On joined up law-making: the privacy/safety/security dynamic, and what this means for data governance

Review of data governance legislation in train in the European Union reveals a number of potential problems for security operations worldwide. This paper explores key tensions between different rights and interests, and recent proposals for achieving greater policy and regulatory integration.

Victoria Baines
Visiting Fellow, Bournemouth University – vbaines@bournemouth.ac.uk[i]

The last ten years have witnessed the introduction of landmark data governance measures in the European Union and beyond. In the interests of safety, security and the fundamental right to a private life, data has been subjected to controls. At the same time, measures aimed at increasing transparency, asserting individual ownership over personal data and fostering innovation have emphasised the need for openness. This tension between control and openness is a key dynamic in data governance that merits further scrutiny and continued consideration by stakeholders and legislators alike. As the EU Digital Services package makes its way through the legislative process, and as the EU-US Trade and Technology Council gets to grips with a range of data-centred issues, this paper seeks both to probe interactions between control and openness imperatives, and to highlight the risks attached to siloed regulation.

The privacy/safety/security dynamic

In the field of public safety, the relationship between security/safety and privacy is often depicted as a trade-off, not least in the debate concerning online surveillance.[ii] According to this framing, the ability of government authorities to intrude into citizens' private communications is to some degree accepted for the prevention and investigation of serious crime and terrorism, and where there is judicial or similar oversight to challenge its abuse. Following this line of argument, in countries where there is greater surveillance of citizens' online and offline activities, privacy is ceded in the interest of public safety; in those countries in which citizens enjoy greater freedom, this freedom may be accompanied by a perception of reduced levels of public safety and security. While this thinking is by no means unassailable, it is the foundation of most intelligence and national security work the world over: the more a government knows about its citizens, the greater the control it has over public safety and security issues, whether these are misdemeanours or national security threats.

Figure 1: Simplified visualisation of the privacy/public safety dynamic

Although the graphic above over-simplifies the considerations at stake, it nevertheless illustrates the need to consider privacy and public safety *together*. The conception of this tension as a spectrum reflects the fact that policy makers and legislators around the world may

choose to prioritise public safety over privacy, or vice versa, or indeed seek a mid-point between the two. At the same time, equal consideration for privacy and public safety may not result in 'moving the needle', but in cut-outs for certain types of data, actors and purposes, as in the exemption of law enforcement purposes from the requirements of the General Data Protection Regulation (2016/679, Article 19), and the concurrent force of the Law Enforcement Directive (2016/680).

But this is not *simply* a public safety / privacy interaction. The dynamic becomes more complex when the concept of information security is introduced. Defined by the Oxford English Dictionary as "the state of being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this", information security incorporates key elements of privacy and public safety, while being not quite one or the other.

The European Union benefits from a mature information security profession that has been active for well over two decades, and is supported by the European Network and Information Security Agency (ENISA) and the EU Cybersecurity Strategy. The Network and Information Security (NIS) Directive (2016/1148) provides the legal framework for competent authorities to build national capacity through the operations of Computer Security Incident Response Teams (CSIRTs), Member State strategic cooperation and information sharing, and the fostering of a security culture in sectors providing essential services and digital infrastructure. Of note, the Directive simultaneously "establishes security and notification requirements for operators of essential services and for digital service providers", and in doing so applies *both* control measures for the protection of data *and* provision for sharing data in the interest of public safety and national security.

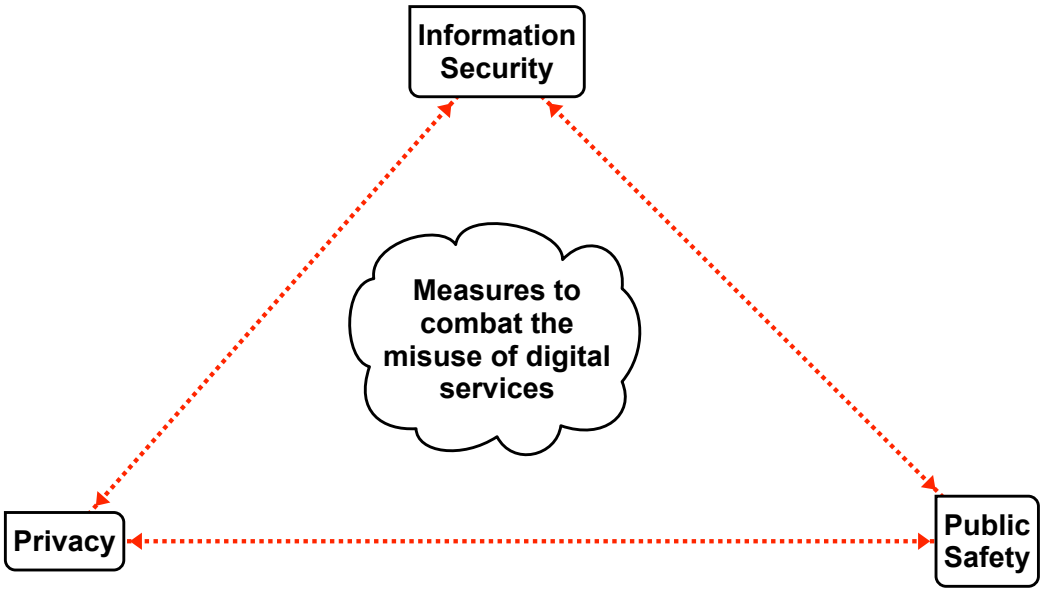

Figure 2: Simplified visualisation of privacy/public safety/information security dynamics

Failure to give due weight in data governance to each of these imperatives can result in unintended and counter-productive consequences. Two cases in recent years will serve to illustrate.

In 2015, the then Belgian Privacy Commission (now Belgian Data Protection Authority) initiated a case against Facebook for its use of cookies to track the web browsing of internet users in Belgium, including those without Facebook accounts. While the Court of First Instance of Brussels ruled that this processing of personal data violated Belgian law, Facebook defended its use of the 'datr' cookie for security reasons, outlining its use to "help differentiate legitimate visits to our website from illegitimate ones", and warning that the legal action "could undermine our efforts to keep the accounts of people in Belgium safe."[iii] Facebook was ordered to desist from deploying these cookies in Belgium, but successfully appealed in 2016 on the basis that the Belgian regulator had no jurisdiction over its European operations headquartered in Ireland.

This did not, however, mark the end of the matter: Facebook was once again convicted by the Court of First Instance in 2018, prompting a fresh appeal on jurisdictional grounds by Facebook in 2019 and subsequent referral to the European Court of Justice to clarify the competency of the Belgian Data Protection Authority under GDPR, especially in relation to the 'one-stop shop' mechanism, which designates the Irish Data Protection Commission as the lead regulator for Facebook's European data processing. Notwithstanding that the basis for appeal is squarely on jurisdiction rather than purpose, the alleged use of the 'datr' cookie in combating the creation of fake Facebook accounts, account takeovers, theft of user content and denial of service attacks raises the possibility that, if successfully enforced, this prohibition would bring Belgian citizens greater data protection at the cost of greater vulnerability to certain threats to their security and that of the services they use. There is no objectively 'right' or 'wrong' answer in such a pass, but a situation in which competing rights need to be balanced, and alternative solutions developed where possible.

The global dimension is pertinent also when it comes to interactions between privacy legislation and personal safety. Globally popular US-based digital services are required by law to report apparent online child sexual exploitation to the National Center for Missing and Exploited Children (NCMEC), a non-governmental organisation with statutory responsibility for routing these reports to the relevant law enforcement agencies, including in the EU. In addition to responding to user and trusted partner flagging, these platforms use automated tools to identify known Child Sexual Abuse Material, the most widely used of which is Microsoft's PhotoDNA. This tool ascribes a unique signature – a 'hash value' – to known images, and enables platforms to detect, report and remove illegal material without having to view the content of communications. In 2020, US platforms made over 1 million such reports concerning users in the EU. These reports are used by Member States' law enforcement as evidence of the serious crimes of production, distribution and possession of Child Sexual Abuse Material.[iv]

This automated scanning was found to be non-compliant with the E-privacy Directive (2002/58/EC) after 21st December 2020, when the definition of 'electronic communication service' was updated to include number-independent interpersonal communications services such as voice chat, messaging and web-based mail, bringing them within scope of the Directive's provisions for the confidentiality of communications and traffic data (Articles 5(1) and 6(1)). NCMEC published data showing an immediate reduction in reports for the EU, which they attributed to the Directive's prohibition on platforms scanning EU users' content.[v] Following a concerted effort from child protection stakeholders, in July 2021 Regulation (EU) 2021/1232 on a temporary derogation from the relevant provisions of the Directive for the purpose of combating online child sexual abuse passed. The derogation applies until August 2024. So, while platforms can now resume their operations to combat child sexual exploitation

and abuse, a more lasting solution will need to be found that both upholds citizens' right to privacy and the right of children to live free from sexual abuse, as enshrined in the UN Convention on the Rights of the Child.

Indeed, key EU data governance instruments are undergoing or are set for reform. A review of the E-privacy Directive as part of the Digital Single Market Strategy led in 2017 to a proposal for an ePrivacy Regulation, which at the time of writing (late 2021) is awaiting Parliament's position in a first reading.[vi] Revision of the Network and Information Security Directive ('NIS 2') is awaiting decision from the relevant parliamentary committees.[vii] The hope is that lessons learned from interactions between earlier iterations and other instruments will inform a 'joined-up' approach to drafting and review that seeks to minimise unwanted consequences for privacy, safety and security. Other landmark data governance legislation is also in development, including a proposed Regulation on European data governance (or 'Data Act', 2020/0340/COD) providing for re-use of public sector data, business to government (B2G) data-sharing, and 'personal data-sharing intermediaries.'

The Digital Services Package and Information Security

Described by the European Commission as "the centrepieces of the European digital strategy", the proposed Digital Services Act (DSA, 2020/0361/COD) and Digital Markets Act (DMA, 2020/0374/COD) "aim to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses."[viii] The latter seeks to introduce a number of obligations on "gatekeepers", defined as a provider of core platform services that (Article 3)

- has a significant impact on the internal market;
- operates a core platform service which serves as an important gateway for business users to reach end users; and
- enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future.

A number of provisions in the current draft of the DMA would appear to be problematic for effective security operations, among them Article 5(a), which obliges gatekeepers to "refrain from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and provided consent in the sense of Regulation (EU) 2016/679." The reality of cybercrime investigation – whether by national law enforcement authorities or by platforms – is that cross-platform forensic investigation is often instrumental, even essential to timely enforcement and prevention of further offences against citizens and networks. Usernames and registration credentials such as email addresses and phone numbers are re-used in different online settings. Cross-platform analysis is both good information security practice and a widely-used law enforcement technique.[ix] The exemption for cases in which the end user has given consent to the platform is an inadequate remedy for this conflict, not least because criminals may be less likely to give consent.

In cases involving more sophisticated criminals such as Buster Hernandez, who used sexual blackmail and made death threats to at least 375 child victims, it can take several years of cross-platform analysis by service providers and law enforcement – sometimes working together – for the suspect to be identified and brought to justice.[x] Following the sentencing of Hernandez,

also known as BrianKil, US law enforcement released a list of his known usernames, to assist in the identification of further potential offences on other platforms.[xi] Without the ability to link datasets, opportunities to identify suspects and victims can be missed.

The DMA also obliges gatekeepers to "allow the installation and effective use of third party software applications or software application stores using, or interoperating with, operating systems of that gatekeeper and allow these software applications or software application stores to be accessed by means other than the core platform services of that gatekeeper" (Article 6(c)); also, to "allow business users and providers of ancillary services access to and interoperability with the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services" (6(f)). Granted that the current draft provides that "The gatekeeper shall not be prevented from taking proportionate 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" (6(c)), there is an identified need for greater clarity concerning the security impacts of such openness, and the process and precise circumstances for exemption from Articles 5 and 6 on grounds of public security (Article 9.2).[xii]

The Computer & Communications Industry Association's (CCIA) observation in relation to proposed US Antitrust legislation that measures aimed at improving access to markets, and data portability and interoperability, may in fact "inadvertently undermine U.S. national security by transferring sensitive data to adversaries and granting foreign competitors access to U.S. digital platforms, hardware, and software" may apply equally in the European context.[xiii] Without clear guidance on which third parties should be excluded from the obligations of the DMA for security reasons, gatekeepers may lose their ability to apply established security controls that restrict access to those deemed to pose a risk. In light of evidence for the use of malicious apps by state-sponsored cybercriminals and repressive governments, reducing controls in the interest of greater openness is also of primary geopolitical concern, with touch-points in the extensive and ongoing United Nations open-ended working group on developments in the field of information and telecommunications in the context of international security; also the proposal, led by Russia and China, for a new comprehensive treaty on countering the use of information and communications technologies for criminal purposes.[xiv]

Moreover, since large online platforms routinely make use of data from different sources in their security operations and restrict access to their services by third parties assessed to pose a security risk, exemption on grounds of public security is more likely to be the norm, not exceptional. In the absence of a systemic exemption, the administrative burden of processing requests for exemption from the obligations set out in Articles 5 and 6 may be considerable.

Similar concerns emerge from select provisions in the DMA's sibling instrument, the Digital Services Act (DSA). Article 15 of the draft text prescribes for the statement by providers to affected users of reasons for restricting content. Among the types of required information listed are "the facts and circumstances relied on in taking the decision, including where relevant whether the decision was taken pursuant to a notice submitted in accordance with Article 14 [notification by any individual or entity]" (15.2.(b)); and, "where applicable, information on the use made of automated means in taking the decision, including where the decision was taken in respect of content detected or identified using automated means" (15.2.(c))". Both these provisions appear to assume that all users are benevolent or infringe unwittingly. In the absence of a specific exemption for notifications submitted by law enforcement, criminal

justice authorities and intelligence agencies, the former risks 'tipping off' malicious actors that they are subject to investigation, and would arguably breach some states' requirement of confidentiality in relation to ongoing criminal investigations. An understandable drive towards greater transparency needs to be weighed carefully against the potential for jeopardising operations to counter serious crimes such as child abuse and terrorism, or efforts to disrupt coordinated disinformation campaigns.

Just as law enforcement authorities have to consider how much to disclose publicly about their techniques, online platforms will be faced with the task of trying to ensure that as far as possible their disclosure of reasons, techniques, and tools used for detection of infringing content does not hand malicious actors valuable information on how to 'game' platform protections or compromise network and information security. Article 15.3's stipulation that disclosure should be "as precise and specific as reasonably possible under the given circumstances" opens up the possibility for exemption, but does not provide a specific cut-out for public safety or security of the kind seen in the DMA. Article 33 on transparency reporting obligations for very large online platforms (VLOPs) prescribes public disclosure of additional information including the results of risk assessments on the dissemination of illegal content and influence operations such as those aimed at electoral interference (Article 26). It does, however, provide (Article 33.3) that:

> Where a very large online platform considers that the publication of information pursuant to paragraph 2 may result in the disclosure of confidential information of that platform or of the recipients of the service, may cause significant vulnerabilities for the security of its service, may undermine public security or may harm recipients, the platform may remove such information from the reports. In that case, that platform shall transmit the complete reports to the Digital Services Coordinator of establishment and the Commission, accompanied by a statement of the reasons for removing the information from the public reports.

By virtue of omission, smaller platforms do not explicitly have this option. Further, a proposed amendment in the context of the Committee on the Internal Market and Consumer Protection (IMCO) would see this paragraph deleted.[xv] Suggested insertion of an Article 33b in relation to interoperability, requiring VLOPs to "make the core functionalities of their services interoperable to enable cross-platform exchange of information with third parties," risks replicating the security issues of the DMA while confusing the terminology and provisions, perhaps most markedly in the duplicate designation of gatekeepers and VLOPs.[xvi] A suggested provision enabling VLOPs to limit such access when justified by an obligation under the NIS 2 Directive or GDPR (Amendment 106) again casts security as a secondary, even exceptional, consideration. The requirement for such limitations to "be notified within 24 hours to affected third parties and to the Agency" established under the act presents precisely the same problem of over-disclosure in cases where third parties are malicious actors. As in the DMA, so also in the DSA it is likely that restriction of information and access for public safety and security reasons will be more prevalent than currently anticipated.

The general thrust of both texts, that security is exceptional grounds, appears to run counter to the provisions of the existing Network and Information Security Directive, according to which "digital service providers should ensure the security of the network and information systems which they use" (52) through measures that "ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements: (a) the security of systems and facilities; (b) incident handling; (c) business

continuity management; (d) monitoring, auditing and testing; (e) compliance with international standards." (Article 16.1). Foremost among these international standards, and given headline mention by ENISA in its *Technical Guidelines for the implementation of minimum security measures for Digital Service Providers* is ISO27001, comprising no less than 114 control objectives and recommended control measures, not least the restriction and control of access to systems, applications and information (A.11.2, A.11.6).[xvii] These are reflected in ENISA's own guidance as the security objectives of access control (SO 10), security of data at rest, interface security, and software security (SO 23-25).

Central to good information security practice is the process of risk assessment, as highlighted in ISO27001, the OECD's Guidelines for the Security of Information Systems and Networks,[xviii] and ENISA's guidance for digital service providers: "DSPs wishing to establish, implement, operate, monitor and continuously maintain and improve an appropriate level of security, must also carefully and continuously consider and assess the actual level of preparedness and the related security risks they face" (p.12). Absent any public information to the contrary, it would appear that a risk assessment has not been conducted on the potential impact of the DMA on network and information security within – and indeed outside – the EU.

The European Commission's *Communication on a European strategy for data* (COM(2020) 66 final) recognises both the risk attached to unfettered data sharing with providers in some third countries and the need to balance rights and imperatives. Noting that, "service providers operating in the EU may also be subject to legislation of third countries, which presents the risk that data of EU citizens and businesses are accessed by third country jurisdictions that are in contradiction with the EU's data protection framework. In particular, concerns have been voiced about several Chinese laws related to cybersecurity and national intelligence," the Commission foresees that "the new data paradigm where less data will be stored in data centres, and more data will be spread in a pervasive way closer to the user 'at the edge', brings new challenges for cybersecurity. It will be essential to preserve data security when data are being exchanged. Ensuring the continuity of access controls (i.e. how security attributes of data are managed and respected) across data value chains will be a key, but demanding, pre-requisite to foster data sharing and ensure trust among the different actors of European data ecosystems."

These concerns are barely reflected in the current draft of the DMA. Where cybersecurity is mentioned, the onus is placed on gatekeepers to comply with *all relevant legislation*, rather than on ensuring the practical compatibility of instruments (Article 7):

> The measures implemented by the gatekeeper to ensure compliance with the obligations laid down in Articles 5 and 6 shall be effective in achieving the objective of the relevant obligation. The gatekeeper shall ensure that these measures are implemented in compliance with Regulation (EU) 2016/679 and Directive 2002/58/EC, and with legislation on cyber security, consumer protection and product safety.

It is nevertheless possible to some degree to anticipate conflicts of law, not to mention good practice and international standards stemming from that law, and to work to minimise the detrimental impact of proposed data governance regulation on current and future security efforts. As the European Commission has identified in the above Communication (COM(2020) 66 final), "In order to release Europe's potential we have to find our European way, balancing the flow and wide use of data, while preserving high privacy, security, safety and ethical standards."

Possible steps towards joined up law-making

The question is therefore not one of abandoning efforts to enhance interoperability, portability and contestability, but of understanding whether and how these might be achieved without compromising security. Greater coordination and oversight is one option. Ambassador Wolfgang Ischinger, chairman of the Munich Security Conference, has proposed the appointment of a dedicated EU Chief Security Officer, "an official whose job would be to 'security proof' everything the bloc does. Their one and only task would be to check whether key issues of national and international security have been taken into sufficient account in the formulation, negotiation and, ultimately, implementation of new policies."[xix] On a model not dissimilar to the European Data Protection Supervisor, such an appointment would increase security input to other initiatives within the union. Additional efforts may be required to address the global security dynamics of regional data governance policy.

Recent high-level developments in EU-US relations may yet prove fruitful in coordinating policy imperatives and balancing rights across continents. With the stated support of two European Commission Executive Vice Presidents and three US State Secretaries, the recently agreed EU-US Trade and Technology Council (TTC) will initially comprise ten working groups, with membership drawn from multiple relevant departments, services and agencies on both sides.[xx] Mapping public statements on the remit of each group to policy imperatives, rights, and EU legislative initiatives reveals a number of interconnections:

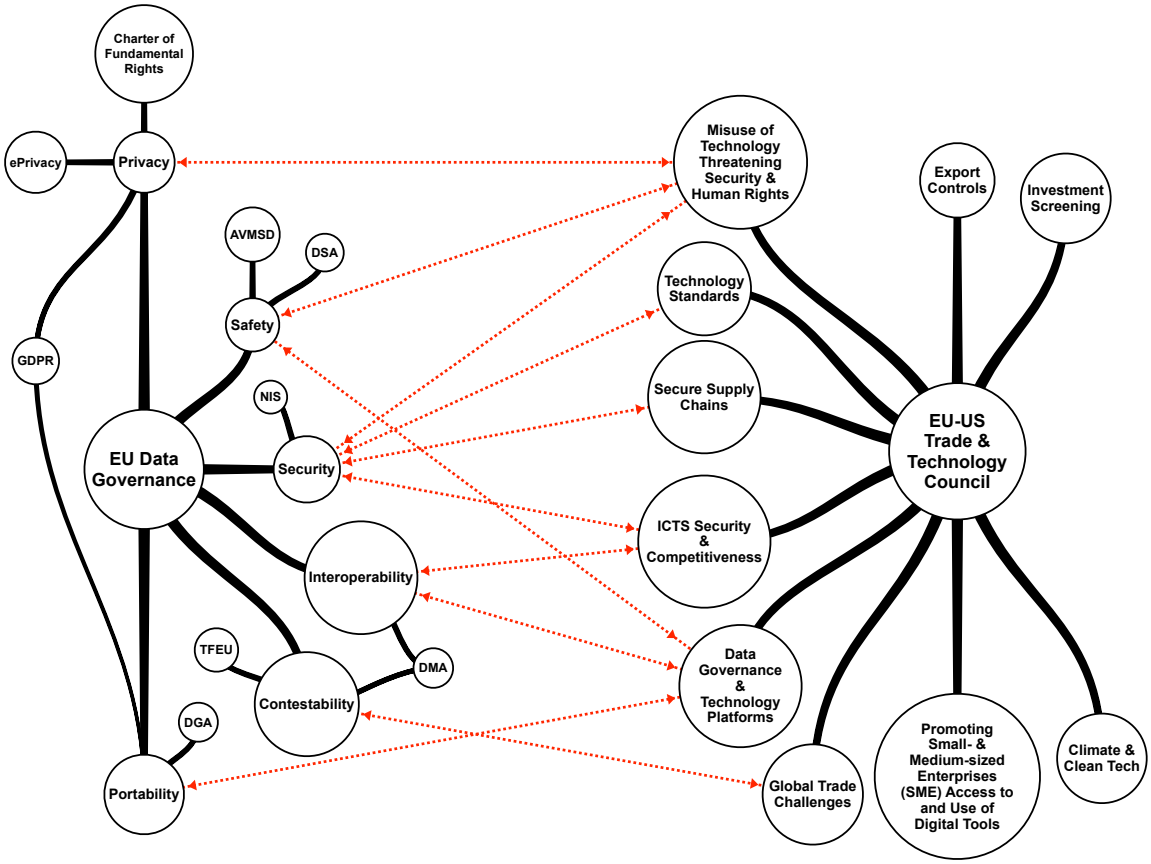

Figure 3: visualisation of data governance imperatives and rights in EU legislation and the EU-US Trade and Technology Council

The above is by no means comprehensive. Rather, it should be seen as an illustration of the multiple points of nexus between EU data governance instruments in train and the interests of the TTC; also of the central role of security in the Council's stated work programme. While the long-term impact of the TTC remains to be seen, the above review of documented tensions between privacy, security and public safety, and of potential issues for security operations in the proposed Digital Markets Act, raises a number of questions suitable for consideration by an inter-continental forum, among them:

- How can the sometimes competing rights to privacy, protection of personal data, consumer protection and security be balanced to the benefit of consumers and businesses?
- Is there more that can be done to harness the security community to risk assess the potential impact of legislation aimed at greater data openness, including the DMA, according to information security good practice?
- Can greater information exchange and coordination between different interest groups assist in anticipating potential conflicts of law and reduce the incidence of unintended consequences?

With involvement from a broad range of stakeholders, the TTC may be well placed to address these crucial considerations. Equally, it would seem to the benefit of all concerned for the security community to claim its seat at the table.

---

[i] Funding support for this study was provided by Google Ireland Ltd. Study design, data collection, analysis and interpretation of data, and reporting and publication of findings are the work of the author alone.

[ii] See, for example, Marc van Lieshout, Michael Friedewald, David Wright & Serge Gutwirth (2013) Reconciling privacy and security, Innovation: The European Journal of Social Science Research, 26:1-2, 119-132, DOI: 10.1080/13511610.2013.723378; also *Surveillance, Privacy and Security: Citizens' Perspectives,* eds. Michael Friedewald, J. Peter Burgess, Johann Čas, Rocco Bellanova, and Walter Peissl. 2017. Routledge.

[iii] https://www.facebook.com/notes/10158831972932929/

[iv] https://www.missingkids.org/gethelpnow/cybertipline

[v] https://www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety

[vi] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0003(COD)&l=en

[vii] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/0359(COD)&l=en

[viii] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

[ix] See, for example, Taylor, DCPJ, Mwiki, H, Dehghantanha, A, Akibini, A, Choo, KKR, Hammoudeh, M and Parizi, R (2019) Forensic investigation of cross platform massively multiplayer online games: Minecraft as a case study. *Science and Justice*; also Warren Pearce, Suay M. Özkula, Amanda K. Greene, Lauren Teeling, Jennifer S. Bansard, Janna Joceli Omena & Elaine Teixeira Rabello (2020) Visual cross-platform analysis: digital methods to research social media images, *Information, Communication & Society*, 23:2, 161-180.

[x] https://www.justice.gov/usao-sdin/pr/child-predator-and-cyberterrorist-buster-hernandez-aka-briankil-sentenced-75-years

[xi] https://www.justice.gov/usao-sdin/press-release/file/1375976/download

[xii] See, for example, the consultation contribution of AmCham EU: "It may also be that in certain circumstances a specific obligation which could create an overall efficiency loss if implemented should not apply because it is not applicable to a specific service; is technically impossible or difficult to implement (e.g. because it may undermine the functioning or integrity of a service or undermine cybersecurity or fraud prevention measures); or is contrary to other legislative requirements" (p.5). Also David Teece's and Henry Kahwaty's analysis for the BRG Institute, *Is the Proposed Digital Markets Act the Cure for Europe's Platform Ills? Evidence from the European Commission's Impact Assessment*: P.37 "For example, Article 6(f)…may require the gatekeeper to complete a substantial re-architecture of its underlying services. Such a reengineering may also impair efficient operations thereafter. In the ancillary service example, in addition to cost, operational impairment may have both performance and security aspects (both on the device and in the cloud)."

[xiii] https://www.ccianet.org/wp-content/uploads/2021/09/CCIA-KS-NatSec-White-Paper.pdf

[xiv] https://www.un.org/disarmament/open-ended-working-group/

[xv] Amendment 1803: https://www.europarl.europa.eu/doceo/document/IMCO-AM-695161_EN.pdf

[xvi] Amendments 1806, 1809 & 1810: https://www.europarl.europa.eu/doceo/document/IMCO-AM-695161_EN.pdf
[xvii] https://www.iso.org/isoiec-27001-information-security.html
[xviii] https://www.oecd.org/sti/ieconomy/15582260.pdf
[xix] https://www.politico.eu/article/security-proof-eu-future/
[xx] https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_4951