig-city/552932/.

50. "Toronto's 'Smart' City," 7 May 2020, *Canadian Civil Liberties Association*, available at ccla.org/waterfront-toronto/.

51. New Yorker Id.

52. A. TIWANA, *Platform Ecosystems: Aligning Architecture, Governance, and Strategy*, Amsterdam, Morgan Kaufmann, 2014, p. 39.

53. A. TIWANA, *Platform Ecosystems: Aligning Architecture, Governance, and Strategy*, *op. cit.*



406540FKH_AILAW_livre.indb 161 10/05/2023 14:16:27

of control may find issue with traditional precepts of judicial independence, which uncompromisingly proscribe reliance on external control mechanisms outside the judiciary's purview.

As Lord Sales cautioned more broadly in a very instructive piece: "[t]he law has to provide structures so that algorithms and AI are used to enhance human capacities, agency and dignity, not to remove them. It has to impose its order on the digital world and must resist being reduced to an irrelevance" (emphasis added).[54]

It should be noted, however, that "[u]nder such a [gatekeeping] arrangement, transparency is minimized, and regulatory and enforcement mechanisms are limited. In turn, individuals have lost control of much of their data, eroding personal privacy, security and autonomy."[5556]

## VI. COURTS "AWASH IN DATA"

The sheer magnitude of the data generated by courts' migration online leaves the justice system particularly vulnerable. As Eric Schmidt, Google's former chief executive observed a decade ago: "From the dawn of civilization to 2003, five exabytes of data were created. The same amount was created in the last two days."[57]

Most significantly perhaps, this model recognizes that all data – including that collected through the justice system – can and ultimately will yield powerful insights and be diverted to known and yet unknown purposes.

54. L. SALES, Justice of the UK Supreme Court, "Algorithms, Artificial Intelligence and the Law," The Sir Henry Brooke Lecture for BAILII delivered at Freshfields Bruckhaus Deringer, London, 12 November 2019, p. 25, online (pdf): bailii.org/bailii/lecture/06.pdf. N. ROSE, "'Deepfake' Warning Over Online Courts," 29 July 2020, *Legal Futures*, available at www.legalfutures.co.uk/latest-news/deepfake-warning-over-online-courts:"Video manipulation software, including 'deepfake' technology, poses problems for remote courts in verifying evidence and that litigants or witnesses are who they say they are, a report has warned. Not only could successful deepfakes find their way into evidence, 'potentially condemning the innocent or exonerating the guilty,' it said, but the mere existence of deepfakes allowed litigants and their lawyers 'to cast doubt on video or audio that is legitimate'".

55. M. LAWRENCE, "Building a Digital Commonwealth: We Need to Rethink How Data and Digital Infrastructure Is Governed, Owned and Used," 13 March 2019, *Open Democracy*, available at www.opendemocracy.net/en/oureconomy/building-digital-commonwealth/.

56. P. CONSTANTINIDES, O. HENFRIDSSON and G. G. PARKER, "Platforms and Infrastructures in the Digital Age," *op. cit.*, p. 14: "The challenge for both platform operators and government representatives charged with protecting citizens' interests is to balance what people *say* they want, against what their actions imply about their preferences. The idea of a property interest in personal data can help users better understand the value of what they are giving away versus the goods and services that systems provide. The EU's proposed tax on pure data platforms, such as Google search, suggests that regulators are exploring such structures."

57. B. CARLSON, "Quote of the Day: Google CEO Compares Data Across Millennia," 3 July 2010, available at *The Atlantic*, www.theatlantic.com/technology/archive/2010/07/quote-of-the-day-google-ceo-compares-data-across-millennia/344989/.



406540FKH_AILAW_livre.indb 162 10/05/2023 14:16:27

As previously noted, the revenue model of most major platforms is one "founded on the extraction and analysis of data generated by users of the platforms for profit and control of the digital infrastructure."[58]

While it is beyond the scope of this endeavor, other entities such as Palantir Legal Intelligence, whose "powerful search capabilities are accessible to anyone with basic computer skills," can scour "public information like web sources and published government data, and even audio recordings."[59]

Moreover, as several scholars – including, but not limited to, Princeton's Arvin Narayanan – have cautioned,[60] commonly used platforms are facing significant rebuke in relation to security flaws. For instance, a security researcher successfully took complete control over a Zoom user's computer as a result of a security vulnerability.[61] Not surprisingly, cybercriminals are increasingly targeting videoconferencing platform users and related.[62] In response, Zoom, for its part, has taken some significant measures to increase platform security.[63] But "[o]rganizations should [also] adopt a consolidated security solution. Otherwise, you end up with big challenges operationally. In the past, the multiplicity of cyber security platforms has served as a blind spot, which has been targeted by malicious actors."[64]

58. M. LAWRENCE, "Building a Digital Commonwealth: We Need to Rethink How Data and Digital Infrastructure Is Governed, Owned and Used," *op. cit.*

59. "Who Needs Our Help," *Palantir Legal Intelligence*, available at www.palantir.com/solutions/legal-intelligence/.

60. K. PAUL, "Worried About Zoom's Privacy Problems? A Guide to Your Video-Conferencing Options," 9 April 2020, available at *The Guardian* theguardian.com/technology/2020/apr/08/zoom-privacy-video-chat-alternatives (quoting Arvin Narayanan); Doc Searls, "Zoom Needs to Clean Up Its Privacy Act," 27 March 2020, *Doc Searls Weblog*, online (blog): www.blogs.harvard.edu/doc/2020/03/27/zoom/.

61. D. REISINGER, "Zoom Bug Gives Hackers Full Control Over Computers," 1 April 2020, *Inc*, available at www.inc.com/don-reisinger/zoom-bug-gives-hackers-full-control-over-computers.html.

62. "Head of Engineering, M. Ostrowski, On Security in the 'New Normal'," 18 September 2020, *Cyber Talk*, available at www.cybertalk.org/2020/09/18/head-of-engineering-mark-ostrowski-on-security-in-the-new-normal/.

63. K. PAUL, "Zoom Releases Security Updates in Response to 'Zoom-Bombings'," 23 April 2020, *The Guardian* available at www.theguardian.com/technology/2020/apr/23/zoom-update-security-encryption-bombing. Zoom has also updated its policies related to the sale of data pursuant to the revelation that the company was sending user data to Facebook for advertising purposes, even where the user did not hold a Facebook account, see J. COX, "Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account," 26 March 2020, *Vice* available at www.vice.com/en/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account.

64. "Head of Engineering, M. Ostrowski, On Security in the 'New Normal'," *op. cit.*



406540FKH_AILAW_livre.indb 163 10/05/2023 14:16:27

## VII. DEEPFAKES DURING AND POST "CYBERPANDEMIC"[65]

While the yet crystalizing, most salient question of deepfakes and evidence in the justice system far exceeds the scope of this present endeavor, it is nonetheless incumbent upon us to raise it.[66] The issues presented in transitioning to online courts and evidence manipulation or other forms of misinformation – including but not limited to deepfakes – are deeply intertwined and invite swift and robust normative "encadrement." Indeed, the matter of ad hoc, unstructured public/private partnerships explored herein (and recently illustrated with Amazon's offer to aid President Biden in the COVID-19 vaccine distribution),[67] epitomizes the thorniness of this reliance.

For instance, and without purporting to offer any sort of analysis at this preliminary stage, US courts have taken to depending on a plethora of novel private companies, whose proprietary facial recognition programs, inter alia, claim to offer some protection from the variety of risks generated by the online transition." For, not surprisingly:

> "AI software companies like SenseTime can create deepfakes from audio sources by using a third party's audio clip and video of the user to generate footage of the user saying the words from the recording. This can not only allow a person to fabricate their identity but can allow a litigant or witness to use their own voice to make the claim that they said something different than what the opposing party claims."[68]

Indeed, underscoring these disturbing implications for the Justice System with which we must immediately grapple,[69] a report on "virtual justice," by New York-based privacy group Surveillance Technology Oversight Project (STOP), noted that parties to online court proceedings may be asked to verify their identity by providing sensitive personal information, biometric data, or facial scans.[70] In the state of Oregon, for instance, judges sign into their virtual court systems using facial recognition.[71] Further, the report warns that:

> "Distrust around digital records has persisted with the advent and ease of photoshopping. Altered evidence can still be introduced if the authenticating party is itself fooled or is lying. In the coming years, courts must also be mindful of emerging AI

65. Y. UNNA, "How Zoom Colonized Our Lives," *op. cit.*

66. B. CHESNEY and D. CITRON, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," 2019 *Cal. L. Rev.* 107, 1753 (for an in-depth discussion on this point).

67. J. KASTRENAKES, "Amazon Offers to Help Biden Administration with Vaccinations,"20 January 2021, *The Verge*, available at www.theverge.com/2021/1/20/22241031/amazon-vaccination-biden-administration.

68. N. ROSE, "'Deepfake' Warning Over Online Courts," *op. cit.*

69. J. ROTHMAN, "In the Age of AI, Is Seeing Still Believing?," 5 November 2018, *The New Yorker*, available at www.newyorker.com/magazine/2018/11/12/in-the-age-of-ai-is-seeing-still-believing (for an overview of "synthetic images" and their consequences).

70. A. FOX CAHN and M. GIDDINGS, "Virtual Justice: Online Courts During COVID-19," 23 July 2020, p. 6, *STOP: Surveillance Technology Oversight Project*, online (pdf): www.stopspying.org/virtual-justice.

71. A. FOX CAHN and M. GIDDINGS, "Virtual Justice: Online Courts During COVID-19," *op. cit.*



406540FKH_AILAW_livre.indb 164 10/05/2023 14:16:27

technology around deepfakes, which allows a user to manipulate images and audio in real time. While this technology is nascent today, it is rapidly advancing and may soon pose a potent threat to trust in online communication."[72]

Thus, "[a]s with today's text-based fake news, the problem is double-edged. Having been deceived by a fake video, one begins to wonder whether many real videos are fake. Eventually, skepticism becomes a strategy in itself."[73]

It stands to reason that, moving forward, courts will not only need to struggle with traditional platforms that already host them in such an impromptu fashion at their whim, but also those private actors whose technology threatens to taint or, at the very least, call into question the judicial process – as well as those who purport to rescue them from these with their own opaque tools. Policymakers should pay close attention to deepfakes in order to mitigate their adverse effects on the court system.

## CONCLUSION – CAUTIONING AGAINST AN "ALGOCRACY" AND THE INFRASTRUCTURE THAT SHIFTS JUSTICE TO PRIVATE HANDS

In light of the above, there lingers little doubt as to the urgency of visiting serious scrutiny on courts' and tribunals' dependence on platforms and intermediaries as a necessary (although perhaps not sufficient) imperative of safeguarding judicial independence.

Increasingly, platforms may come to be defined as public utilities. Thus, "[b]y controlling how this infrastructure is designed and operated, Facebook and Google [inter alia] shape the content and character of our digital public sphere, concentrating not just economic power, but social and political power too."[74] In effect: "a few companies now dominate the construction and maintenance of global digital infrastructures requiring prohibitive amounts of financial and technological resources for market entry… Therefore, further research needs to theoretically grapple with the paradoxical tension of the generative and democratizing force of digital platforms and the monopolistic and controlling force of digital infrastructures."[75]

72. A. FOX CAHN and M. GIDDINGS, "Virtual Justice: Online Courts During COVID-19," *op. cit.*, p. 8.

73. J. ROTHMAN, "In the Age of AI, Is Seeing Still Believing?," *op. cit.*

74. J. SIMONS and D. GHOSH, "Utilities for Democracy: Why and How the Algorithmic Infrastructure of Facebook and Google Must Be Regulated," August 2020, Brookings, available at www.brookings.edu/research/utilities-for-democracy-why-and-how-the-algorithmic-infrastructure-of-facebook-and-google-must-be-regulated/.

75. P. CONSTANTINIDES, O. HENFRIDSSON and G.G. PARKER, "Platforms and Infrastructures in the Digital Age," *op. cit.*, p. 9.



406540FKH_AILAW_livre.indb 165 10/05/2023 14:16:27

Ultimately, it may be fruitful to revisit whether platforms and similar intermediaries should be viewed as "critical infrastructure" and investigate the normative frameworks that best lend themselves to their regulation.

In the short term, and as the "cyberpandemic" constrains us all – including Courts – to rapidly transition to private infrastructure, we must at the very least recognize platforms' fiduciary obligations in the Justice context. As Balkin observes:

> "First, digital companies must accept that they are information fiduciaries toward their end users and toward any persons whose data they collect in the course of their businesses… Second, digital businesses must allow interoperability for other applications, as long as those applications also agree to act as information fiduciaries. Third, digital businesses must allow government regulators to inspect their algorithms for purposes of enforcing competition law, privacy, and consumer protection obligations."[76]

In the medium and longer term, however, the objective is to avoid subsuming Justice in a broader Kafkaesque "algocracy,"[77] thereby potentially giving rise for the need for the doctrine of Drittwirkung, introduced above.

Finally, merely demanding "transparency" of platforms in its traditional sense may not be feasible as AI complexifies, becomes more creative, and escapes its "creator's" intent and meager previsions.[78]

Instead – and in addition to fiduciary duties and Drittwirkung – we must diligently endeavour to focus on the Explanability (rather than transparency) of the algorithmic process, and the possibility of Review and oversight.[79]

For our purposes, the objective, worth reiterating, is curtailing dependence on private infrastructure, as brought into relief by the imperatives of judicial independence, and indeed halting a slide into the privatization of justice – and indeed public service broadly – as a byproduct of the the Covid 19 era.

---

76. M. BALKIN, "Fiduciary Model," *op. cit.*, pp. 32-33.

77. As Ch. RANDELL describes in the Fintech context: "In the 1960s TV series *The Prisoner*, Patrick McGoohan plays a character who is abducted and held captive in an oppressive and surreal community called the Village, where the people have no names, just numbers. He is Number Six. It's impossible to know whom he can trust and who or what the mysterious Number One is that sets the rules of the Village. He is subject to constant surveillance and manipulation", see "How Can We Ensure that Big Data Does Not Make Us Prisoners of Technology?," last updated 11 July 2018, *Financial Conduct Authority*, available at www.fca.org.uk/news/speeches/how-can-we-ensure-big-data-does-not-make-us-prisoners-technology.

78. QUOINE, available at www.quoine.com/api/.

79. Ch. RANDELL available at https://www.fca.org.uk/news/speeches/how-can-we-ensure-big-data-does-not-make-us-prisoners-technology.



406540FKH_AILAW_livre.indb 166 10/05/2023 14:16:27