MINIMIZING PRIVACY RISKS IN REGULATING DIGITAL PLATFORMS: INTEROPERABILITY IN THE EU DMA

BY MIKOŁAJ BARCZENTEWICZ[1]

[1] Senior Scholar, International Centre for Law and Economics; Senior Lecturer and Research Director, University of Surrey Law and Technology Hub; Fellow, Stanford Law School. This paper is based on my working paper *Privacy and Security Implications of Regulation of Digital Services in the EU and in the US*, Stanford–Vienna Transatlantic Technology Law Forum, TTLF Working Papers No. 84 (2022).

CPI ANTITRUST CHRONICLE
JULY 2022

CPI Antitrust Chronicle July 2022

MINIMIZING PRIVACY RISKS IN REGULATING DIGITAL PLATFORMS: INTEROPERABILITY IN THE EU DMA

By Mikołaj Barczentewicz

The EU Digital Markets Act purports to benefit consumers and improve the competitiveness of digital markets. It is likely to have negative and unaddressed consequences, however, in terms of information privacy and security. I illustrate this by focusing on the DMA's interoperability mandates. Only one of those obligations — on the interoperability of messaging services — is accompanied by a potentially adequate safeguard: a requirement that any third-party service must offer at least the same level of user security as the original service. This is a very demanding standard, which may render the interoperability provision a dead letter for the foreseeable future, but which nonetheless offers welcome privacy benefits from the consumer perspective. The remaining obligations that I analyze are accompanied either by no safeguards, or by insufficient safeguards.

I. INTRODUCTION

It is notoriously difficult to use the law to *strengthen* information privacy and security, even where that is the explicit goal of legislation. Thus, perhaps the least we should expect of the law is not to unintentionally weaken the level of privacy and security. Unfortunately, pursuing even seemingly unrelated policy aims may sometimes yield that negative effect. Here, I analyze some of the provisions included in the proposed EU Digital Markets Act ("DMA").[2] The DMA purports to benefit consumers and improve the competitiveness of digital markets. It is likely to have negative and unaddressed consequences, however, in terms of information privacy and security.

For brevity, I chose to focus on one regulatory solution: interoperability mandates in the DMA. I conclude that only one of those obligations — on the interoperability of messaging services — is accompanied by a potentially adequate safeguard: a requirement that any third-party service must offer at least the same level of user security as the original service. This is a very demanding standard, which may render the interoperability provision a dead letter for the foreseeable future, but which nonetheless offers welcome benefits from the consumer perspective. The remaining obligations that I analyze are accompanied either by no safeguards, or by insufficient safeguards.

II. INTEROPERABILITY

Interoperability[3] increasingly is put forward as a potential solution to some of the problems associated with digital services generally, and with large online platforms, in particular.[4] For example, interoperability might allow third-party developers to offer different "flavors" of social-media news feeds, with varying approaches to content ranking and moderation. Were this approach to take hold, it might render the specific content-moderation decisions made by Facebook or other platforms less central to the user experience. Facebook users could choose alternative content moderators, delivering the kind of news feed that those users desire or expect.[5]

The concept of interoperability is popular not only among thought leaders, but also among legislators. The DMA includes interoperability mandates, as do federal bills introduced in the United States by Rep. Mary Gay Scanlon,[6] Rep. David Cicilline,[7] and Sen. Amy Klobuchar.[8]

A. Privacy and Security Risks of Interoperability

At the most basic level, in the context of digital services, interoperability refers to the capacity to exchange information between computer systems. Email is an example of an interoperable standard that most of us use today. It is telling, however, that supporters of interoperability mandates point to services like email as their model examples. Email (more precisely, the SMTP protocol) originally was designed in a notoriously insecure way.[9] It is a perfect illustration of the opposite of privacy-by-design.[10] As originally conceived, email offered roughly the

[2] *Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector* ("Digital Markets Act"). Most recent publicly available version from 11 May 2022 is available at https://www.consilium.europa.eu/media/56086/st08722-xx22.pdf.

[3] This section builds on my previous short text *The Digital Markets Act Shouldn't Mandate Radical Interoperability*, Truth on the Market (19 May 2021) https://truthonthemarket.com/2021/05/19/the-digital-markets-act-shouldnt-mandate-radical-interoperability.

[4] Stephen Wolfram, *Testifying at the Senate About A.I.-Selected Content on the Internet*, Stephen Wolfram's Writings (25 Jun. 2019) https://writings.stephenwolfram.com/2019/06/testifying-at-the-senate-about-a-i-selected-content-on-the-internet/; Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, Knight First Amendment Institute (21 Aug. 2019) https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech; Daphne Keller, *If Lawmakers Don't Like Platforms' Speech Rules, Here's What They Can Do About It. Spoiler: The Options Aren't Great*, Techdirt (9 Sep. 2020) https://www.techdirt.com/articles/20200901/13524045226/if-lawmakers-dont-like-platforms-speech-rules-heres-what-they-can-do-about-it-spoiler-options-arent-great.shtml; Francis Fukuyama, *Making the Internet Safe for Democracy*, 32 J. Democr. 37 (2021) https://www.journalofdemocracy.org/articles/making-the-internet-safe-for-democracy.

[5] Of course, this may have its own negative consequences in strengthening "filter bubbles" and fueling polarization.

[6] H.R. 3849, 117th Congress (2021-2022), https://www.congress.gov/bill/117th-congress/house-bill/3849.

[7] H.R. 3816, 117th Congress (2021-2022), https://www.congress.gov/bill/117th-congress/house-bill/3816.

[8] S. 2992, 117th Congress (2021-2022). https://www.congress.gov/bill/117th-congress/senate-bill/2992.

[9] See. e.g. Durumeric et al, *Neither Snow Nor Rain Nor MITM… An Empirical Analysis of Email Delivery*, Security Proceedings of the 2015 Internet Measurement Conference (2015).

[10] See Article 25 of the Regulation (EU) 2016/679 (General Data Protection Regulation).

same levels of privacy and security as a postcard message sent without an envelope that passes through many hands before reaching the addressee. Even today, email continues to be a source of security concerns due to its prioritization of interoperability.[11]

Using currently available technology to provide alternative interfaces or moderation services for social-media platforms, third-party developers would have to be able to access much of the platform content potentially available to a user. This would include not just content produced by users who explicitly agree to share their data with third parties, but also content — e.g. posts, comments, likes — created by others who may have strong objections to such sharing. It does not require much imagination to see how, without adequate safeguards, mandating this kind of information exchange would inevitably result in something akin to the 2018 Cambridge Analytica data scandal.[12]

Imposing a legal duty on digital service providers to make their core services interoperable with any third party creates, as noted by Cory Doctorow and Benedict Cyphers, at least three categories of risks:

1. Data sharing and mining via new APIs;
2. New opportunities for phishing and sock puppetry in a federated ecosystem; and
3. More friction for platforms trying to maintain a secure system.[13]

1. Friction in Ensuring Security

Bearing in mind Doctorow & Cyphers' last point, a crude interoperability mandate could make it much more difficult for service providers to keep up with the fast-evolving threat landscape. For example, it may seem a good idea to require service providers to submit all changes to their interoperability standards (interfaces) for external review, possibly by a public authority. This could potentially help to ensure that service providers do not "break" interoperability or discriminate against some third-party services that would want to benefit from it. However, imposing such a requirement would introduce delay in responding to new threats, potentially putting user data at risk. When it can take just seconds to exfiltrate millions of user profiles, delaying security patches by weeks or even days through regulation is unacceptable.

2. "Phishing and Sock Puppetry"

True interoperability of digital services would mean a two-way exchange of information. For online platforms like social networks, this would mean that, e.g. a Facebook user could interact with users of other interoperable platforms as if they were also Facebook users (exchange direct messages, see their posts, add comments and so on). Doctorow & Cyphers recognized that this would mean that any identity controls (e.g. Facebook's requirement to use real names) could easily be undermined if criminals or state actors run or control their own interoperable platforms. Those in control of such a platform could appear to users of other platforms as their friends in an attempt to hack them (e.g. phishing through direct messages). Such deception already happens on major online platforms, but those platforms are legally free to adopt measures to counteract it. A broad interoperability mandate would disallow service providers from vetting other providers and from imposing their own identity requirements (e.g. requiring the use of real names).

Those risks are well-illustrated by how often users are victimized through one of the most widely used interoperable protocols: telephony and, in particular, telephone numbers.[14] Due to design choices in interoperability of telephony systems, which entirely sidelined security concerns, it is often trivial for any malicious actor to "spoof" the number that appears in a call recipient's "caller ID" feature. They may thus to appear to a victim as if they are calling from, e.g. the victim's bank. Having created an insecure-by-design system that facilitated widespread consumer harm, regulators are slowly and, to date, ineffectively playing catch-up.[15]

[11] See, e.g. Sydney Li, A Technical Deep Dive into STARTTLS Everywhere, Electronic Frontier Foundation (25 Jun. 2018) https://www.eff.org/deeplinks/2018/06/technical-deep-dive-starttls-everywhere.

[12] On the Cambridge Analytica scandal, see, e.g. *Investigation into Data Analytics for Political Purposes*, UK Information Commissioner, https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes.

[13] Cory Doctorow & Benedict Cyphers, *Privacy Without Monopoly: Data Protection and Interoperability*, Electronic Frontier Foundation (12 Feb. 2021) https://www.eff.org/wp/interoperability-and-privacy.

[14] See e.g. Jovi Umawing, More than a Quarter of Americans Fell for Robocall Scam Calls on Past Year, Malwarebytes (1 Jun. 2022) https://blog.malwarebytes.com/reports/2022/06/more-than-a-quarter-of-americans-fell-for-robocall-scam-calls-in-past-year.

[15] *Ibid.*

3. General Data-sharing Risks

Effective interoperability requires sharing of sensitive data among different service providers through new two-way real-time interfaces ("APIs"). Doctorow & Cyphers put forth a plan endorsing broad interoperability mandates,[16] but admirably, they acknowledge the important security and privacy tradeoffs such a mandate would impose. Promoters of the bills analyzed herein frequently do not account for such costs. It is therefore worth analyzing these harms from the perspective of proponents of interoperability mandates. Doctorow & Cyphers are open about the scale of the risk: "[w]ithout new legal safeguards to protect the privacy of user data, this kind of interoperable ecosystem could make Cambridge Analytica-style attacks more common."[17]

The Cambridge Analytica incident illustrates the risks well. The personal data that Cambridge Analytica ultimately used was collected through a Facebook app created by an academic researcher.[18] The app was used by 270,000 people, who expressly granted permission for the app to access their account information, including information about their Facebook contacts. This is how the app's author collected data on more than 50 million Facebook users.

A potential future Cambridge Analytica could benefit from a poorly drafted interoperability mandate. Today, Facebook can and does stop third-party developers who try to exfiltrate data from the platform in violation of the company's terms. Some even believe that Facebook does so too vigorously.[19] But under an interoperability mandate, Facebook may be prevented from vetting and denying access to third parties if a user clicks "yes" in a consent popup. And users may habitually click "yes" in consent popups, irrespective of any "dark patterns" that would nudge them to authorize the desired action ("popup fatigue").[20] This is understandable: users may simply want to access the desired functionality (e.g. to play a game) and may not be willing to invest sufficient time and effort to parse the consequences of what, exactly, they are authorizing.

Thus, one risk is that users will authorize interoperability to an extent that may later surprise them, even if the third-party service providers provide all necessary information in an accessible and intelligible form. It may just be that users will only start caring about the consequences of their choices once they materialize, not before they make a choice.

It is, however, unrealistic to expect all third-party service providers to obey the rules, including rules stipulating that one should act in accordance with unstated user expectations. Some third-party providers may act in good faith when they push the boundaries of what is permitted, due to the (potentially erroneous) belief that users are better served in some particular way. But some will intentionally engage in illegal — even criminal — activity.[21] Such actors may come from foreign jurisdictions (outside of the EU and the United States), which could render *ex post* enforcement of legal rules against them particularly difficult.

B. How can the Risks be Addressed?

What could be done to make interoperability reasonably safe? There are several constraints that an acceptable solution should address.

1. Constraints

First, solutions should be targeted at users of digital services as the really exist, without assuming away some common but inconvenient characteristics. In particular, solutions should not assume unrealistic levels of user interest or technical acumen. As discussed above, users may not

[16] *Supra* note 13.

[17] *Supra* note 13, at 28.

[18] See also Kurt Wagner, *Here's How Facebook Allowed Cambridge Analytica to Get Data for 50 Million Users*, Vox (17 May 2018) https://www.vox.com/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data.

[19] Mitch Stolz & Andrew Crocker, *Once Again, Facebook Is Using Privacy As A Sword To Kill Independent Innovation*, Electronic Frontier Foundation (20 Nov. 2020) https://www.eff.org/deeplinks/2020/11/once-again-facebook-using-privacy-sword-kill-independent-innovation.

[20] See, e.g. Cristian Bravo-Lillo et al., *Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It*, Proceedings of the 10th Symposium On Usable Privacy and Security (2014); Anthony Vance et al., *Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiments*, 42 Management Information Systems Quarterly (MISQ) 355 (2018).

[21] As the Organisation for Economic Co-operation and Development (OECD) noted: "Even where individuals and organisations agree on and consent to specific terms for data sharing and data re-use, including the purposes for which the data should be re-used, there remains a significant level of risk that a third party may intentionally or unintentionally use the data differently." *Enhancing Access to and Sharing of Data. Reconciling Risks and Benefits for Data Re-use Across Societies*, Organisation for Economic Co-operation and Development (2019), chapter 4, Risks and challenges of data access and sharing." https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en.

demonstrate concern about privacy and security settings *until* some negative consequences materialize from authorized interoperability. It is telling that mandate proponents tend to invoke as models for interoperability those digital services that are used by exceptionally motivated and informed users, which also tend to be small-scale (e.g. Mastodon) or have unacceptably poor usability for most of today's Internet users (e.g. Usenet).[22]

Second, solutions must address the issue of effective enforcement. Doctorow & Cyphers argued that there is a "need for better privacy law" to make interoperability safe.[23] Somewhat surprisingly, however, Doctorow wrote soon after that "the existence of the GDPR *solves* the thorniest problem involved in interop and privacy."[24] But problems can be solved by legislation only if such legal rules are followed; this requires addressing the problem of procedures and enforcement.

The current EU framework and enforcement of privacy law offers little confidence that misuses of broadly construed interoperability would be detected and prosecuted, much less that they would be prevented.[25] This is especially true for smaller and "judgment-proof" rule-breakers, including those from outside the European Union. In the United States, no such privacy framework exists, as yet, on the federal level; state laws like California's Consumer Privacy Act face enforcement problems similar to the EU GDPR.[26]

When digital service providers are placed under a broad interoperability mandate with non-discrimination provisions (preventing effective vetting of third parties, unilateral denials of access, etc.), the burden placed on law enforcement is mammoth. It could take just one bad actor — perhaps working from Russia or North Korea — to take advantage of interoperability mandates in order to exfiltrate user data or to execute a hacking (e.g. phishing) campaign, causing immense damage. Of course, such foreign bad actors would be in violation of the EU GDPR, but that is unlikely to have any practical significance.

It would not be sufficient to allow (or require) service providers to enforce merely technical filters, such as a requirement to check whether the interoperating third parties' IP addresses are located in jurisdictions with sufficient privacy protections. For motivated bad actors, evading such technical limitations does not pose significant difficulty.

2. The Open Banking Solution

One solution that might potentially address the information privacy and security concerns in interoperability of digital services, without significant technological changes, would be to follow the example of the UK Open Banking regime.[27] As described by the United Kingdom's Competition and Markets Authority:

> Open Banking enables consumers and small and medium-sized enterprises ("SMEs") to share their bank and credit card transaction data securely with trusted third parties who are then able to provide them with applications and services which save time and money.[28]

Open Banking was introduced in 2017 and is a heavily regulated interoperability scheme with its own special oversight body — the Open Banking Implementation Entity (OBIE). According to Geoffrey Manne & Sam Bowman, one of the key lessons from Open Banking is that:

[22] "mastodon" https://github.com/mastodon/mastodon; https://en.wikipedia.org/wiki/Usenet.

[23] *Supra* note 13, at 33.

[24] Cory Doctorow, *The GDPR, Privacy and Monopoly*, Electronic Frontier Foundation, (11 Jun. 2021) https://www.eff.org/deeplinks/2021/06/gdpr-privacy-and-monopoly.

[25] See e.g. *Communication from the Commission to the European Parliament and the Council*, "Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation" COM(2020) 264, 24 Jun. 2020, available at https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v6_1.pdf; *The Long and Winding Road: Two Years of the GDPR: A Cross-Border Data Protection Enforcement Case from a Consumer Perspective*, Bureau Européen des Unions de Consommateurs (5 Aug. 2020) available at https://www.beuc.eu/publications/beuc-x-2020-074_two_years_of_the_gdpr_a_cross-border_data_protection_enforcement_case_from_a_consumer_perspective.pdf.

[26] An apparently credible legislative proposal for a U.S. federal privacy statute was released for discussion in June 2022 by a bipartisan group of members of the House of Representatives and of the Senate. See *House and Senate Leaders Release Bipartisan Discussion Draft of Comprehensive Data Privacy Bill*, U.S. House Committee on Energy and Commerce (3 Jun. 2022) https://energycommerce.house.gov/newsroom/press-releases/house-and-senate-leaders-release-bipartisan-discussion-draft-of.

[27] On Open Banking, see, e.g. *Open Banking*, Open Banking Implementation Entity, https://www.openbanking.org.uk; Sam Bowman, *Why Data Interoperability Is Harder Than It Looks: the Open Banking Experience*, CPI Antitrust Chronicle (April 2021) available at https://laweconcenter.org/wp-content/uploads/2021/06/CPI-Bowman.pdf; Geoffrey A. Manne & Sam Bowman, *Issue Brief: Data Portability and Interoperability: The Promise and Perils of Data Portability Mandates as a Competition Tool*, International Center for Law & Economics (10 Sep. 2020) https://laweconcenter.org/resource/issue-brief-data-portability-and-interoperability-the-promise-and-perils-of-data-portability-mandates-as-a-competition-tool.

[28] *Update on Open Banking*, Competition and Markets Authority (5 Nov. 2021) https://www.gov.uk/government/publications/update-governance-of-open-banking/update-on-open-banking.

Open Banking has been costly and time-consuming to implement. This is despite the fact that the data involved — chiefly transaction history and account balance data — is relatively simple and does not differ between different banks. The main difficulties have been around security, user authentication, and the authorization of new third-party services, and it has taken ongoing monitoring by a new agency set up by the CMA and several re-iterations to get these right, and may require more in the future. For services where the data is more sophisticated and unique to each service, the cost of implementing data portability and/or interoperability may be commensurately higher.[29]

Applying the lessons from Open Banking to digital services could mean that:

1. There would likely be a need for a regulator to set technical standards, oversee the scheme, and possibly to enforce the rules in case of violations.
2. To be able to participate, any potential interoperating party would have to undergo expensive and thorough regulatory vetting (of the kind that financial institutions need to be allowed to operate).

Among the main problems with applying the Open Banking model to digital services is that Open Banking applies to relatively simple and homogenous data (i.e. bank transactions), whereas the digital services offered by the largest providers are much more varied and continuously evolve. Imposing the kinds of detailed technical data standards used in Open Banking would stifle innovation in digital services. Given that some standardization of data formats is likely to be a feature of any interoperability mandate, this may be sufficient reason not to adopt an interoperability mandate, but that issue is beyond the scope of this paper.

Requiring all participating parties to undergo regulatory approval, as in Open Banking, could significantly address the problems of bad actors or of insufficient motivation to follow privacy and security rules. However, some proponents of broad interoperability might object that this would partially defeat the purpose of interoperability mandates, as few small startups would be able to benefit from it. But it must be asked in response whether the risks of opening interoperability to such potentially unreliable providers are worth the potential benefits of their involvement.

C. Mandated Interoperability and Data Flows in the EU Digital Markets Act

The original DMA proposal included several interoperability and data-portability obligations regarding the designated "core platform services" of "gatekeepers" — i.e. the largest online platforms. Those provisions were changed considerably during the legislative process. The most recent version of the DMA, from 11 May 2022, contains, among other provisions:

1) a prohibition on restricting users — "technically or otherwise" — from switching among and subscribing to software and services "accessed using the core platform services of the gatekeeper" (Art 6(6));
2) an obligation for gatekeepers to allow interoperability with their operating system or virtual assistant (Art 6(7)); and
3) an obligation "on interoperability of number-independent interpersonal communications services" (Art 7).

To varying degrees, these provisions attempt to safeguard privacy and security interests, but the first two do so in a clearly inadequate way.

First, the Article 6(6) prohibition on restricting users from using third-party software or services "accessed using the core platform services of the gatekeeper" notably applies to web services (web content) that a user can access through the gatekeeper's web browser (e.g. Safari for iOS).[30] Given that web content is typically not installed in the operating system, but used through a browser (i.e. likely "accessed using a core platform service of the gatekeeper"), earlier "side-loading" provisions (Article 6(4), which is discussed further below) would not apply here.

This leads to what looks like a significant oversight: the gatekeepers appear to be almost completely disabled from protecting their users when they use the Internet through web browsers, one of the most significant channels of privacy and security risks. The Federal Bureau of Investigation ("FBI") has identified "phishing" as one of the three top cybercrime types, based on the number of victim complaints.[31] A successful phishing attack normally involves a user accessing a website that is impersonating a service the user trusts (e.g. an e-mail account or corporate login). Browser developers can prevent some such attacks, e.g. by keeping "block lists" of websites known to be malicious and warning about,

[29] *Supra* note 27, Manne & Bowman, at 23.

[30] Web browsers are defined as core platform services in Art 2(2) DMA.

[31] *Internet Crime (IC3) Report 2020*, Federal Bureau of Investigation (2020) available at https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

or even preventing, access to such sites. An exceptionless prohibition on platforms restricting their users from accessing third-party services, however, would also prohibit this vital cybersecurity practice.

Under Art 6(4), in case of installed third-party software, the gatekeepers can take:

> measures to ensure that third party software applications or software application stores do not endanger the integrity of the hardware or operating system provided by the gatekeeper, provided that such measures go no further than is strictly necessary and proportionate and are duly justified by the gatekeeper.

The gatekeepers can also apply:

> measures and settings other than default settings, enabling end users to effectively protect security in relation to third party software applications or software application stores, provided that such measures and settings go no further than is strictly necessary and proportionate and are duly justified by the gatekeeper.

None of those safeguards, insufficient as they are — see the discussion below of Art 6(7) — are present in Art 6(6). Worse still is that the anti-circumvention rule in Art 13(6) applies here, prohibiting gatekeepers from offering "choices to the end-user in a non-neutral manner." That is precisely what a web-browser developer does when warning users of security risks or when blocking access to websites known to be malicious — e.g. to protect users from phishing attacks.

This concern is not addressed by the general provision in Art 8(1) requiring the gatekeepers to ensure "that the implementation" of the measures under the DMA complies with the GDPR, as well as "legislation on cyber security, consumer protection, product safety." The first concerns is that this would not allow the gatekeepers to offer a *higher* standard of user protection than that required by the arguably weak or overly vague existing legislation. Also, given that the DMA's rules (including future delegated legislation) are likely to be more specific — in the sense of constituting *lex specialis* — than EU rules on privacy and security, establishing a coherent legal interpretation that would allow gatekeepers to protect their users is likely to be unnecessarily difficult.

Second, the obligation from Art 6(7) for gatekeepers to allow interoperability with their operating system or virtual assistant only includes the first kind of a safeguard from Art 6(4), concerning the risk of compromising "the integrity of the operating system, virtual assistant or software features provided by the gatekeeper." However, the risks from which service providers aim to protect users today are by no means limited to system "integrity." A user may be a victim of, e.g. a phishing attack that does not explicitly compromise the integrity of the software they used.

Moreover, as in Art 6(4), there is a problem with the "strictly necessary and proportionate" qualification. This standard may be too high and push gatekeepers to offer more lax security to avoid liability for adopting measures that would be judged by EU Commission and the courts as going beyond what is strictly necessary or indispensable.

The relevant recitals from the DMA preamble, instead of aiding in interpretation, add more confusion. The most notorious example is in recital 50, which states that gatekeepers "should be prevented from implementing" measures that are "strictly necessary and proportionate" to effectively protect user security "as a default setting or as pre-installation." What possible justification can there be for prohibiting providers from setting a "strictly necessary" security measure as a default? We can hope that this manifestly bizarre provision will be corrected in the final text, together with the other issues identified above.

Finally, there is the obligation "on interoperability of number-independent interpersonal communications services" from Art 7. Here, the DMA takes a different and much better approach to safeguarding user privacy and security. Art 7(3) states that: "The level of security, including the end-to-end encryption, where applicable, that the gatekeeper provides to its own end users shall be preserved across the interoperable services." There may be some concern that the Commission or the courts will not treat this rule with sufficient seriousness. Ensuring that user security is not compromised by interoperability may take a long time and may require excluding many third-party services that had hoped to benefit from this DMA rule. Nonetheless, EU policymakers should resist watering down the standard of equivalence in security levels, even if it renders Art 7 a dead letter for the foreseeable future.

It is also worth noting that there will be no presumption of user opt-in to any interoperability scheme (Art 7(7)-(8)), which means that third-party service providers will not be able to simply "on-board" all users from a gatekeeper's service without their explicit consent. This is to be commended.

III. CONCLUSIONS

By and large, the DMA betrays a policy preference for privileging uncertain and speculative competition gains at the cost of introducing new and clear dangers to information privacy and security. This is clearly the case in Articles 5 and 6 of the DMA. Proponents of those or even stronger legislative interventions have demonstrated that they are much more concerned, for example, that privacy safeguards are "not abused by Apple and Google to protect their respective app store monopoly in the guise of user security."[32] Given the difficulties in ensuring effective enforcement of privacy protections, however (especially with respect to actors coming from outside of the EU, the United States, and other broadly privacy-respecting jurisdictions), the mentions of privacy and security in Articles 5 and 6 amount to not much more than lip service. It is reasonable to expect a much more detailed vision of concrete safeguards and mechanisms of enforcement from policymakers who are proposing rules that come with entirely predictable and very significant privacy and security risks. One solution worth considering is already to be found in Article 7(3) DMA: the requirement that any third-party service providers offer at least the same level of security as the gatekeepers.

I do not want to suggest that interoperability is undesirable. The argument of this paper was focused on *legally mandated* interoperability. Firms experiment with interoperability all the time; the prevalence of open APIs on the Internet is a testament to this. My aim, however, is to highlight that interoperability is complex and exposes firms and their users to potentially large-scale cyber vulnerabilities. Generalized obligations imposed on firms to open their data or to create service interoperability short-circuit the private ordering processes that seek out the forms of interoperability and sharing that pass a cost-benefit test.

The result will likely be both overinclusive and underinclusive. It would be overinclusive by requiring all firms that are in the regulated class to broadly open their services and data to all interested parties, even where it wouldn't make sense for privacy, security, or other efficiency reasons. It is underinclusive, because the broad mandate will necessarily sap regulated firms' resources and deter them from looking for new innovative uses that *might* make sense, but that are outside of the broad mandate. Thus, the likely result is less security and privacy, more expense, and less innovation.

[32] Damien Geradin, *Digital Markets Act (DMA): Where Is the Council Headed to?*, The Platform Law Blog (18 Oct. 2021) https://theplatformlaw.blog/2021/10/18/digital-markets-act-dma-where-is-the-council-headed-to.