NATIONAL SECURITY AND FEDERALIZING DATA PRIVACY INFRASTRUCTURE FOR AI GOVERNANCE

*Margaret Hu, Eliott Behar & Davi Ottenheimer**

This Essay contends that data infrastructure, when implemented on a national scale, can transform the way we conceptualize artificial intelligence (AI) governance. AI governance is often viewed as necessary for a wide range of strategic goals, including national security. It is widely understood that allowing AI and generative AI to remain self-regulated by the U.S. AI industry poses significant national security risks. Data infrastructure and AI oversight can assist in multiple goals, including: maintaining data privacy and data integrity; increasing cybersecurity; and guarding against information warfare threats. This Essay concludes that conceptualizing data infrastructure as a form of critical infrastructure can reinforce domestic national security strategies. With the growing threat of AI weaponry and information warfare, data privacy and information security are core to cyber defense and national security. Data infrastructure can be seen as an integrated critical infrastructure strategy in constructing AI governance legally and technically.

INTRODUCTION 1830

I. DATA PRIVACY AS A NATIONAL SECURITY PRIORITY IN THE AGE OF AI 1835

A. AI Governance and National Security 1836

B. Data Privacy Infrastructure as a National Security Priority 1838

* Margaret Hu is the Taylor Reveley Research Professor and Professor of Law, and the Director of the Digital Democracy Lab at William & Mary Law School. Eliott Behar is a data privacy and international human rights attorney. Davi Ottenheimer is the Vice President of Trust and Digital Ethics at Inrupt. The authors are grateful for the editorial leadership of Noah Mathews, Sonia Autret, and Abigail Shaun McCabe. We also wish to extend our gratitude to the support of Frederick Dingledy and Michael Umberger, and the feedback of John Bagby, Yafit Lev-Aretz, Steve Miskinis, Phil Nichols, and the participants of the Data Law and AI Ethics Research Colloquium. This Essay was prepared for the Symposium entitled *The New AI: The Legal and Ethical Implications of ChatGPT and Other Emerging Technologies*, hosted by the *Fordham Law Review* and cosponsored by Fordham University School of Law's Neuroscience and Law Center on November 3, 2023, at Fordham University School of Law.

II. THE FLEMISH DECREE AND FEDERALIZING DATA PRIVACY 1841
A. The Flanders Experiment in Federalizing Data Privacy Infrastructure 1842
B. Integrating Data Privacy Infrastructure into AI Governance 1845
III. FEDERALIZING PRIVACY INFRASTRUCTURE AS A NATIONAL SECURITY DEFENSE STRATEGY 1846
A. Data Privacy and National Security 1846
B. Cyber Defense and Data Privacy Infrastructure 1848
CONCLUSION 1853

INTRODUCTION

Congress and the Executive Branch have proposed and adopted multiple initiatives to address the increasing threats of artificial intelligence (AI) weaponry and cyber conflict.[1] On February 28, 2024, for example, the White House released an Executive Order on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern."[2] The Executive Order was issued pursuant to the International Emergency Economic Powers Act[3] and the National Emergencies Act,[4] and it expanded on two prior Executive Orders:

1. Congress has made multiple efforts to address the threats of foreign interference and foreign influence campaigns. *See, e.g.*, John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636 (2018) (codified as amended in scattered sections of the U.S.C.). Similarly, both Presidents Donald J. Trump and Joseph R. Biden have undertaken measures to address AI-driven risks to information security and national security. *See, e.g.*, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Exec. Order No. 14,110, 88 Fed. Reg. 75191 (Oct. 30, 2023); *Fact Sheet: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI*, WHITE HOUSE (July 21, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/ [https://perma.cc/G84K-L4JQ]; *Fact Sheet: Biden-Harris Administration Secures Voluntary Commitments from Eight Additional Artificial Intelligence Companies to Manage the Risks Posed by AI*, WHITE HOUSE (Sept. 12, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/12/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-eight-additional-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/ [https://perma.cc/6E9G-QTVW]; Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, Exec. Order No. 13,960, 3 C.F.R. § 480 (2020).

2. Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, Exec. Order No. 14,117, 89 Fed. Reg. 15421 (Feb. 28, 2024).

3. 50 U.S.C. §§ 1701–1705.

4. Pub. L. No. 94-412, 90 Stat. 1255 (1976) (codified as amended in scattered sections of the U.S.C.).

Executive Order 13,873,[5] titled "Securing the Information and Communications Technology and Services Supply Chain," and Executive Order 14,034,[6] titled "Protecting Americans' Sensitive Data from Foreign Adversaries."[7] Privacy law experts immediately noted that the Executive Order signaled an important trend in the AI age: the coalescing of data privacy and cybersecurity regulation, on the one hand, and national security regulation, on the other hand, to thwart AI-related national security risks posed by foreign adversaries.[8]

This Essay invites a conversation on whether and how national security advantages can attach to a federalized data privacy infrastructure and, if so, whether it can preempt threats ex ante. Because threats to national security are increasingly manifested through cyberwar and information warfare,[9] as well as through the exploitation of soft war targets,[10] new approaches to generative AI governance—such as the European Union's (EU) AI Act[11] and

5. Securing the Information and Communications Technology and Services Supply Chain, Exec. Order No. 13,873, 3 C.F.R. § 317 (2020); *see* Exec. Order No. 14,117, 89 Fed. Reg. at 15421.

6. Protecting Americans' Sensitive Data from Foreign Adversaries, Exec. Order No. 14,034, 3 C.F.R. § 594 (2022); *see* Exec. Order No. 14,117, 89 Fed. Reg. at 15421.

7. Exec. Order No. 14,117, 89 Fed. Reg. at 15421.

8. *See, e.g.*, Peter Swire & Samm Sacks, *Limiting Data Broker Sales in the Name of U.S. National Security: Questions on Substance and Messaging*, LAWFARE (Feb. 28, 2024, 8:38 PM), https://www.lawfaremedia.org/article/limiting-data-broker-sales-in-the-name-of-u.s.-national-security-questions-on-substance-and-messaging [https://perma.cc/UA98-94Q2].

9. *See, e.g.*, WILLIAM MARCELLINO, CHRISTIAN JOHNSON, MAREK N. POSARD & TODD C. HELMUS, RAND CORP., FOREIGN INTERFERENCE IN THE 2020 ELECTION: TOOLS FOR DETECTING ONLINE ELECTION INTERFERENCE 1 (2020), https://www.rand.org/pubs/research_reports/RRA704-2.html [https://perma.cc/J22B-7JH8] ("In the aftermath of that election, it became clear that agents acting on behalf of the Russian government went online and engaged in a very sophisticated malign information effort meant to sow chaos and inflame partisan divides in the U.S. electorate."); Ellen Nakashima, Karoun Demirjian & Philip Rucker, *Top U.S. Intelligence Official: Russia Meddled in Election by Hacking, Spreading of Propaganda*, WASH. POST (Jan. 5, 2017, 9:17 PM), https://www.washingtonpost.com/world/national-security/top-us-cyber-officials-russia-poses-a-major-threat-to-the-countrys-infrastructure-and-networks/2017/01/05/36a60b42-d34c-11e6-9cb0-54ab630851e8_story.html [https://perma.cc/XT38-VWN9].

10. U.S. DEP'T OF HOMELAND SEC., SOFT TARGETS AND CROWDED PLACES SECURITY PLAN OVERVIEW 1–2 (2018), https://www.cisa.gov/sites/default/files/publications/DHS-Soft-Target-Crowded-Place-Security-Plan-Overview-052018-508_0.pdf [https://perma.cc/D852-2FNP].

11. European Parliament Press Release 20231206IPR15699, Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI (Sept. 12, 2023), https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai [https://perma.cc/B3Q9-ZL7V]; *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:52021PC0206 [https://perma.cc/7Q44-FZYL].

China's recent AI regulatory framework[12]—must be studied and debated on national security grounds as well as consumer protection grounds.

With rapid advances in AI weaponry and cyberwar, data privacy and information security form a key strategic backbone to any effective national security strategy, especially when information warfare increasingly joins and commingles with other threats to sovereignty and national defense.[13] It is widely understood that allowing generative AI to remain self-regulated in the United States poses risks to national security.[14] In addition, AI governance is often viewed as necessary for a wide range of oversight functions.[15]

What is not easily understood is how AI governance, through the federalization of data infrastructure, may potentially reinforce domestic national security strategies. In a field as nascent as AI, the need for generative AI regulation is often prioritized in private law contexts that focus on how generative AI might adversely impact individual citizens, such as individual users and AI technology consumers.[16]

This Essay proposes how and why data privacy infrastructure can serve a role in deepening our understanding of critical infrastructures. Currently, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA) is guided by critical infrastructure principles as set forth by Presidential Policy Directive 21 (PPD-21), titled "Critical Infrastructure

12. *See generally* Matt Sheehan, China's AI Regulations and How They Get Made (July 10, 2023) (unpublished manuscript), https://carnegieendowment.org/files/202307-Sheehan_Chinese%20AI%20gov.pdf [https://perma.cc/FQT8-6FYW].

13. *See generally* U.S. DEP'T OF DEF., STRATEGY FOR OPERATIONS IN THE INFORMATION ENVIRONMENT (2023), https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-DEPARTMENT-OF-DEFENSE-STRATEGY-FOR-OPERATIONS-IN-THE-INFORMATION-ENVIRONMENT.PDF [https://perma.cc/8RT9-SX39].

14. *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFF., GAO-23-106782, SCIENCE & TECH SPOTLIGHT: GENERATIVE AI 1 (2023), https://www.gao.gov/assets/830/826491.pdf [https://perma.cc/6BKT-HAUM] (noting that "[g]enerative AI may also spread disinformation and presents substantial risks to national security"); WILLIAM MARCELLINO, NATHAN BEAUCHAMP-MUSTAFAGA, AMANDA KERRIGAN, LEV NAVARRE CHAO & JACKSON SMITH, RAND CORP., THE RISE OF GENERATIVE AI AND THE COMING ERA OF SOCIAL MEDIA MANIPULATION 3.0: NEXT-GENERATION CHINESE ASTROTURFING AND COPING WITH UBIQUITOUS AI 2 (2023), https://www.rand.org/pubs/perspectives/PEA2679-1.html [https://perma.cc/H3X6-BUSY].

15. *See* Bernd W. Wirtz, Jan C. Weyerer & Benjamin J. Sturm, *The Dark Sides of Artificial Intelligence: An Integrated AI Governance Framework for Public Administration*, 43 INT'L J. PUB. ADMIN. 818, 818–20, 827 (2020); Tim Mucci & Cole Stryker, *What Is AI Governance?*, IBM (Nov. 28, 2023), https://www.ibm.com/topics/ai-governance [https://perma.cc/YYB9-CABZ] ("AI governance encompasses oversight mechanisms that address risks like bias, privacy infringement and misuse while fostering innovation and trust."); *see also* DAN HUTTENLOCHER, ASU OZDAGLAR & DAVID GOLDSTON, MIT AD HOC COMM. ON AI REG., A FRAMEWORK FOR U.S. AI GOVERNANCE: CREATING A SAFE AND THRIVING AI SECTOR (2023), https://computing.mit.edu/wp-content/uploads/2023/11/AIPolicyBrief.pdf [https://perma.cc/5L8F-XK45] (noting that the effective implementation of AI requires prioritizing "security," "individual privacy and autonomy," "safety," "shared prosperity," and "democratic and civic values").

16. *See, e.g.*, Gai Sher & Ariela Benchlouch, *The Privacy Paradox with AI*, REUTERS (Oct. 31, 2023, 1:15 PM), https://www.reuters.com/legal/legalindustry/privacy-paradox-with-ai-2023-10-31/ [https://perma.cc/ZFG8-3PMB].

Security and Resilience."[17] There are currently sixteen sectors designated as critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.[18] After revelations of foreign interference in the 2016 U.S. presidential elections,[19] election infrastructure was designated as part of critical infrastructure under CISA through the government facilities subsector designation.[20]

The foreign interference in the 2016 election provided a window into not only why influence campaigns and disinformation/misinformation campaigns threaten democracy, but also why data privacy and data protection are now national security priorities. Some countries have embraced a "wave of protectionist [data] localization measures"[21] and digital balkanization, sometimes referred to as splinternet, to safeguard national security interests.[22] This type of data protectionism and digital protectionist localization has been criticized as inconsistent with U.S. national security strategy.[23] Cyber balkanization may include erecting parallel internets and internet firewalls, and restricting—or building in the capacity to cut—internet access for political reasons.[24]

---

17. *See Critical Infrastructure Sectors*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors [https://perma.cc/677P-J4E7] (last visited Mar. 3, 2024); *see also* Directive on Critical Infrastructure Security and Resilience, 2013 DAILY COMP. PRES. DOC. 92 (Feb. 12, 2013).

18. *See Critical Infrastructure Sectors*, *supra* note 17.

19. *See* Nakashima et al., *supra* note 9.

20. *Election Security*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/election-security [https://perma.cc/42V5-MQQG] (last visited Mar. 3, 2024) ("In January 2017, the Department of Homeland Security officially designated election infrastructure as a subset of the government facilities sector, making clear that election infrastructure qualifies as critical infrastructure.").

21. Swire & Sacks, *supra* note 8.

22. *See* JAMES A. LEWIS, CTR. FOR STRATEGIC & INT'L STUD., SOVEREIGNTY AND THE EVOLUTION OF INTERNET IDEOLOGY 2 (2020), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201030_Lewis_Sovereignty_Evolution_Internet_Ideology_1.pdf [https://perma.cc/RMJ7-DESX].

23. Swire & Sacks, *supra* note 8 (arguing that the U.S. technology sector will be targeted globally by protectionist localization and "localization weakens cooperation with allies by making it more difficult to effectively share data for law enforcement, intelligence, cybersecurity, health research, and other common purposes").

24. *See, e.g.*, A. Michael Spence & Fred Hu, *Preventing the Balkanization of the Internet*, COUNCIL ON FOREIGN RELS. (Mar. 28, 2018, 12:00 PM), https://www.cfr.org/blog/preventing-balkanization-internet [https://perma.cc/N2GW-Y5Y5]; *Balkanization of the Internet*, BUS. EXECS. FOR NAT'L SEC., https://bens.org/balkanization-of-internet-pt1/ [https://perma.cc/S9DT-MHLD] (last visited Mar. 3, 2024) ("Countries with authoritarian governments are already creating environments where censorship is easier achieved and occurs with far greater frequency. Already a complex network of national laws and regulations, and centrally administered firewalls is facilitating the removal, by some governments, of access to disruptive material, silencing of dissidents, and crushing of free expression online. This is likely only to intensify as the internet balkanizes even more.").

The ability to avoid protectionist localization and splinternet impulses and move toward sustainable data privacy and information security solutions is complex and requires a combination of legal and technological responses. One potential prescription can be found in the recent research of the founder of the World Wide Web, Sir Tim Berners-Lee.[25] Generated from an academic research project at the Massachusetts Institute for Technology, Sir Berners-Lee launched a cybersecurity and data privacy startup, Inrupt, that promotes a Web decentralization project.[26] The project offers a platform for linked-data applications that is not connected to the Web to allow for more user-centric control.[27] Through a product referred to as Solid (social linked data), Inrupt offers open-sourced data infrastructure software that protects personal data and increases cybersecurity.[28] Sir Berners-Lee described Solid as a democracy-protecting innovation, as it aims to make the Web more democratic by "separat[ing] the Web's apps from its data" and "[t]o give information and power back to users."[29] In doing so, Inrupt seeks to decentralize Big Tech "and make the Web more open, more private, . . . more useful and more secure."[30]

This Essay relies on a case study, referred to as the Flemish Decree of 2022, to anchor a discussion on how data infrastructure or data privacy infrastructure may hold the potential to both safeguard data privacy on an individual level and reinforce cybersecurity and national security on a federal level.[31] Conceptualizing data privacy infrastructure requires first understanding a new technology, Solid Privacy Pods, and how the innovation works to achieve its purported goals. Second, federalizing privacy infrastructure is illustrated by the decision by the Government of Belgium's Flemish Region ("Flanders") to implement Solid Privacy Pods—also known as "data vaults"—on a national scale under a data privacy governance mandate.

The Flanders Government is now in the process of implementing a Solid-based data infrastructure that will provide each of its 6.5 million Flemish citizens with access to their own Solid Privacy Pod in which to store their data.[32] These citizen Solid Privacy Pods—or "data vaults," as referred to by the Flanders Government—are designed to serve as hubs for a data

25. *See infra* Part I.

26. *See infra* Part I.

27. *See* Stephen Shankland, *Tim Berners-Lee Startup Launches Privacy-Focused Service to Secure Your Data*, CNET (Nov. 9, 2020, 7:22 AM), https://www.cnet.com/news/privacy/tim-berners-lee-startup-launches-privacy-focused-service-to-secure-your-data/ [https://perma.cc/B7A6-6RUH]; Harry McCracken, *Tim Berners-Lee Is Building the Web's 'Third Layer.' Don't Call It Web3*, FAST CO. (Nov. 8, 2022), https://www.fastcompany.com/90807852/tim-berners-lee-inrupt-solid-pods [https://perma.cc/SZQ3-E8L8].

28. *See* McCracken, *supra* note 27.

29. James Shackell, *Rage Against the Machine: How the Inventor of the Web Is Trying to Save It*, ROLLING STONE AUSTL. (Sept. 16, 2022), https://au.rollingstone.com/culture/culture-features/web-rage-against-machine-42845 [https://perma.cc/Z6NV-C5KE].

30. *Id.*

31. *See infra* Part II.

32. *See infra* Part II.

ecosystem to provide citizens with the ability to see, understand, and control how their information is being used and shared.[33]

To better understand why federalizing data privacy infrastructure may potentially provide a strategic national security advantage to nations that can execute it effectively, one must understand how technological innovation interacts with legal innovation. Those nations who capitalize on utilizing both technological and legal innovation will likely have a strategic advantage in the AI age.

This Essay proceeds in three parts. In Part I, the Essay will discuss why, in the AI age and with the advent of generative AI in particular, data privacy must be understood as a national security priority. In Part II, the Essay examines how the Flemish Decree, by federalizing the implementation of the Solid Privacy Pods, creates a space to discuss the way in which a data privacy infrastructure can unfold on a national scale. Finally, Part III offers a comparative national security perspective on data privacy infrastructure. There is currently an active debate on the efficacy and purpose behind the EU's General Data Protection Regulation (GDPR) and EU's AI Act, on the one hand, and data privacy and generative AI regulatory regimes adopted in China and other countries, on the other hand. Part of this debate centers on whether newly introduced regulatory frameworks enhance security defense strategies as a result of greater oversight over the deployment and use of AI and emerging technologies.

This Essay concludes that the 2024 White House Executive Order on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" signals an understanding that data privacy is a core national security priority as the negotiation of geopolitical power focuses on AI dominance. Federalizing data privacy and information security protection through ex ante design offers one policy option for the future of AI oversight.[34]

I. DATA PRIVACY AS A NATIONAL SECURITY PRIORITY IN THE AGE OF AI

Generative AI increases the urgency for a national conversation on why data privacy, data protection, and cybersecurity must be understood as central to U.S. national security strategy. Part I.A contends that, in recognition of this, policymakers are increasingly structuring AI governance frameworks in ways that centralize the importance of data protection and cybersecurity goals. Part I.B argues that, due to the increasing importance of data privacy to national security, privacy infrastructure can operate on a similar footing as other sectors of critical infrastructure.

33. *See infra* Part II.
34. *See infra* Part III.

A. AI Governance and National Security

There is growing literature that demonstrates the collateral benefits of securing data privacy and increasing privacy regulation.[35] There is also growing evidence that policymakers increasingly view data privacy as necessary for promoting both cybersecurity and national security.[36] The weaponization of social media platforms in information warfare, in particular, has necessitated new regulatory responses.[37] According to Pew Research Center, around 72 percent of the public in 2021 used some type of social media platform.[38] The most widely used online platforms in 2021 were Facebook and YouTube, with Twitter, Pinterest, Instagram, and LinkedIn closely behind.[39] Roughly 70 percent of people who use Facebook reference it at least once a day.[40] Moreover, in January of 2021, the study found that eight out of ten Americans receive their news from a digital platform.[41] And within that population, 53 percent often or sometimes receive their news from social media.[42]

35. *See, e.g.*, Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1011 (2013) (arguing that increasing privacy protections is related to reducing monopolistic power and addressing antitrust concerns); Ignacio N. Cofone, *Algorithmic Discrimination Is an Information Problem*, 70 HASTINGS L.J. 1389, 1394 (2019); Yafit Lev-Aretz & Katherine J. Strandburg, *Privacy Regulation and Innovation Policy*, 22 YALE J.L. & TECH. 256, 264 (2020) (contending that increasing privacy regulation is critical in supporting innovation policy and addressing supply-side information market failures).

36. *See, e.g.*, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Exec. Order No. 14,110, 88 Fed. Reg. 75191 (Oct. 30, 2023).

37. *Cf., e.g.*, Russell L. Weaver, *Social Media Platforms and Democratic Discourse*, 23 LEWIS & CLARK L. REV. 1385, 1415 (2020) (explaining that "[t]he internet is the first truly democratic means of mass communication because it is readily accessible by most people through devices" and that social media companies hold a unique position in history as informational gatekeepers).

38. *See* Brooke Auxier & Monica Anderson, *Social Media Use in 2021*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021 [https://perma.cc/4Z3D-HLL4].

39. *See Social Media Fact Sheet*, PEW RSCH. CTR. (Jan. 31, 2024), https://www.pewresearch.org/internet/fact-sheet/social-media [https://perma.cc/3R64-LWG5].

40. *See* Auxier & Anderson, *supra* note 38 ("Seven-in-ten Facebook users say they use the site daily . . . .").

41. *See* Elisa Shearer, *More than Eight-in-Ten Americans Get News from Digital Devices*, PEW RSCH. CTR. (Jan. 12, 2021), https://www.pewresearch.org/fact-tank/2021/01/12/more-than-eight-in-ten-americans-get-news-from-digital-devices [https://perma.cc/PUD2-E3XD].

42. *Id.*

Foreign interference in the 2016 U.S. elections,[43] combined with the Cambridge Analytica-Facebook scandal,[44] ushered in new awareness on how social media platforms and digital data were being commandeered to influence elections.[45] Congress has attempted to address the threats of foreign interference and foreign influence campaigns.[46] Some legislative efforts have specifically focused on AI and cybersecurity protections. For instance, the AI for National Security Act of 2022[47] proposed that, in the procurement of cyber products and services, the U.S. Department of Defense could prevent cyberattacks by deploying AI-based security to reduce internet connectivity requirements.[48]

Similarly, the 2023 White House Executive Order on "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" prioritizes both data privacy and cybersecurity.[49] Issued in October 2023, the order explained that AI systems must be safe and secure, and it addressed the need to acknowledge AI systems' national security risks in cybersecurity and critical infrastructure:

> Artificial Intelligence must be safe and secure. Meeting this goal requires robust, reliable, repeatable, and standardized evaluations of AI systems, as well as policies, institutions, and, as appropriate, other mechanisms to test, understand, and mitigate risks from these systems before they are put to use. It also requires addressing AI systems' most pressing security risks—including with respect to biotechnology, cybersecurity, critical infrastructure, and other national security dangers—while navigating AI's opacity and complexity.[50]

The order further directed the National Institute of Standards and Technology to establish standards for red-team testing (i.e., a "structured testing effort to

---

43. *See, e.g.*, *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security*, HOMELAND SEC. (Oct. 7, 2016), https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national [https://perma.cc/Y228-CFNJ]; *Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity*, HOMELAND SEC. (Dec. 29, 2016), https://www.dhs.gov/news/2016/12/29/joint-dhs-odni-fbi-statement-russian-malicious-cyber-activity [https://perma.cc/4L5R-S9KY]; OFF. OF THE DIR. OF NAT'L INTEL., INTELLIGENCE COMMUNITY ASSESSMENT: ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf [https://perma.cc/N59B-SDRC].

44. *See generally* Margaret Hu, *Cambridge Analytica's Black Box*, BIG DATA & SOC'Y, July–Dec. 2020, at 1*; see also* INFO. COMM'RS OFF., DEMOCRACY DISRUPTED?: PERSONAL INFORMATION AND POLITICAL INFLUENCE (2018), https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf [https://perma.cc/KJ8P-QXW5]; Young Mie Kim, Jordan Hsu, David Neiman, Colin Kou, Levi Bankston, Soo Yun Kim, Richard Heinrich, Robyn Baragwanath & Garvesh Raskutti, *The Stealth Media?: Groups and Targets Behind Divisive Issue Campaigns on Facebook*, 35 POL. COMMC'N 515 (2018).

45. *See* MARCELLINO ET AL., *supra* note 9, at 1.

46. *See, e.g.*, *supra* note 1 and accompanying text.

47. AI for National Security Act, H.R. 7811, 117th Cong. (2022).

48. *See id.* § 2.

49. Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Exec. Order No. 14,110, 88 Fed. Reg. 75191, 75191 (Oct. 30, 2023).

50. *Id.*

find flaws and vulnerabilities in an Al system") of AI technologies to ensure safety before public release.[51] The order also directed the U.S. Department of Homeland Security to apply those standards to critical infrastructure sectors to assess AI systems' threats to critical infrastructure and cybersecurity risks, among others.[52]

The U.S. Government Accountability Office also addressed AI's risks and the need to take action, stating that AI "is expected to transform all sectors of society, including, according to Department of Defense (DOD), the very character of war. Failure to adopt and effectively integrate AI technology could hinder national security."[53]

B. Data Privacy Infrastructure as a National Security Priority

Over the past five years, there has been a significant global expansion of legislation aimed at protecting users' privacy rights.[54] The legislative developments, however, have not been accompanied by a structural framework by which personal data can be controlled and shared. This technological structure has been increasingly referred to as data privacy infrastructure.[55]

The lack of national privacy-supporting infrastructure for data may impede meaningful progress with respect to the fundamental privacy and security of

---

51. *Id.* at 75194.

52. *Id.* at 75196.

53. *How Artificial Intelligence Is Transforming National Security*, U.S. GOV'T ACCOUNTABILITY OFF.: WATCHBLOG: FOLLOWING FED. DOLLAR (Apr. 19, 2022), https://www.gao.gov/blog/how-artificial-intelligence-transforming-national-security [https://perma.cc/G4ZK-FV2C].

54. Examples include the EU's GDPR, adopted in 2016 and effective in 2018, *see* Regulation 2016/679, General Data Protection Regulation art. 7, 2016 O.J. (L 119) 1 (EU); Brazil's General Personal Data Protection Law, *see* Lei No. 13.709, de 14 de Agosto de 2018, Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.); The California Consumer Privacy Rights Act of 2018, which itself stands alongside an increasing number of other state privacy laws, *see* CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2024); Canada's Consumer Privacy Protection Act, *see* Bill C-11, Digital Charter Implementation Act, 2d Sess., 43rd Parl., 2020 (Can.); and South Korea's Personal Information Protection Act, *see* Gaein jungbo boho beob [Personal Information Protection Act] art. 4(3) (S. Kor.). *See also* Joshua P. Meltzer, *Toward International Cooperation on AI Governance—the US Executive Order on AI*, BROOKINGS (Nov. 1, 2023), https://www.brookings.edu/articles/international-cooperation-the-us-executive-order-on-ai [https://perma.cc/V5WM-NVGJ] (noting that the EU, "Brazil, the U.K., Canada, and Japan are all developing their own approaches to AI governance").

55. Data privacy infrastructure has been used as a term in the industry to describe technological solutions and products that enhance data privacy through technical frameworks. *See generally* Transcend Team, *Introducing Privacy_Infra(), a New Virtual Meetup*, TRANSCEND (July 30, 2020), https://transcend.io/blog/introducing-privacy-infra [https://perma.cc/Y5UT-82MZ] ("Our approach at Transcend has always been to solve the biggest data privacy challenges with engineering-first solutions, and an engineering-led approach. Along those lines, we wanted to create something just for engineers working on privacy infrastructure projects."). *See also* Stijn Viaene, *A Flemish Data Utility Company: Flanders Understands*, VLERICK BUS. SCH. (Jan. 12, 2022), https://www.vlerick.com/en/insights/how-setting-up-a-flemish-data-utility-company-could-herald-the-start-of-a-magnificent-flemish-digital-success-story/ [https://perma.cc/9YFX-2G6B].

users' data.[56] These structural limitations have effectively prevented users from being able to understand and control their personal information and have thus engendered significant and widespread privacy and security vulnerabilities at a national level.[57]

The reality of current data processing is that data portability rights are limited, as companies that are reliant on users' personal information must collect, store, and process their own instances of that data independently.[58] Privacy laws generally operate on top of this closed and individualized infrastructure, placing a set of requirements on individual organizations with respect to how they must treat the data under their control.[59] But these laws operate in a context in which users cannot see their data. In many cases, users do not recall or were never made aware of who is in possession of their data, and they are all but required to share their data independently with a vast range of organizations.[60] This essentially precludes users from

56. *See, e.g.*, BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 2–9, 50–61 (2015); Wirtz et al., *supra* note 15, at 818 (contending that "many challenges and risks are associated with implementing AI in public administration" and "vary from issues of data privacy and security, to workforce replacement and ethical problems like the agency and fairness of AI"); *see also* Makenzie Holland, *Lack of Federal Data Privacy Law Seen Hurting IT Security*, TECHTARGET (Oct. 27, 2023), https://www.techtarget.com/searchcio/news/366557453/Lack-of-federal-data-privacy-law-seen-hurting-IT-security [https://perma.cc/2NFB-E99W].

57. *See* Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/articles/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ [https://perma.cc/5TSV-HL9Z]; Brian Dabbs, *AI Threats Are Here. Are Biden and the Energy Industry Ready?*, E&E NEWS (Oct. 30, 2023, 6:50 AM), https://www.eenews.net/articles/ai-threats-are-here-are-biden-and-the-energy-industry-ready/ [https://perma.cc/3F7X-QWXF] ("Privacy experts say authorities available to a president are limited, arguing that new legislation on Capitol Hill is necessary to protect Americans from AI-caused data breaches. The privacy risk in the energy sector comes from potentially faulty AI products that disseminate data, including from Chinese malware projects that use AI, according to experts.").

58. *See* SCHNEIER, *supra* note 56, at 2–9, 50–61; Richard Bird, Aedan Collins, Theresa Ehlen, Jan Niklas di Fabio, Adam Gillert, Christine Lyon, Giles Pratt & Philipp Roos, *New Data Portability Rights: Challenges and Opportunity*, *in* DATA TRENDS 2024, at 20 (Freshfields ed., 2023), https://www.freshfields.us/4ad2bb/globalassets/our-thinking/campaigns/data-top-trends-2024/data-trends-2024.pdf [https://perma.cc/98R8-HXXR] (noting that, as of late 2023, "data portability rights (such as those found in privacy laws) generally do not play a major role in practice due to legal and technical limitations"); Inge Graef & Jens Prüfer, *Governance of Data Sharing: A Law & Economics Proposal*, RSCH. POL'Y, Nov. 2021, at 1,1 ("Many big data are generated while individual users interact with websites, apps, or programs (henceforth: services) of companies, who automatically log users' choices and digital characteristics . . . .").

59. *See* SCHNEIER, *supra* note 56, at 197–206; *see also* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (and Why It Matters)*, N.Y. TIMES: WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/A57L-ZAC7] ("The data collected by the vast majority of products people use every day isn't regulated. Since there are no federal privacy laws regulating many companies, they're pretty much free to do what they want with the data, unless a state has its own data privacy law . . . .").

60. *See, e.g.*, SCHNEIER, *supra* note 56, at 195–97.

understanding and exercising control over where their data lives and how it is used.

To properly conceptualize the problem and the vulnerabilities it engenders, we need to think about what data usage looks like from the perspective of real-world users, who share their data, create new accounts, and engage separately with a broad range of companies and systems on a daily basis.[61] A user might purchase groceries online in the morning and provide their name, address, contact information, and a full shopping list to that grocery store, while sharing their payment information with a different online payment service and another loyalty points company. That afternoon, they may separately share another set of data with a different company to buy shoes or to order food from a restaurant. Whether signing up for a streaming service, applying for a credit card, purchasing clothing, reserving accommodations, paying bills, or engaging in a vast range of other common transactions, a user's personal data is shared without any consistent or overarching data structure through which that user can see, control, or understand their data usage. As this cycle continues throughout the weeks, months, and years of a consumer's activities, the result is a growing accumulation of largely untethered personal data out in the world.[62]

Thus, to achieve privacy and security at a national scale, the Flemish Decree adopts a broader and more systematic effort: a federalized data privacy infrastructure that operationalizes the ability of users to see the data they share with different organizations and exert control over how that data gets used. This infrastructure allows individuals and organizations to use data without requiring them to separately obtain and handle their own version of each user's data. The key to this solution lies in a centralized technological infrastructure that is designed and engineered to give users visibility and control over their data across different organizations and that extends that visibility and control throughout the lifecycle of any given piece of data.

For example, Solid is a Web standards–based specification protocol that lets people use a personal data store (a "Privacy Pod" or "data vault") to make choices with respect to whether, when, how, and with whom their data is shared.[63] Instead of users needing to independently share their data with every company that wants or needs a copy of it, the Solid Privacy Pod model lets users store their data in their own pod and then control how that data gets shared.[64] A user's pod can thus serve as a control center for personal data, allowing the pod-holder to see the organizations they are sharing data with

61. *See* Jack Flynn, *40 Fascinating Mobile App Industry Statistics [2023]: The Success of Mobile Apps in the U.S.*, ZIPPIA: CAREER EXPERT (Mar. 20, 2023), https://www.zippia.com/advice/mobile-app-industry-statistics/ [https://perma.cc/SW8T-ZATR] (noting that "[t]he average smartphone owner uses 9-10 apps per day").

62. *See* SCHNEIER, *supra* note 56, at 195–97; *see also* Graef & Prüfer, *supra* note 58, at 1.

63. *See* KNOWLEDGE CENTRE DATA & SOC'Y, WHAT ARE DATA VAULTS, AND WHAT CAN THEY MEAN TO YOU? (2023), https://data-en-maatschappij.ai/uploads/brAInfood_solid_ENG_2023-11-15-075539_gnhx.pdf [https://perma.cc/BE5L-UEVT]; *Solid: Vault Technology for Consumers and Businesses*, ATHUMI, https://athumi.be/en/technologies/solid [https://perma.cc/PHY3-WW3X] (last visited Mar. 3, 2024).

64. *See supra* note 63.

and the particular data elements that they are sharing and then make ongoing choices about that data.[65]

Building on Solid, Sir Berners-Lee's new development effort Inrupt has created an enterprise-grade Solid server (ESS) to deploy Pod services, which a range of companies and governments already use.[66] An ESS Pod allows its owner to see and change a consent grant at any time; if the owner makes any consent-related changes, the relevant organizations are sent notifications informing them that they no longer have consent to process the data for the initially consented-to purpose.[67] Through their Pods, users can see "[w]ho accessed their data"; "[w]hat data was accessed"; "[w]hen the data was accessed"; "[w]hether the data was read or written"; "[w]hat, if any, changes were made to the data"; "[w]hat application was used to access the data"; and "[w]hether the data was accessed via consent."[68] Moreover, if consent was provided, users can review when that consent was granted and for what specific purpose.[69]

Infrastructure like ESS pods are more important than ever given the exponential and alarming growth of personally identifiable information on U.S. citizens that can be trafficked online.[70] A declassified intelligence report described the purchase of online personal data as an "increasingly powerful" tool that has been deployed by foreign adversaries.[71] Indeed, China, Russia, and other foreign adversaries are amplifying intelligence capacities by simply resorting to webscraping, data breaches, or purchasing data of U.S. citizens and the citizens of other nations.[72]

II. THE FLEMISH DECREE AND FEDERALIZING DATA PRIVACY

Under the Flemish Decree, the Flanders Government is assembling a federal "data utility" company, Athumi, which is an autonomous organization owned and operated by the government.[73] Part II.A explores how the implementation of the Flanders experiment by Athumi—which was tasked with the oversight of the Solid infrastructure and "data vaults," or

65. *See supra* note 63.

66. *See Enterprise Solid Server*, INRUPT, https://www.inrupt.com/products/enterprise-solid-server [https://perma.cc/PC7Z-BSK9] (last visited Mar. 3, 2024).

67. *See* Eliott Behar, *The Graveyard of Past Consents: Rethinking the Consent Problem and Building for Better Privacy*, INRUPT (Sept. 9, 2022), https://www.inrupt.com/blog/the-graveyard-of-past-consents [https://perma.cc/D349-RBMZ].

68. *Id.*

69. *See id.*

70. *See* Sean Lyngaas, *US Intelligence Agencies Buy Americans' Personal Data, New Report Says*, CNN (June 12, 2023, 6:35 PM), https://www.cnn.com/2023/06/12/politics/intel-agencies-personal-data/index.html [https://perma.cc/F4YP-HCF7].

71. *Id.*

72. Sean Lyngaas, *Biden Administration Planning Action to Stop Hostile Foreign Governments Exploiting Americans' Personal Data*, CNN (Jan. 24, 2024, 2:09 PM), https://www.cnn.com/2024/01/23/politics/biden-administration-foreign-governments-exploiting-personal-data/index.html [https://perma.cc/M62J-E35K].

73. *Flemish Government Launches Data Company Athumi*, BELGA NEWS AGENCY (May 5, 2023), https://www.belganewsagency.eu/flemish-government-launches-data-company-athumi [https://perma.cc/4J7H-JMXV].

Privacy Pods—is a form of federalizing data privacy infrastructure. Part II.B describes how this move signals that, like the management of electricity, water, and other critical infrastructure, data ecosystem management—including privacy and security of data—is a federalized priority.

Athumi has already started the process of developing various data vault partnerships.[74] Theoretically, the data vaults facilitate individualized user control over one's own personal data.[75] Also theoretically, Athumi will enable safe, private, and secure data exchanges between government, businesses, and citizens.[76] As an added layer of data privacy protection for the citizenry, Athumi "will not interact directly with citizens. The existing identity authentication app itsme will use the technology and provide data vaults."[77]

A. The Flanders Experiment in Federalizing Data Privacy Infrastructure

The Flanders Government implemented a privacy-centric data infrastructure, utilizing the Solid protocol to provide each of Flanders' 6.5 million citizens with access to their own "data vaults."[78] These are designed to act as hubs through which individuals can store, see, and exert control over their personal data.[79] They operate as part of an ecosystem that is intended to enable data to flow securely within the government, as well as between the government and the private sector.[80]

This initiative grew from the Flanders Government's desire to fuel data-based innovation and enhance citizen interactions with the Government and across the private sector, while at the same time building trust in its citizens with respect to how their personal data is used. For instance, Flemish Prime Minister Jan Jambon stated that "[l]etting data flow is the key to giving our society and our economy a huge boost in the 2020s. But that requires trust."[81]

To implement this new data architecture, the Flanders Government completed a comprehensive, multilevel review of the privacy and security compliance of this proposal, and the Flemish Parliament issued a decree to enshrine this new data infrastructure in law ("the Decree").[82] In doing so,

74. *See Athumi Supplies Flemish Data Vault Technology in the Netherlands*, ATHUMI (Jan. 23, 2024), https://athumi.eu/blog/nieuws/athumi-levert-vlaamse-datakluistechnologie-in-nederland [https://perma.cc/6A5E-7A6X].

75. *Flemish Government Launches Data Company Athumi*, *supra* note 73.

76. *See id.*

77. *Id.*

78. *Id.*; KNOWLEDGE CENTRE DATA & SOC'Y, *supra* note 63.

79. *Flemish Government Launches Data Company Athumi*, *supra* note 73.

80. *See id.*

81. *The Flemish Data Utility Company*, AGENTSCHAP DIGITAAL VLAANDEREN, https://www.vlaanderen.be/digitaal-vlaanderen/athumi-het-vlaams-datanutsbedrijf/the-flemish-data-utility-company [https://perma.cc/L7DX-M6HF] (last visited Mar. 3, 2024).

82. Decreet van 2 december 2022 houdende machtiging tot oprichting van het privaatrechtelijk vormgegeven extern verzelfstandigd agentschap Vlaams Datanutsbedrijf in de vorm van een naamloze vennootschap [Decree Authorizing the Establishment of the Private

the Flanders Government has provided a novel case study to assess how a technology like Solid can use federal data infrastructure to empower its citizens and protect their data—and thereby move toward meaningfully better privacy and security outcomes in the long term.

The Decree empowered the Government to create an autonomous public company, Athumi, that is responsible for the data processing under this Solid infrastructure.[83] The Decree specifies that the objective of this utility company is to facilitate secure data-sharing for citizens and to optimize the exercise of citizens' data rights "with a minimum of administrative burdens."[84]

Athumi describes its mission as both (1) serving businesses by making data more usable and (2) serving consumers by "guaranteeing more control over personal data, [thus] enabling them to participate safely in innovative services."[85] It describes its mission in the following ways: facilitating "insights from more data, which will create social and economic progress"; increasing "better data to flow, which will lead to new services"; supporting "transparent data ecosystems that businesses and citizens justifiably trust"; and establishing "a unified European data space."[86]

Much of the privacy-focused content in the Decree places requirements on Athumi that are already required by the GDPR as part of its basic legal governance architecture.[87] In these respects, the Decree does not add anything substantive or new; it is essentially compelling Athumi to do what it was already required to do—to act in accordance with the structure that accompanies the GDPR. For example, the Decree's consent requirements reiterate the GDPR consent requirements that are also inherent to the basic structure of Inrupt ESS Pods:

> Consent from a citizen [must] always [be] expressly granted, whereby the citizen is informed in advance about the processing of personal data to which the consent relates. That consent may be withdrawn in accordance with Article 7(3) of the General Data Protection Regulation. A citizen's consent [must be] requested for any processing of personal data to which the consent relates.[88]

Similarly, Article 27 of the Decree addresses data retention and again essentially reiterates what is already required by the GDPR—that the data processed must not be kept longer than necessary to achieve its purposes or

---

Law External Independent Agency Vlaams Datanutsbedrijf in the Form of a Public Limited Company], M.B., Dec. 14, 2022, https://www.ejustice.just.fgov.be/cgi/api2.pl?lg=nl&pd=2022-12-14&numac=2022034593 [https://perma.cc/Q83W-9ZFB] [hereinafter Flemish Decree].

83. *See id.* art. 4, § 1; *Flemish Government Launches Data Company Athumi*, *supra* note 73.

84. Flemish Decree, *supra* note 82, art. 4.

85. *Mission*, ATHUMI, https://athumi.be/en/about-us/mission [https://perma.cc/77WR-KBE2] (last visited Mar. 3, 2024).

86. *Id.*

87. *See Privacy Policy*, ATHUMI, https://athumi.be/en/privacy-policy [https://perma.cc/YDP6-GPJF] (last visited Mar. 3, 2024).

88. Flemish Decree, *supra* note 82, art. 29; *see also* Regulation 2016/679, *supra* note 54.

must be deleted on request by the user.[89] Although these types of privacy requirements do not require any additional legislation, it may be that the Decree is reiterating them and enshrining them in law to provide additional clarity and to reassure both citizens and other governmental entities that this new system will continue to uphold the GDPR's data rights and requirements.

The Decree also includes certain restrictions on the uses to which data can be put, including, most notably, an outright restriction on the ability of Athumi to conduct automated decision-making and profiling: "the Flanders Data Utility Company does not carry out any automated decision-making, including profiling, on the personal data that is processed."[90]

In theory, the motivation for adoption on a national scale is to represent a safer environment in which to conduct AI and machine learning—or to conduct profiling—than more conventional ways of storing data.[91] Also theoretically, the data vaults can provide the ability for users to see, understand, and make choices about how their data is being used for AI and machine learning, as well as to understand whether and how they are being profiled.[92] The Flemish Parliament's intention in adopting the technology specified in the Decree was to facilitate an intuitive way to show and explain data processes, including greater visibility into what specific inputs automated systems may rely on and what outputs they generate.[93]

Although automated decision-making and profiling are often associated with for-profit business models—and can presumably still be utilized by third-party companies in this ecosystem—these forms of processing have other uses, including for a range of safety and security purposes.[94] As such, these processes could have utility for Athumi going forward. For a first implementation, in which citizens, government agencies, and private organizations will have their initial touchpoints with this technology and the interface, measured steps and building trust incrementally may be necessary

89. *See* Flemish Decree, *supra* note 82, art. 27; Regulation 2016/679, *supra* note 54, art. 5(1)(e) ("Personal data shall be . . . kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes . . . .").

90. Flemish Decree, *supra* note 82, art. 28.

91. *See* Alex Scroxton, *Taking Back Control: Could a Distributed Model Breed a Better AI?*, COMPUTERWEEKLY.COM (Mar. 7, 2023, 12:30 PM), https://www.computerweekly.com/news/365531892/Taking-back-control-Could-a-distributed-model-breed-a-better-AI [https://perma.cc/49XM-GSCD].

92. *See supra* Part I.

93. *See supra* Part I.

94. *See* Maciej Kuziemski & Gianluca Misuraca, *AI Governance in the Public Sector: Three Tales from the Frontiers of Automated Decision-Making in Democratic Settings*, TELECOMM. POL'Y, Apr. 2020, at 1, 10 (arguing that the danger of digital infrastructures and data-driven decision-making systems is, in part, "the temptation of . . . imposing restrictions on individual rights, such as privacy . . . [and trusting] supposedly benevolent AI-enabled applications and predictive modelling systems"); Ulrik B.U. Roehl, *Automated Decision-Making and Good Administration: Views from Inside the Government Machinery*, GOV'T INFO. Q., Aug. 2023, at 2.

in the implementation; this could include efforts related to transparency, robust testing, and methods of accountability.[95]

B. Integrating Data Privacy Infrastructure into AI Governance

Professor Woodrow Hartzog and other scholars have championed the need to consider "Privacy by Design."[96] To pave the way for the national adoption of the Solid Privacy Pod as a new data architecture—or a new data privacy infrastructure—the Flanders Government's experiment enshrined a new data ecosystem in law.[97] In doing so, Flanders has provided an interesting early case study to assess how Solid may potentially enable next-level data architecture and the federalization of data privacy infrastructure as a form of AI governance. The goals of the Decree are to provide intuitive visibility, control, and interoperability for governmental data, while also providing robust privacy protections that comply with the GDPR.[98]

The Decree, and the accompanying review of this new data infrastructure, requires an examination of exactly how the Flemish Government will implement the Solid Privacy Pod model from a legal and structural perspective. Specifically, the Government will have to consider what controls and limitations it should place on data processing and what steps, if any, to take to satisfy itself that this new system would ensure the fundamental privacy protections provided by the GDPR.[99]

The Decree's enabling process has already subjected the proposed Solid model to a review of its privacy and security compliance—including its specific compliance with the GDPR—and this deployment has now been approved for widespread civilian use.[100] By codifying the requirements for this Solid infrastructure, the Decree has taken steps to provide certainty and reassurance to its citizens, and to the government itself, in key areas.[101]

---

95. Kuziemski & Misuraca, *supra* note 94, at 10–11; *see also* WHITE HOUSE OFF. SCI. & TECH. POL'Y, BLUEPRINT FOR AN AI BILL OF RIGHTS: MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE (2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf [https://perma.cc/J6KB-VLD6]; NAT'L INST. OF STANDARDS & TECH., ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (AI RMF 1.0) (2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf [https://perma.cc/A8KD-QCBX].

96. *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 12 (2018).

97. *See supra* Part II.A.

98. *See supra* Part II.A.

99. *See supra* Part II.A.

100. *See* Chris Middleton, *Could Sir Tim Berners-Lee One Day Unite Europe on a Shared Data Platform?*, DIGINOMICA (Sept. 5, 2022), https://diginomica.com/could-sir-tim-berners-lee-one-day-unite-europe-shared-data-platform [https://perma.cc/TC79-TJEA].

101. *See* Christy Kuesel, *Digital Flanders Reconnects Citizens with Their Data Through Inrupt's Solid Server*, INRUPT (Sept. 15, 2022), https://www.inrupt.com/blog/digital-flanders-reconnects-citizens-with-their-data-through-inrupts-solid-server [https://perma.cc/5NNB-AP58].

III. FEDERALIZING PRIVACY INFRASTRUCTURE AS A NATIONAL SECURITY DEFENSE STRATEGY

Part III offers a comparative national security perspective on privacy infrastructure. Part III.A discusses why newly introduced privacy regulatory frameworks may enhance security defense strategies of some nations over others as a result of greater oversight over the deployment and use of AI and other emerging technologies. Part III.B contends that the EU's AI Act, along with data privacy and generative AI regulatory regimes adopted in China and other countries, represents a federalizing of data privacy and data protection through ex ante design. Part III.B further contends that these innovations in data privacy will give these nations a comparative advantage in AI governance and national security.

A. Data Privacy and National Security

The Flemish Government's federalization of data vaults as a form of privacy infrastructure was not necessarily motivated by national security.[102] More and more nations, however, are considering the adoption of a federalized data privacy infrastructure[103] as the threat of AI weaponry grows and the deployment of cyberpsychological[104] operations becomes more widespread.[105] In light of this threat, President Joseph R. Biden recently issued an Executive Order on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern."[106]

102. *See, e.g.*, Steve Lohr, *He Created the Web. Now He's Out to Remake the Digital World.*, N.Y. TIMES (Jan. 10, 2021), https://www.nytimes.com/2021/01/10/technology/tim-berners-lee-privacy-internet.html [https://perma.cc/92H6-MUYY].

103. *See, e.g.*, Rory Cellan-Jones, *NHS Data: Can Web Creator Sir Tim Berners-Lee Fix It?*, BBC (Nov. 9, 2020), https://www.bbc.com/news/technology-54871705 [https://perma.cc/GFG9-T2CW]; K.G. Orphanides, *The BBC's Radical New Data Plan Takes Aim at Netflix*, WIRED (Sept. 29, 2021, 6:00 AM), https://www.wired.co.uk/article/bbc-data-personalisation [https://perma.cc/9PBN-WFYT].

104. "Cyberpsychology is the study of psychological processes related to, and underlying, all aspects and features of technologically interconnected human behavior." *What Is Cyberpsychology and Why Is It Important?*, N.J. INST. TECH. (Feb. 7, 2023), https://www.njit.edu/admissions/blog-posts/what-cyberpsychology-and-why-it-important [https://perma.cc/A8TJ-VVPH].

105. *See, e.g.*, Andrea M. Matwyshyn & Miranda Mowbray, *Fake*, 43 CARDOZO L. REV. 643, 663–70 (2021); Eric Lipton, *From Land Mines to Drones, Tech Has Driven Fears About Autonomous Arms*, N.Y. TIMES (Nov. 21, 2023), https://www.nytimes.com/2023/1/21/us/politics/drones-ai-weapons-war.html [https://perma.cc/4U8N-YNWF]; Elias Groll, *US Intelligence Research Agency Examines Cyber Psychology to Outwit Criminal Hackers*, CYBERSCOOP (May 30, 2023), https://cyberscoop.com/iarpa-cyber-psychology-hackers/ [https://perma.cc/A56M-9ZCK].

106. Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, Exec. Order No. 14,117, 89 Fed. Reg. 15421 (Feb. 28, 2024).

Very few users exercise their data rights,[107] and those that do achieve little in return for their efforts.[108] This is not to criticize the creation of these rights, by any means. It is to say, instead, that we need to do better in enabling these rights so that they can be exercised in a simple way that delivers useful results. Our failure to make data truly visible and to place it under ongoing control has real costs, both for the individuals who share their data and for the organizations and governments with whom they share it.[109]

The solution to this problem lies not in new laws and regulations alone, nor in improved platform messaging, nor in user education. The solution requires technology that is actually designed and engineered to give users visibility and control over their data, as well as to extend that visibility and control beyond the moment of consent and throughout the lifecycle of any given piece of data. What we need, in other words, is technology that breathes new life back into our data.

Until organizations adopt privacy-centered frameworks through which users can actually see and control their personal information, it will be difficult to expect those users to feel any sense of control or comfort with respect to their data. The average user's daily activities and the sheer volume of personal information that they share on a regular basis mean that expecting users to remember and track where they have shared their data and the terms under which they have shared it is simply unrealistic.[110] What we need, then, is to build and implement systems that let users see and control their data past the moment of initial consent—and to make this process so easy that it comes as second nature.

---

107. *See* The Editorial Board, Opinion, *America, Your Privacy Settings Are All Wrong*, N.Y. TIMES (Mar. 6, 2021), https://www.nytimes.com/2021/03/06/opinion/data-tech-privacy-opt-in.html [https://perma.cc/7QZQ-YLTL]; Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1071–73 (2019) ("People encounter so many privacy policies in their daily lives that it would be irrational to read each of them—one study calculated that it would take the average person 200 hours per year. There are also all kinds of cognitive phenomena that prevent individuals from obtaining meaningful information from privacy policies in the way that a notice and choice regime assumes they do, such as hyperbolic discounting and optimism bias." (footnote omitted)); Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCI. MAG. 509, 510 (2015) (noting that "people who claim to care about privacy often show little concern about it in their daily behavior").

108. JOSEPH TUROW, YPHTACH LELKES, NORA A. DRAPER & ARI EZRA WALDMAN, ANNENBERG SCH. FOR COMMC'N, UNIV. OF PA., AMERICANS CAN'T CONSENT TO COMPANIES' USE OF THEIR DATA 6 nn.25–28 (2023), https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf [https://perma.cc/3J9T-ZDD6].

109. *See* Ron Arden, *The Role of Enhanced Visibility for Data Privacy and Security*, TECHSPECTIVE (Nov. 7, 2023), https://techspective.net/2023/11/07/the-role-of-enhanced-visibility-for-data-privacy-and-security/ [https://perma.cc/YP7V-JEVQ].

110. *See* Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/HK2H-5CRQ].

Building consent that works in the present and that scales for the future will not only yield benefits for users but also for the companies, nonprofits, and governments that need this data to operate. Through transparency and control, these organizations can build and leverage real user trust.[111]

B. Cyber Defense and Data Privacy Infrastructure

In information warfare, everyone with digital communications is seen as a potential soft target.[112] Relatedly, anyone with digital communications can also be seen as a potential combatant to be recruited or radicalized, especially in non-state conflicts and grey conflict zones, such as cyberwar.[113] If threats are cognitive, as well as exploitative of virtual and physical vulnerabilities, data privacy and data protection take on new meaning in national security and cyber defense.

There is a concern that although the United States achieved dominance in traditional warfare, it is falling behind in the context of national cybersecurity.[114] Before the election interference of 2016, Russia announced that they had developed weaponry that would allow it to speak as geopolitical equals.[115] Experts believe that this has been reflected in a convergence of hacking tools and cyberpropaganda/influence campaigns.[116] Due to

111. Timothy Morey, Theodore Forbath & Allison Schoop, *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV., May 2015, at 96.

112. *See supra* note 10; *see also* Christopher Woody, *Russia's War in Ukraine Shows Why Troops Need to Learn to Put Their Phones Away, Top US Marine General Says*, BUS. INSIDER (Dec. 31, 2022, 12:42 PM), https://www.businessinsider.com/russia-ukraine-war-shows-battlefield-phone-risk-top-marine-says-2022-12 [https://perma.cc/G6VG-YFN2].

113. Lukasz Olejnik, *Smartphones Blur the Line Between Civilian and Combatant*, WIRED (June 6, 2022, 9:00 AM), https://www.wired.com/story/smartphones-ukraine-civilian-combatant/ [https://perma.cc/6W3R-7ZT6].

114. *See* Jack Corrigan, *Social Media Is 'First Tool' of 21st-Century Warfare, Lawmaker Says*, NEXTGOV FCW (Sept. 28, 2017), https://www.nextgov.com/digital-government/2017/09/social-media-first-tool-21st-century-warfare-lawmaker-says/141379/ [https://perma.cc/2WHH-9TN5] (noting that Senator Mark Warner said that "[w]e may have in America the best 20th-century military that money can buy, but we're increasingly in a world where cyber vulnerability, misinformation and disinformation may be the tools of conflict"); *see also* Sarah Rajtmajer & Daniel Susser, Automated Influence and the Challenge of Cognitive Security 1 n.3 (Sept. 21, 2020) (unpublished manuscript), https://dl.acm.org/doi/10.1145/3384217.3385615 [https://perma.cc/LN5K-DVU4]. Russia's interference in the 2016 U.S. presidential election led experts to question how and why data breaches, new techniques of information warfare, and the commandeering of social media platforms might impinge on national sovereignty, violate the laws of war as a form of cyberattack, or be unlawful under other aspects of international law. *See, e.g.*, JENS DAVID OHLIN, ELECTION INTERFERENCE: INTERNATIONAL LAW AND THE FUTURE OF DEMOCRACY 2–9 (2020). Jens David Ohlin has argued that this new form of post–Cold War conflict is a violation of the right to self-determination by a citizenry. *See id.* at 3 n.4 (citing Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579 (2017)).

115. *See* David Ignatius, Opinion, *Russia's Radical New Strategy for Information Warfare*, WASH. POST (Jan. 18, 2017, 6:02 PM), https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/ [https://perma.cc/BHC5-C5VM].

116. *See, e.g.*, SCOTT JASPER, RUSSIAN CYBER OPERATIONS: CODING THE BOUNDARIES OF CONFLICT 3, 49–52, 71–75 (2020); P.W. SINGER & EMERSON T. BROOKING, LIKEWAR: THE WEAPONIZATION OF SOCIAL MEDIA 148–217 (2018); *see also* 1 ROBERT S. MUELLER III, U.S.

asymmetric military dominance since the Cold War and an unprecedented investment in the military since the close of World War II, many believe that Russia and others will not easily compete with the United States as equals in traditional warfare.[117] Experts are concerned, however, that foreign adversaries can outpace the United States in breaches and disinformation/misinformation campaigns.[118]

The evolution of national security is always affected by technological progress; technological advances can allow for tactical shifts in how nations organize around and engage with conflict.[119] Understanding disruptive machine innovations extends beyond engineering and into societal redefinition of military concepts and strategies.

Propaganda saw innovations in cognitive attack tactics and techniques using radio that demanded a radical defense adaptation. For instance, Nazi Minister for Public Enlightenment and Propaganda Joseph Goebbels wrote in his diary that he believed that it would be "easy to carry on the fight" by 1933. He wrote: "Radio and press are at our disposal. We shall stage a masterpiece of propaganda."[120] In 1938, Goebbels gave a celebratory speech, drawing from Napoleon's infamous abuse of the press, in which he declared radio to be the "Eighth Great Power"—a technological advantage that could enable Hitler to end democracy.[121]

DEP'T OF JUST., REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 14–65 (2019), https://www.justice.gov/archives/sco/file/1373816/download [https://perma.cc/U9FR-ZFGH].

117. *See, e.g.*, JASPER, *supra* note 116, at 27–70; MICHAEL G. MCLAUGHLIN & WILLIAM J. HOLSTEIN, BATTLEFIELD CYBER: HOW CHINA AND RUSSIA ARE UNDERMINING OUR DEMOCRACY AND NATIONAL SECURITY v–xiv (2023); Corrigan, *supra* note 114; Massimo Calabresi, *Inside Russia's Social Media War on America*, TIME (May 18, 2017, 3:48 PM), https://time.com/4783932/inside-russia-social-media-war-america/ [https://perma.cc/YEV8-FFK2] ("Marrying a hundred years of expertise in influence operations to the new world of social media, Russia may finally have gained the ability it long sought but never fully achieved in the Cold War: to alter the course of events in the U.S. by manipulating public opinion."). For more information on asymmetric warfare strategies, see generally STEVEN METZ & DOUGLAS V. JOHNSON II, STRATEGIC STUD. INST., ASYMMETRY AND U.S. MILITARY STRATEGY: DEFINITION, BACKGROUND, AND STRATEGIC CONCEPTS (2001), https://apps.dtic.mil/sti/pdfs/ADA387381.pdf [https://perma.cc/F9ZB-JDXT].

118. *See, e.g.*, KATHLEEN HALL JAMIESON, CYBERWAR: HOW RUSSIAN HACKERS AND TROLLS HELPED ELECT A PRESIDENT: WHAT WE DON'T, CAN'T, AND DO KNOW 67–69 (2018); MALCOLM NANCE, THE PLOT TO HACK AMERICA: HOW PUTIN'S CYBERSPIES AND WIKILEAKS TRIED TO STEAL THE 2016 ELECTION 152–53 (2016).

119. *Cf., e.g.*, Erin Blakemore, *How the Advent of Nuclear Weapons Changed the Course of History*, NAT'L GEOGRAPHIC (July 15, 2020), https://www.nationalgeographic.com/history/article/how-advent-nuclear-weapons-changed-history [https://perma.cc/6RV6-WCU4].

120. Maja Adena, Ruben Enikolopov, Maria Petrova, Veronica Santarosa & Ekaterina Zhuravskaya, *Radio and the Rise of the Nazis in Prewar Germany*, 130 Q.J. ECON. 1885, 1886 (2015).

121. JOSEPH GOEBBELS, SIGNALE DER NEUEN ZEIT: 25 AUSGEWÄHLTE REDEN VON DR. JOSEPH GOEBBELS (1938).

Overall, the evidence suggests that platforms can play a role in the fall or preservation of a democracy.[122] In particular, restrictions of extremist speech are an important safeguard of democracy.[123] Without such restrictions, mass media can become a catalyst for the establishment of a dictatorial rule.[124] In the ever-evolving landscape of global security, the advent of the digital era has brought about a paradigm shift in the nature of threats that nations face.[125] The emergence of cognitive threats, coupled with the exploitation of virtual and physical vulnerabilities, has transformed the traditional notions of national security.[126] In an era in which information is power, data privacy and protection have taken on unprecedented significance. This transformation is not merely a technological evolution but a conceptual redefinition of warfare itself.

Any informed conversation on AI and national security requires a comparative perspective on the recent AI developments in the People's Republic of China. Among national security experts, it is understood that China is outpacing the United States in the regulation of AI and is attempting to outpace the United States in AI technological innovation.[127] China has recently proposed a comprehensive set of AI regulations: the 2022 Administrative Provisions on Algorithm Recommendation for Internet Information Services;[128] the Provisions on Management of Deep Synthesis in Internet Information Service;[129] the Provisional Provisions on

122. *See, e.g.*, JAMIESON, *supra* note 118, at 21–27. *See generally* Darren L. Linvill & Patrick L. Warren, *Engaging with Others: How the IRA Coordinated Information Operation Made Friends*, MISINFORMATION REV., Apr. 2020, at 1.

123. *See, e.g.*, Alexandra Olteanu, Carlos Castillo, Jeremy Boy & Kush R. Varshney, The Effect of Extremist Violence on Hateful Speech Online 221 (Apr. 16, 2018) (unpublished manuscript), https://arxiv.org/abs/1804.05704 [https://perma.cc/MTR3-RTFM]; *see also* JEFF KOSSEFF, LIAR IN A CROWDED THEATER 303–06 (2023) (arguing for the need to preserve First Amendment protections when combatting disinformation and misinformation campaigns).

124. *See, e.g.*, Adena et al., *supra* note 120, at 1886.

125. *See, e.g.*, Nakashima et al., *supra* note 9.

126. *See, e.g.*, Rajtmajer & Susser, *supra* note 114, at 1–3 ("Advances in AI are powering increasingly precise and widespread computational propaganda, posing serious threats to national security."); Justin Sherman, *The Open Data Market and Risks to National Security*, LAWFARE (Feb. 3, 2022, 8:01 AM), https://www.lawfaremedia.org/article/open-data-market-and-risks-national-security [https://perma.cc/22D5-LELT].

127. *See, e.g.*, Mohar Chatterjee, *Senate Intelligence Chair: China Leads the World on AI Rules*, POLITICO (June 15, 2023, 12:32 PM), https://www.politico.com/news/2023/06/15/senate-intelligence-chair-china-leads-the-world-on-ai-rules-00102168 [https://perma.cc/5DEQ-2J2E].

128. *See* Rogier Creemers, Graham Webster & Helen Toner, *Translation: Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022*, DIGICHINA (Jan. 10, 2022), https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/ [https://perma.cc/NV4Z-75BJ].

129. *See* Rogier Creemers & Graham Webster, *Translation: Internet Information Service Deep Synthesis Management Provisions (Draft for Comment) – Jan. 2022*, DIGICHINA (Feb. 4, 2022), https://digichina.stanford.edu/work/translation-internet-information-service-deep-synthesis-management-provisions-draft-for-comment-jan-2022 [https://perma.cc/M64Y-L3G2].

Management of Generative Artificial Intelligence Services;[130] and the Trial Measures for Ethical Review of Science and Technology Activities.[131]

The fact that China immediately moved to block ChatGPT after its release[132] and proclaimed AI to be among the greatest threats to its national security[133] is a signal that it envisions modern warfare in a different way than the United States and the EU. China moved immediately to create a legal framework for regulating generative AI,[134] and the country now has its own generative AI system that it controls.[135] Senator Mark Warner, Chairman of the U.S. Senate Select Committee on Intelligence, stated that it is this combination of legal and technical innovation by China and other nations (and China's unitary control over industry, research, deployment and regulation of technology) that may give China a competitive advantage strategically.[136]

Privacy laws like the GDPR provide users with certain fundamental rights in relation to their personal data.[137] For example, they require individual organizations to let users delete, request a copy of, and correct their personal data.[138] Although the existence of these data rights seems meaningful on the

130. *See* Anna Gamvros, Edward Yau & Steven Chong, *China Finalises Its Generative AI Regulation*, NORTON ROSE FULBRIGHT (July 25, 2023), https://www.dataprotectionreport.com/2023/07/china-finalises-its-generative-ai-regulation/ [https://perma.cc/2RYU-3J3Z].

131. *See* Giulia Interesse, *Ethical Review of Science and Technology in China: Draft Trial Measures*, CHINA BRIEFING (May 11, 2023), https://www.china-briefing.com/news/china-ethical-review-of-science-and-technology-draft-trial-measures/ [https://perma.cc/NC22-M6BD]; *see also* LATHAM & WATKINS, CLIENT ALERT COMMENTARY: CHINA'S NEW AI REGULATIONS (2023), https://www.lw.com/admin/upload/SiteAttachments/Chinas-New-AI-Regulations.pdf [https://perma.cc/MPM7-MYFG].

132. *See, e.g.*, Siladitya Ray, *ChatGPT Reportedly Blocked on Chinese Social Media Apps—as Beijing Claims AI Is Used to Spread Propaganda*, FORBES (Feb. 22, 2023, 4:45 AM), https://www.forbes.com/sites/siladityaray/2023/02/22/chatgpt-reportedly-blocked-on-chinese-social-media-apps-as-beijing-claims-ai-is-used-to-spread-propaganda/?sh=50eed661372c [https://perma.cc/XWX7-MG6J].

133. *See China Warns of Artificial Intelligence Risks, Calls for Beefed-Up National Security Measures*, AP (May 31, 2023, 4:26 AM), https://apnews.com/article/china-artificial-intelligence-national-security-00a38e550ef6b4ac12cd1fd418363d2b [https://perma.cc/Z5PT-C42D].

134. *See, e.g.*, Zeyi Yang, *Four Things to Know About China's New AI Rules in 2024*, MIT TECH. REV. (Jan. 17, 2024), https://www.technologyreview.com/2024/01/17/1086704/china-ai-regulation-changes-2024/ [https://perma.cc/HU3S-SVM4]; *China Proposes Blacklist of Training Data for Generative AI Models*, REUTERS (Oct. 12, 2023, 12:46 PM), https://www.reuters.com/technology/china-proposes-blacklist-sources-used-train-generative-ai-models-2023-10-12/ [https://perma.cc/8LMW-EHZV].

135. *See, e.g.*, Evelyn Cheng, *China's AI Chatbots Haven't Yet Reached the Public Like ChatGPT Did*, CNBC (Apr. 28, 2023, 2:37 AM), https://www.cnbc.com/2023/04/28/how-chinas-chatgpt-ai-alternatives-are-doing.html [https://perma.cc/VZ7W-F5SB].

136. *See, e.g.*, Chatterjee, *supra* note 127.

137. *See, e.g.*, *Global Comprehensive Privacy Law Mapping Chart*, IAPP, https://iapp.org/resources/article/global-comprehensive-privacy-law-mapping-chart/ [https://perma.cc/2YHF-9SZP] (Apr. 2022); *see also* Luis Miguel M. del Rosario, Note, *On the Propertization of Data and the Harmonization Imperative*, 90 FORDHAM L. REV. 1699, 1715 (2022).

138. *See* del Rosario, *supra* note 137, at 1715; Matt Burgess, *What Is GDPR?: The Summary Guide to GDPR Compliance in the UK*, WIRED (Mar. 24, 2020, 4:30 PM),

surface, the fact that every user's data is individually siloed across a huge number of separate organizations makes it almost impossible to meaningfully exercise those rights.[139] Deleting or obtaining copies of your data means knowing all the various organizations that have copies of your data—a nonstarter for the vast majority of people—and then requires reaching out to them one by one, either via email or via an individualized data portal (if the organization has such a mechanism). And even if an individual user was able to know and recall every organization in possession of their data and was willing to take the time to exercise their rights in relation to each individual organization, the results would almost certainly be unsatisfactory, as data deletion requests leave users with no real ability to see or verify what data was deleted and what data was retained in relation to various legal exceptions.[140] By the same token, data access requests still typically return copies of users' data in unusable and often unintelligible formats.[141]

---

https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 [https://perma.cc/SP5E-BNWL]; *see also, e.g.*, *California Consumer Privacy Act (CCPA)*, ELEC. PRIV. INFO. CTR., https://epic.org/california-consumer-privacy-act-ccpa/ [https://perma.cc/S7RT-AGTD] (last visited Mar. 3, 2024) (providing guidance to consumers on how to exercise their deletion request rights under California's Consumer Privacy Act).

139. *See* Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh & Florian Schaub, An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites 395 (Sept. 17, 2022) (unpublished manuscript), https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-hana_habib.pdf [https://perma.cc/DL32-R97G] (observing that "[d]ata deletion mechanisms vary by website"); SCHNEIER, *supra* note 56, at 41–61, 78–82, 210–12; *Your Data Is Shared and Sold . . . What's Being Done About It?*, KNOWLEDGE AT WHARTON (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/ [https://perma.cc/Q6B8-KBLC] (noting that "consumers are often not aware all of this tracking and analysis is going on and thus don't do anything about it" and that "companies don't make it easy for consumers to find out exactly how their data is being used"); U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-106096, CONSUMER DATA: INCREASING USE POSES RISKS TO PRIVACY (2022) ("As technologies change, consumers may not always know what data businesses are collecting about them, or how those data are used and shared. Advanced, internet-connected technologies help businesses gather increasing amounts of personal data, track online behavior, and monitor consumers' locations and activities, intensifying concerns about the privacy and accuracy of consumer data."); *see also* TUROW ET AL., *supra* note 108, at 2–6.

140. *See* Habib et al., *supra* note 139, at 395 ("How soon the data would actually be deleted was often ambiguous."); *id.* (documenting that some websites allow users to remove only certain types of data or temporarily suspend their account, whereas others allow users to delete all of their data permanently); TUROW ET AL., *supra* note 108, at 2–10 (explaining that most users are unaware of how their data is being collected, stored, and used). To provide users with more data control, for instance, the EU's GDPR allows for data subjects to exercise a right to erasure, sometimes referred to as a right to data deletion or "right to be forgotten." Regulation 2016/679, *supra* note 54, arts. 17, 19. Other data rights include legal and technological innovation that provides more meaningful control over one's data. *See* SCHNEIER, *supra* note 56, at 200–06.

141. *See, e.g.*, Issie Lapowsky, *One Man's Obsessive Fight to Reclaim His Cambridge Analytica Data*, WIRED (Jan. 25, 2019, 6:00 AM), https://www.wired.com/story/one-mans-obsessive-fight-to-reclaim-his-cambridge-analytica-data/ [https://perma.cc/6GUT-BVJS] (documenting a consumer's failure to receive an adequate and complete response to his data disclosure request under U.K. law); *see also* SCHNEIER, *supra* note 56, at 214–16.

Our failure to make data truly visible and to place it under ongoing control has real costs, both for the individuals who share their data and for the organizations and governments with whom they share it.

CONCLUSION

Technological innovation has the potential to reinforce democracy and national security in the AI age. However, realizing this potential will require forward-looking perspectives from lawmakers and regulators, as well as from leaders in civil society, the military, and the national security community. It is difficult to conceptualize the legal and technical infrastructure necessary to not only regulate the newly introduced innovation, but also to guarantee that the innovation is safe and effective for users of the innovation on an individual level. It is even more of a challenge to ensure that AI can operate in a way that reinforces democracy, sovereignty, and national security interests.

The Flemish Parliament's Decree should be understood as federalized data privacy infrastructure. This new type of infrastructure can be viewed as an emerging type of critical protection and AI governance under a critical infrastructure framework. Whether the Solid protocol or other forms of data privacy infrastructure should be introduced in other nations is a question that warrants further inquiry, particularly once the efficacy of Privacy Pods or "data vaults" can be assessed.

After the revelations of foreign interference in the 2016 presidential election, the U.S. Government recognized the way that election systems and data systems were vulnerable to exploitation by foreign adversaries. This Essay opens a conversation on whether and how data privacy infrastructure can be seen as part of a nation's critical infrastructure. Part of that dialogue involves questioning whether data privacy infrastructure can and should be federalized the way that other critical infrastructure programs are federalized for the nation's protection. Cyber defense and preempting information warfare threats require examining how data privacy infrastructure can be seen as a potential integrated strategy in constructing AI governance legally and technically to secure both data privacy rights and security.