POLYCENTRIC REGULATORY MODELS FOR THE SAFEGUARDING OF PERSONAL DATA PRIVACY AND IP IN CYBER INFORMATION SHARING PLATFORMS

Ostrom Workshop Colloquium Series
Deborah Housen-Couriel
November 16, 2020

[Initial draft for comment and discussion – please see questions at p. 21]

Abstract: The increasing costs of hostile cyber events are a critical global issue, estimated in billions of dollars annually. Malicious cyber actors act from various motives - financial, political, military, and social - but they share the attacker's advantage of only needing to succeed once in exploiting their target's vulnerabilities, whereas defenders need to maintain robust levels of cybersecurity. Information sharing (IS) among trusted stakeholders addresses this informational asymmetry, and the advantages of a polycentric approach to cyber IS are clear: a diversity of trusted stakeholders sharing a broad spectrum of threat data and mitigation strategies can significantly boost sharers' cybersecurity. This research paper focuses on the advantages of cyber IS and its present challenges. It explores the regulatory means to best incentivize IS that includes sensitive data, in light of rapidly evolving personal data privacy regulations and IP safeguards. The recent "Schrems II" decision of the CJEU serves as a case study of these challenges.

Contents

1. INTRODUCTION

The sharing of information about cyber risks, vulnerabilities, and threats; and for mitigating all of these both tactically and strategically, has been established as a critical tool for boosting cybersecurity. If implemented optimally, information sharing accomplishes this common goal by establishing a trusted platform for interactions among vetted stakeholders who bring value to one another in the context of defending against malicious cyber actors.[1] Such malicious actors may target organizations from various motives - financial, political, military, and social - but they share the attacker's advantage of only needing to succeed once in exploiting their target's vulnerabilities; whereas defenders need to maintain robust levels of cybersecurity.

Information sharing (IS) among trusted stakeholders addresses this informational asymmetry, and the potential advantages of a polycentric approach to cyber IS in this context are clear: a diversity of trusted stakeholders sharing a broad spectrum of threat data and mitigation strategies can significantly boost sharers' cybersecurity by expanding situational awareness for sharers and equipping them with an array of tactical and strategic defenses against malicious cyber activity.

In this paper we discuss information sharing specifically in a legal and regulatory context, based on a dual analysis of (a) the challenges of incentivizing stakeholders to share relevant cyber data with one another in a timely and usable manner, and (b) measures to ensure the substantive rights protection of two specific types of shared data, private personal data and corporate intellectual property. We argue that a polycentric regulatory model for information sharing – within which a diversity of sharers act to address the common problem of cybersecurity – is optimal for such rights protection. Yet regulators have long struggled with the appropriate incentivization of information sharing, both within national/domestic legal systems and at the multilateral/international level – at both the operational and substantive levels.

The article is structured as follows. A working definition of information sharing, its advantages, and some of its operational aspects is introduced in the next section, Part 2. In Part 3 we examine the regulatory incentivization of IS, explore the inclusion by regulators of substantive rights protections for IS of sensitive data, present the case study of the European Union's Court of Justice ruling on Schrems II in July 2020, and briefly examine the benefits of polycentricity for IS. Part 4 presents three regulatory dilemmas for discussion: (a) whether to require IS as a statutory obligation, or to offer it as a voluntary

[1] The 2016 NIST Guide to Cyber Threat Information Sharing has noted the advantages of IS measures as a means of leveraging the collective knowledge, experience, and capabilities of both state and non-state actors within the sharing community, in order to enhance the capability of each to make informed decisions regarding development of policies, defensive capabilities, threat detection techniques, and mitigation strategies (CHRIS JOHNSON ET AL., NAT'L INST. OF STANDARDS & TECH. (NIST) SPECIAL PUB. 800-150, GUIDE TO CYBER INFORMATION THREAT SHARING, at iii (2016) (herein - NIST).

measure; (b) whether sectoral IS constitutes a more robust basis for IS than generic IS; and (c) the impact of increased automation of IS on its regulation. In Part 5 we conclude with some observations and issues for further study on the benefits of adopting a polycentric regulatory approach to cyber information sharing. These issues include the advantages of polycentricity as an element of regulatory oversight for substantive rights protections; quantifying IS success; and the need to gain insights from information sharing in regulatory frameworks for collective action problems other than cybersecurity (public health, environmental quality, the elimination of debris in outer space).

2. DEFINING INFORMATION SHARING AS A MEASURE FOR REDUCING INFORMATIONAL ASSYMMETRY TO BOOST CYBERSECURITY

2.1 Defining information sharing

Information sharing is a measure for inter-organizational, inter-sectoral and inter-governmental exchange of data that is deemed by sharers to be relevant to the resolution of a common challenge, by definition a collective action problem. In the present analysis, this problem is the maintenance of a robust level of cybersecurity for the sharing community.[2] IS for bolstering cybersecurity may be defined as the agreed-upon exchange of an array of cybersecurity-related information such as risks, vulnerabilities, threats and internal security issues (which may be characterized as *tactical IS*); as well as best practices, standards, intelligence, and business continuity planning (which may be characterized as *strategic IS*).[3] In the 2016 *Guide to Cyber Threat Information Sharing* published by the US National Institute of Standards and Technology (NIST),[4] the advantages of IS measures for improving cybersecurity are described as follows:

> By exchanging cyber threat information within a sharing community, organizations can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face. Using this knowledge, an organization can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies. By correlating and analyzing cyber threat information from

[2] "Cybersecurity" is a term describing the array of actions and activities employed by organizations to mitigate threats and vulnerabilities in cyberspace. The term does not describe a static condition, but rather the ongoing process of applying a "range of actions for the prevention, mitigation, investigation and handling of cyber threats and incidents, and for the reduction of their effects and of the damage caused by them prior, during and after their occurrence." (Israeli Government Resolution No. 2444, Advancing the National Preparedness for Cyber Security, Feb. 15, 2015 (Isr.)).

[3] See the information sharing standard developed by the International Standards Organization, INT'L ORG. FOR STANDARDIZATION, ISO/IEC 27010:2015, INFORMATION TECHNOLOGY—SECURITY TECHNIQUES—INFORMATION SECURITY MANAGEMENT FOR INTER-SECTOR AND INTER-ORGANIZATIONAL COMMUNICATIONS (2015), https://www.iso.org/standard/44375.html..

[4] NIST, *supra* note 1 at ii.

> multiple sources, an organization can also enrich existing information and make it more actionable.[5]

Although not the sole means of closing organizational gaps in cybersecurity, nor by any means a blanket remedy, IS serves as a key measure for bolstering organizational, sectoral, national and, ultimately, global cybersecurity by mitigating cyber threats and events. Information sharing is presently included in many instances of national law and policy as a recommended best practice, or (more rarely) as a measure required by regulators; as well as a confidence building measure in tens of multilateral and bilateral instruments promoting the governance of cyberspace.[6] Elsewhere, we have analyzed the benefits of the regulatory application of IS in the frameworks of both domestic law and the multi-stakeholder / international law context.[7]

IS thus provides participating actors with relevant information, both tactical and strategic, for the reduction of cyber risk that they would not have been able to receive on their own, leveraging interdependencies.[8] This risk mitigation through IS takes place in three chief ways: (a) by reducing information asymmetries between hostile actors and targeted organizations, (b) by producing over time, and assuming effective operations, a "trust externality" among vetted stakeholders in the IS platform; and (c) by enabling stakeholders to opt into engagement in joint collective action against cyber threats, as an outcome of the first two elements. Examples of these types of risk mitigation include global responses to the May 2017 WannaCry ransomware attack[9] and the January 2020 alert on vulnerabilities in Microsoft Windows operating systems discussed in Part 2.3 below.

Despite these positive attributes and growing evidence of the effectiveness of information sharing in boosting cybersecurity for sharing entities, regulators struggle with the appropriate modalities for incentivizing and optimizing its use. Presently, most domestic

[5] NIST, *supra* note 1at iii (emphasis added).

[6] Deborah Housen-Couriel, *An Analytical Review of and Comparison of Operative Measures included in Cyber Diplomatic Initiatives*, BRIEFINGS FROM THE RESEARCH ADVISORY GROUP, Issue Brief No. 1, Global Commission on the Security of Cyberspace, November 2017, 46-84. Three examples are the OSCE's Confidence-Building Measures for Cyberspace (echoed in the Paris Call); the EU's Network and Information Security Directive (art.'s 2,5,11); and the Shanghai Cooperation Organization's International Code of Conduct for Information Security (2015 version, art. 10).

[7] "Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace", in Shackelford et al (eds), Cyber Peace [ref TBA]

[8] See, for example, the 2017 takedown of Andromeda malware through cooperation between the FBI, Europol's European Cybercrime Centre (EC3), the Luneburg Central Criminal Investigation Inspectorate in Germany, and private-sector partners (Europol Press Release, *Andromeda botnet dismantled in international cyber operation*, 4 December 2017, https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation).

[9] "WannaCry Ransomware Attack and International Information Sharing", Billington CyberSecurity Blog (no date), https://billingtoncybersecurity.com/wannacry-ransomware-attack-international-information-sharing/.

law information sharing platforms are voluntary, with government regulators largely refraining from requiring participation by organizations and private sector, sectoral-based platforms only able to offer IS as a benefit to membership in platforms such as the Information Sharing and Analysis Organizations (ISAO's) established under the US Department of Homeland Security,[10] the sectoral Information Sharing and Analysis Centers, [11] and sector-specific platforms such as Israel's Cyber and Finance Continuity Center, which is supported and maintained by the Ministry of Finance and the Cyber Directorate.[12] Interesting exceptions to governmental regulatory restraint can be found in the growing trend of regulatory requirement of IS imposed upon operators of critical infrastructure and governmental contractors, such as US Department of Defense suppliers.

As we shall see in Part 3 below, the overall reluctance of regulators to impose IS requirements, and the disincentives for organizations that may prevent full participation in voluntary IS platforms include both *operative* and *normative-substantive* considerations, which will be examined therein.

2.2 Key issues in establishing IS platforms

Several key issues arise when defining the modalities of information sharing for any given IS platform:

- **Agreed thresholds for events, technical specifications data to be shared** - A key element of information sharing is the prior agreement among participants as to the threshold events which will trigger the need to share information, especially for the real-time sharing of vulnerabilities and cyberattacks which may require specific defensive actions. The determination, it should be emphasized, will be a technical one that is based on system protection and incident response, rather than legal or policy considerations.

- **Identity of the sharing entities** – Effective IS platforms create communities of trust, and thus the organizational or personal identity of sharing entities should be

[10] See https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos and the Executive Order encouraging their use: Executive Order -- Promoting Private Sector Cybersecurity Information Sharing, February 13, 2015.

[11] See https://www.nationalisacs.org/member-isacs.

[12] Memorandum from the Finance Cyber and Continuity Centre (FC3) (Sept. 4, 2017), https://docs.google.com/viewer?url=http%3A%2F%2Fwww.export.gov.il%2Ffiles%2Fcyber%2FFC3.PDF%3Fredirect%3Dno. *See* Anat Diamant, Presentation at ISACA/INSS Forum on Supply Chain Security (May 1, 2018); Micha Weis, Presentation at National Fintech Cyber Ecosystem Round Table (Sept. 17, 2017) (notes on file with author); Deborah Housen-Couriel, *Information Sharing for Mitigation of Hostile Activity in Cyberspace (Part 1)*, 4 EUR. CYBERSECURITY J., no. 3, 2018; Deborah Housen-Couriel, *Information Sharing for Mitigation of Hostile Activity in Cyberspace (Part 2)*, 5 EUR. CYBERSECURITY J., no. 1, 2019.

explicit and transparent to participants.[13] Moving from the local to the global, sharing of cybersecurity-relevant data may take place among individuals (cyber analysts), within a corporate sector (financial organizations, public health organizations), between private sector entities and governmental agencies (as in the CISCP example below), among one country's governmental agencies, between states (bilaterally) or among them (multilaterally), and in the framework of international organizations.[14] This list of sharing entities is not exhaustive or closed, and it illustrates, the criticality of a polycentric approach to the governance of cyberspace in general and information sharing in particular, as discussed in Part 3.3 below (see also Figure 1 for a depiction of two possible models for the identity of sharing entities). For purposes of the present analysis, we exclude exchanges with military or other covert state operators due to the lack of transparency of most such arrangements.[15]

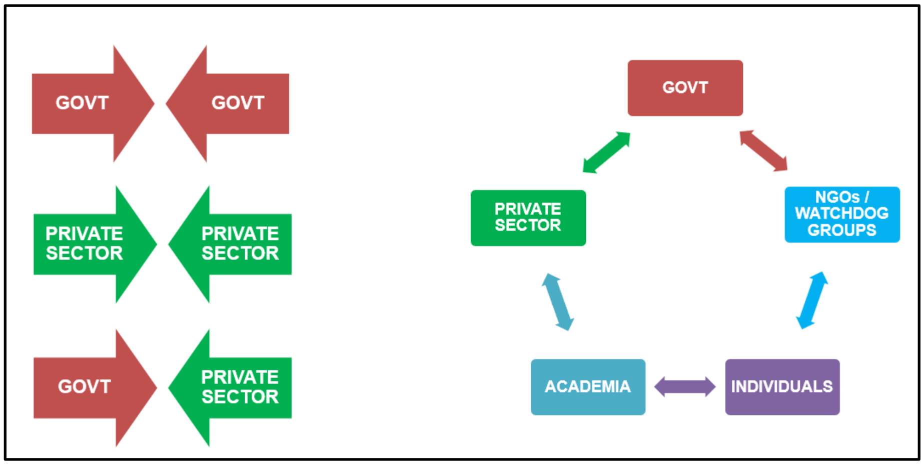


Figure 1: Two models for information sharing among stakeholders, the second conceptualizing a polycentric approach to IS (Source: Author, 2020)

[13] See Ming-Ji James Lin, Shiu-Wan Hung & Chih-Jou Chen, *Fostering the determinants of knowledge sharing in professional virtual communities*, COMPUTERS IN HUMAN BEHAVIOR, 25:4 (2009) 929-939 ("…trust significantly influences knowledge sharing self-efficacy, perceived relative advantage and perceived compatibility, which in turn positively affect knowledge sharing behavior.

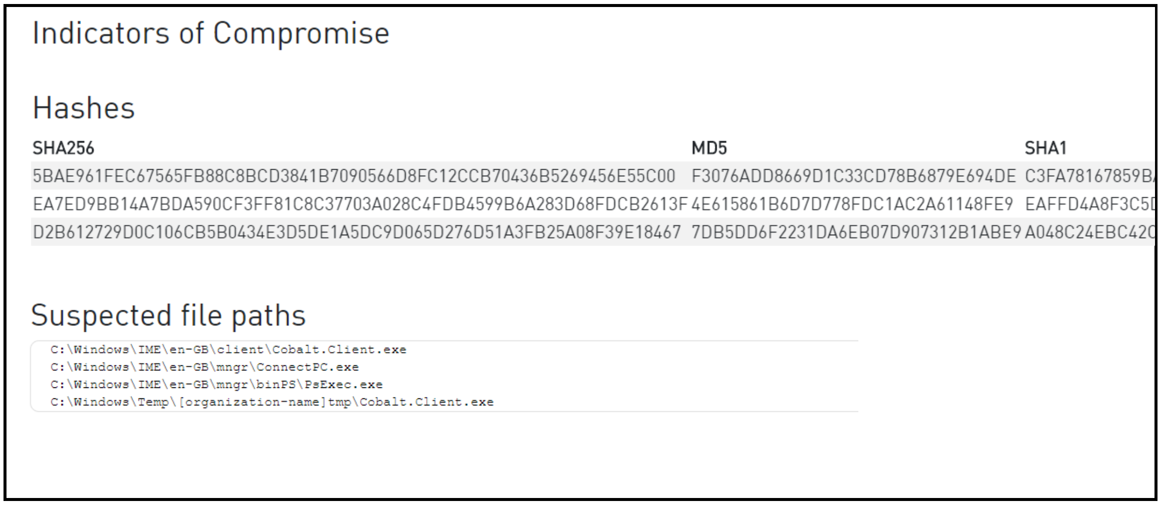
[14] Based on Neil Robinson and Emma Disley, *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*, ENISA, 2010, at. 9. It should also be noted that open-source sharing communities are being established, making threat indicators publicly available. See, for example, Citizen Lab Reports, "Targeted Threats", https://citizenlab.ca/category/research/targeted-threats/. There are also many examples of analyst reports that are openly shared online. Such publicly available data is definitionally distinct from IS, which relies upon the existence of a constructed community for its effectiveness.

[15] While there are examples of military actors sharing cyber threat data publicly, as in the US Cyber Command's utilization of the VirusTotal platform in September 2019 to share malware samples associated with the North Korean Lazarus Group, such sharing is neither consistent nor transparent, and is thus difficult to analyze conclusively (Shannon Vavra, *CyberCommand's Biggest VirusTotal Upload Looks to Expose North Korean-Connected Malware*, September 8, 2019, https://www.cyberscoop.com/cyber-command-virus-total-north-korean-malware; and Shannon Vavra, *Why did Cyber Command back off its recent plans to call out North Korean hacking?* October 22, 2019, https://www.cyberscoop.com/cyber-command-north-korea-lazarus-group-fastcash/.

- **The types of information shared** – Each IS platform specifies the typologies of relevant information to be shared by participants, often in a Terms of Use or similar document that is often not transparent to non-participants. Current developments are moving towards standardization of relevant threat indicators and automatization of the sharing, towards a "commoditization" of cyber threat data within communities of trust. Such data includes:[16]

    - Automated threat indicators (including “indicators of compromise” or IOCs);
    - Tactics, techniques and procedures (TTPs);
    - Real-time security alerts;
    - Threat intelligence reports;
    - Tool configurations to support automated IOC application;
    - Recommendations for mitigation of threats;
    - Best practices for tactical and strategic cybersecurity measures;
    - Strategic evaluations of trends in cybersecurity overall.[17]

Figure 2 shows an example of such real-time security data, in this case IOCs and suspected malware file paths, relevant to the Pay2Key ransomware that attacked private companies in mid-November 2020.[18] The malware spread throughout corporate networks in under an hour, making rapid response critical.



Indicators of Compromise

Hashes

SHA256	MD5	SHA1
5BAE961FEC67565FB88C8BCD3841B7090566D8FC12CCB70436B5269456E55C00	F3076ADD8669D1C33CD78B6879E694DE	C3FA78167859B
EA7ED9BB14A7BDA590CF3FF81C8C37703A028C4FDB4599B6A283D68FDCB2613F	4E615861B6D7D778FDC1AC2A61148FE9	EAFFD4A8F3C5
D2B612729D0C106CB5B0434E3D5DE1A5DC9D065D276D51A3FB25A08F39E18467	7DB5DD6F2231DA6EB07D907312B1ABE9	A048C24EBC42

Suspected file paths

```
C:\Windows\IME\en-GB\client\Cobalt.Client.exe
C:\Windows\IME\en-GB\mngr\ConnectPC.exe
C:\Windows\IME\en-GB\mngr\binPS\PsExec.exe
C:\Windows\Temp\[organization-name]tmp\Cobalt.Client.exe
```

Figure 2: Indicators of compromise and suspected file paths of the Pay2Key ransomware (Source: Checkpoint, November 6, 2020, https://research.checkpoint.com/2020/ransomware-alert-pay2key/)

[16] NIST, *supra* note 1, at pp. 2-3.

[17] See CISA, *Building A More Resilient ICT Supply Chain: Lessons Learned During The COVID-19 Pandemic*, November 2020, https://www.cisa.gov/publication/ict-supply-chain-lessons-learned-covid-19.

[18] Checkpoint,“Pay2Key-The Plot Thickens”, November 12, 2020, research.checkpoint.com/2020/pay2key-the-plot-thickens/.

Beyond these key issues, IS must develop in concert with the changing cyber threat landscape in order to retain its relevance and credibility for participants. Ongoing technological improvements to IS platforms that ease their use, allow for a diverse array of sharers, and prove their value in boosting cybersecurity for all participants will ultimately reduce the informational asymmetries that so deeply characterize the vulnerability of targets of hostile cyber actors at present. The next section describes one example of an IS platform that is currently working to leverage such ongoing developments.

2.3 Information sharing among governmental and private sector organizations: the DHS' Cyber Information Sharing and Collaboration Program

Background to the CISCP

The example used here to illustrate some of the operational aspects of how IS works is that of the Cyber Information Sharing and Collaboration Program (CISCP) platform supported by the US Department of Homeland Security and Department of Justice. Originally established as a platform for the benefit of critical infrastructure operators,[19] the CISCP is a generic, voluntary, free-of-charge IS platform, open to public and private sector organizations that are based in the U.S. and abroad.[20] The platform specifically includes the sector-based Information Sharing and Analysis Centers and Organizations (ISACs and ISAOs), non-profit entities originally established pursuant to Presidential Decision Directive-63 of May 1998 and referred to above.[21] Sectors utilizing ISACs and ISAOs presently include aviation communications, electricity, financial services, health, information technology, and maritime activities.[22]

CISCP aims "to build cybersecurity resiliency and to harden the defenses of the United States and its strategic partners",[23] by including operators of critical infrastructures and other private and governmental organizations into one information sharing platform on a voluntary basis. Prospective participants sign on to an agreement establishing the modalities of the exchange of anonymized cybersecurity information, and ensuring protection from legal liability that may ensue from the sharing of protected information such as personal data, information subject to sunshine laws, and some proprietary data.[24]

[19] For a review of the legal basis of critical infrastructure information sharing in the U.S., see Sean Gallagher and Michael Neugebauer, *Critical Infrastructure Information Sharing*, IEEE International Conference on Technologies for Homeland Security, 2004.

[20] Information Sharing and Analysis Centers (IASCs) and Information Sharing and Analysis Organizations (ISAOs) are sectoral groupings of information sharing organizations. *See* ENISA, Cooperative Models for Information Sharing and Analysis Centers (ISACs), 2017, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.

[21] Presidential Decision Directive-63 (PDD-63), May 22, 1998, https://fas.org/irp/offdocs/pdd/pdd-63.htm. *See esp.* the section on "Warning and information Centers".

[22] See the full listing at https://www.nationalisacs.org/member-isacs.

[23] Cyber Information Sharing and Collaboration Program [CISCP], https://www.cisa.gov/ciscp.

[24] Cyber Information Sharing and Collaboration Agreement (CISCA). The text of the agreement is currently being revised (email in author's possession of April 7, 2020 from the Cybersecurity and Infrastructure Security Agency. The analysis of sharer's legal exposures and liabilities is beyond the present

Upon completion of an onboarding training session, participating organizations may take advantage of two types of CISCP activities. The first type is ongoing cyber threat information that is made available from CISCP to participants through indicator bulletins, analysis reports, and malware reports. Two examples are the Weekly Bulletin, summarizing new vulnerabilities according to NIST's National Vulnerability Database classification system;[25] and a Joint Alert issued in early April 2020, together with the UK NCSC, on the exploitation of COVID-19 by malicious cyber actors.[26] The second type of information that is shared is real-time data about emerging cyber threats and attacks, characterized by mutual sharing of actionable data that includes warnings, vulnerabilities, indicators of compromise, and measures for resolving them.

The January 2020 alert on a Microsoft Windows system vulnerability

An example of real-time cyber threat IS by the CISCP is the January 2020 alert regarding serious vulnerabilities in Microsoft Windows operating systems, designated CVE 2020-0601 (also, less officially, "Curveball" and "Chain of Fools").[27] The alert warned of a spoofing vulnerability in the way that Windows validates a certain type of encrypted certificate: an attacker could exploit this vulnerability to obtain sensitive information, such as financial data, by impersonating a user's bank website; or to install malware on a targeted system. The exploit could have permitted man-in-the-middle attacks and realistic-looking phishing websites. The shared Microsoft Security Advisory addressed CVE 2020-0601 by ensuring that the relevant encrypted certificates were completely validated, and the simultaneously-released National Security Agency advisory provided relevant detection measures for targeted organizations (although remediation measures are not necessarily shared together with vulnerability disclosures).[28] As a result of this IS, the Windows vulnerability could be quickly addressed by those affected.[29] Analysts have noted that CVE 2020-0601 was especially effective in resolving a "dangerous zero-day vulnerability" because of the pro-active disclosure made by the NSA to Microsoft, then allowing the vulnerability and patch to be rapidly shared at “machine speed” through the CISCP’s

scope, but see The Department of Homeland Security and the Department of Justice, Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015, June 15, 2016, 12-18 and the tables at 19-20 and Annex 1. The liability protections apply, *inter alia*, to the sharing of private personal data, some proprietary data certain governmental uses of data, and in the context of antitrust regulation.

[25] See, for example, Bulletin SB-20-097, March 30, 2020, https://www.us-cert.gov/ncas/bulletins/sb20-097.

[26] Alert (AA20-009A): Covid-19 Exploited by Malicious Cyber Actors, April 8, 2020, https://www.us-cert.gov/ncas/alerts/aa20-099a.

[27] Chester Wisniewski, *Looking for Silver Linings in the CVE 2020-0601 Crypto Vulnerability*, Naked Security, 23 January 2020, https://nakedsecurity.sophos.com/2020/01/23/looking-for-silver-linings-in-the-cve-2020-0601-crypto-vulnerability/.

[28] Alert (AA20-014A), *Critical Vulnerabilities in Microsoft Windows Operating System*, January 14, 2020, https://www.us-cert.gov/ncas/alerts/aa20-014a.

[29] See the Israeli CERT notification of January 14, 2020, *Urgent Warning: Vulnerabilities in Windows Operating System 2019*, (Hebrew), https://www.gov.il/BlobFolder/reports/microsoft-update-jan2020/he/MICROSOFTJAN20-CERT-IL-W-1021.pdf .

automated indicator sharing capability.[30] The CVE 2020-0601 cyber event thus showed the importance of IS among a diversity of actors, including national security agencies and private companies.[31]

The standardization of information sharing on the CISCP and additional platforms
Such information sharing on cyber threats and vulnerabilities of all types that passes through the CISCP platform requires technological measures to safeguard IS at three levels: (a) the provision of data by the sharing organization, which is often sensitive and the source of which may be anonymized; (b) its transmission; and (c) its processing, distribution, and storage on the IS platform. To that end, CISCP utilizes standardized reporting forms for provision of cyber threat indicators,[32] the specialized STIX and TAXII indicator architectures[33] that also enable automated information sharing (AIS),[34] and the standard Traffic Light Protocol (TLP), which classifies the security levels of the shared data using four colors in order to indicate the rules for sharing perimeters (see Figure 3 below). TLP requires that prior and explicit permission be obtained from the source of the data, should a recipient need to share the information more widely than indicated.

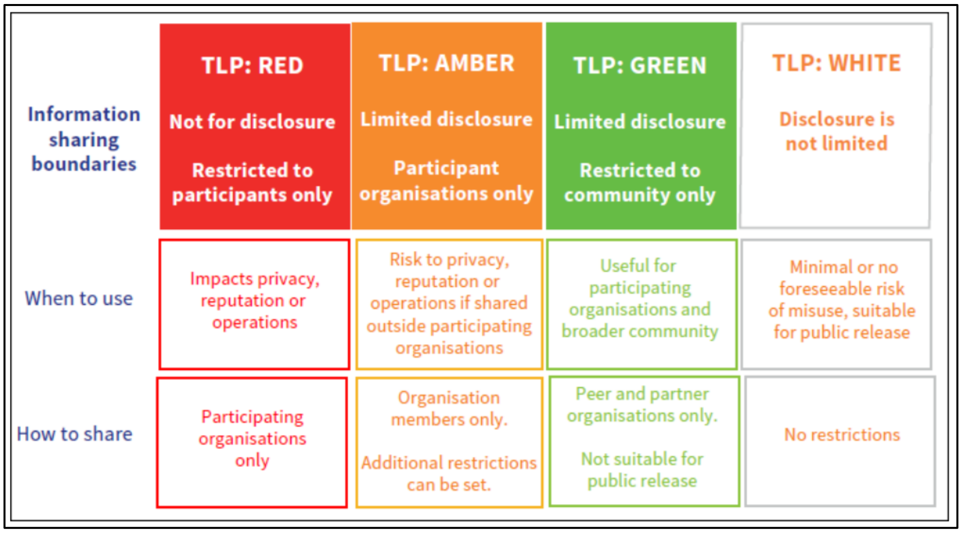
[30] Wisniewski, *supra* note 27.

[31] Bruce Schneier commended the NSA for its information sharing. He wrote: "[Cybersecurity Directorate head Anne Neuberger] said that this is not the first time the NSA sent Microsoft a vulnerability to fix, but it was the first time it has publicly taken credit for the discovery. The reason is that the NSA is trying to rebuild trust with the security community, and this disclosure is a result of its new initiative to share findings more quickly and more often. Barring any other information, I would take the NSA at its word here. So, good for it."(Schneier on Security, *Critical Windows Vulnerability Discovered by NSA*, January 15, 2020, https://www.schneier.com/blog/archives/2020/01/critical_window.html).

[32] *See* CISA Incident Reporting System, https://www.us-cert.gov/forms/report and US-CERT DHS Cyber Threat Indicator and Defensive Measure Submission System, https://www.us-cert.gov/forms/share-indicators.

[33] "STIX is a language being developed in collaboration with all interested parties for the specification, capture, characterization and communication of standardized cyber threat information. It does so in a structured fashion to support more effective cyber threat management processes and application of automation."(Sean Barnum, STANDARDIZING CYBER THREAT INTELLIGENCE INFORMATION WITH THE STRUCTURED THREAT INFORMATION EXPRESSION (STIX™) (2014), at 7, http://stixproject.github.io/about/STIX_Whitepaper_v1.1.pdf.). See also Koen Van Impe, *How STIX, TAXII and CyBox Can Help with Standardizing Threat Information*, SECURITY INTELLIGENCE (Mar. 26, 2015), https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-with-standardizing-threat-information/.

[34] See *Automated Indicator Sharing (AIS)*, https://www.us-cert.gov/ais. Participants must sign on to terms of use document that specifies modalities (U.S. Department of Homeland Security Automated Indicator Sharing Terms of Use, https://www.us-cert.gov/sites/default/files/ais_files/AIS_Terms_of_Use.pdf.



	TLP: RED	TLP: AMBER	TLP: GREEN	TLP: WHITE
Information sharing boundaries	Not for disclosure Restricted to participants only	Limited disclosure Participant organisations only	Limited disclosure Restricted to community only	Disclosure is not limited
When to use	Impacts privacy, reputation or operations	Risk to privacy, reputation or operations if shared outside participating organisations	Useful for participating organisations and broader community	Minimal or no foreseeable risk of misuse, suitable for public release
How to share	Participating organisations only	Organisation members only. Additional restrictions can be set.	Peer and partner organisations only. Not suitable for public release	No restrictions

*Figure 3: Traffic Light Protocol (Source:*Australian Access Federation, October 2020).

The DHS' CISCP platform is one example of government-supported information sharing to bolster cybersecurity. 'There are many additional examples of IS platforms utilizing similar, standardized systems for threat indicator transmission, including both governmental and private sector platform operators, including NATO;[35] The EU's CSIRT network established under the 2016 Network and Information Security Directive;[36] the Cyber Threat Alliance;[37] Israel's "Showcase" (*Chalon Raávah*)[38] and Cyber and Finance Continuity Center;[39] the Cyber Security Information Sharing Partnership (CiSP) of the UK National Cyber Security Center;[40] and the "Informationspool" platform supported by

[35] Sander Oudkerk and Koknrda Wrona, *Using NATO Labelling to Support Controlled Information Sharing between Partners* in Eric Luiijf and Pieter Hartel (eds) CRITICAL INFORMATION INFRASTRUCTURES SECURITY, LECTURE NOTES IN COMPUTER SCIENCE, vol 8328 (2013).

[36] Directive 2016/1148, of the European Parliament and of the Council of 6 July 2016 concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. (L194) 1 [hereinafter EU NIS]. The relevant NIS Annex, entitled "Requirements and Tasks of CSIRTs", stipulates their monitoring of risks and incidents; the provision of alerts and other operative indicators to stakeholders; as well as support for incident response.

[37] The CTA is a non-profit IS organization founded by private companies (www.cyberthreatalliance.org). See *Cyber Threat Alliance Expands Mission through Appointment of President, Formal Incorporation as Not-for-Profit and New Founding Members,* https://www.fortinet.com/ru/corporate/about-us/newsroom/press-releases/2017/cyber-threat-alliance-expands-mission.html.

[38] Israel Cyber Directorate, Israel's 'Showcase' for Evaluation of Cyber Risks" (in Hebrew), https://www.gov.il/he/departments/general/systemfororg.

[39] Israel's FC3 is supported and maintained by the Ministry of Finance and the Cyber Directorate, Memorandum from the Finance Cyber and Continuity Centre (FC3) (Sept. 4, 2017), https://docs.google.com/viewer?url=http%3A%2F%2Fwww.export.gov.il%2Ffiles%2Fcyber%2FFC3.PDF%3Fredirect%3Dno. *See* Housen-Couriel, *supra* note 12.

[40] See the CiSP Terms and Conditions, v.5 [no date], https://www.ncsc.gov.uk/files/UK%20CISP%20Terms%20and%20Conditions%20v5.0.pdf.

Germany's Department for Information Sharing (Bundesamt für Sicherheit in der Informationstechnik, BSI) through its "cyber alliance" (Allianz für Cyber-Sicherheit).[41]

In addition to these IS platforms which foster IS among governmental, corporate, and some other institutional actors in cyberspace[42] for a broad range of cyber threats and risks, several specialized IS platforms focus on a narrower risk typology that pinpoints cybercrime and terrorist activity on the internet. Examples include INTERPOL's Cybercrime and Cyber-terrorism Fusion Centres;[43] EUROPOL's European Cybercrime Centre (EC3);[44] and the Hash Sharing Consortium established in the framework of the Global Internet Forum to Counter Terrorism (GIFCT) founded in 2016 by Facebook, Google, YouTube, Twitter and to share information on extremist and terrorist content online.[45]

These and other such IS platforms reflect organizational and regional differences in the modes of gathering and processing cyber threat indicators and other operational data. Nevertheless, they all rely on standardized and vetted protocols that promote trust among sharing entities.[46] These protocols are increasingly automated, supporting more rapid distribution of key cybersecurity indicators among sharers.

3. THE REGULATORY CHALLENGE: INCENTIVIZATION AND SELECTED DILEMMAS

3.1 The regulatory challenge of IS: operational and substantive disincentives

As noted above, information sharing is in its essence an exercise in trust-building to achieve the common aim of an optimal level of ongoing cybersecurity for the sharing entities. Regulators at both the national and international levels are challenged by the need to incentivize IS and optimize participation. It is rare that governmental regulators establish statutory requirements for information sharing, and these are usually restricted to sharing among governmental entities themselves, certain critical infrastructure operators, and

[41] See the description of the "Informationspool", https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/_function/Informationspool_Formular.html;jsessionid=44A7CF329463873BACD747ABEBA5CB17.1_cid351?nn=6643342 (unofficial translation).

[42] See *supra* for the discussion of the identity of participants in IS platforms.

[43] "The Cyber Fusion Centre (CFC) brings together cyber experts from law enforcement and industry to gather and analyse all available information on criminal activities in cyberspace to provide countries with coherent, usable intelligence which can be transformed into operational action to both prevent crime and aid in the identification of criminals."(INTERPOL, Cybercrime, https://www.interpol.int/content/download/5267/file/Cybercrime.pdf).

[44] EC3-European Cyber Crime Centre, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

[45] GIFCT, Joint Tech Innovation, https://gifct.org/joint-tech-innovation/. See also the materials on cyber counter-terrorism information sharing collected by the International Cyber Terrorism Regulation Project (ICTRP), www.ictrp.org.

[46] For an example of a formal standard on IS, *see* ISO/IEC 27010:2015, *supra* note 3.

governmental suppliers such as US Department of Defense contractors. Private-sector organizations may themselves initiate IS as a voluntary (or self-regulatory) measure for bolstering their own organizational cybersecurity, as well as sectoral cybersecurity – with or without the participation of governmental authorities.[47]

Yet, at present, the incentivization of sector stakeholders for both types of IS platforms – government-mandated and voluntary - is less than optimal for achieving desired levels of cybersecurity It is important to note that IS does not constitute a universally-endorsed measure for boosting cybersecurity and mitigating risk.[48] Despite the advantages that IS can bring, organizations may fail to fully adopt and operationalize IS for reasons that may be characterized as either (a) operative or (b) normative-substantive.
The **operational disincentives** include:

- The *inability to establish trust* among sharing entities, some of whom may be competitors, including the concern regarding free riders (entities who benefit from IS without contributing themselves).

- *Costs* related to IS including recruitment, training and retention of appropriate cybersecurity personnel; and organizational time spent on IS, including time devoted to "false positives" (*i.e.* incorrect alerts that are based on bad information) when IS may be less than optimal;[49]

[47] *See* Sharon Yadin, *Self-Regulation in the Israeli Banking Sector*, 45 RIV'ON LEBANKAUT 19, 19-26 (2010) (Heb.) (discussing types of regulation, including self-regulation, by banks); Richard Borden, Joshua Mooney, Mark Taylor & Matthew Sharkey, *Threat Information Sharing and GDPR*, https://www.fsisac.com/hubfs/5442200/Resources/FS-ISAC_Threat_Information_Sharing_and_GDPR.pdf.

[48] The well-known example of the 2017 breach into the Equifax credit reporting company illustrates the pitfalls that characterize the reluctance of some financial sector actors to engage effectively with IS. *See* ELIZABETH WARREN, BAD CREDIT: UNCOVERING EQUIFAX' FAILURE TO PROTECT AMERICANS' PERSONAL INFORMATION 5 (2018). See also Michèl Fournoy and Michael Sulmeyer, Battlefield Internet: a Plan to Secure Cyberspace, Foreign Affairs, September/October 2018, https://www.foreignaffairs.com/articles/world/2018-08-14/battlefield-internet ("For decades, information sharing has been the clarion call, the idea being that the sooner potential victims are tipped off about impending threats and the sooner actual victims reveal how they have been compromised, the better defended the entire system will be. In practice, however, information sharing has taken hold only in certain sectors—in the United States, mostly among financial institutions and between defense contractors and the military. And these are exceptions: government and corporate cultures still disincentivize acknowledging a breach, which makes it more likely that others will remain vulnerable to attack.").

[49] *See* Benjamin Powell, *Is Cybersecurity a Public Good? Evidence from the Financial Services Industry*, 1 J. L. ECON. & POL'Y 497 (2005). at 507 (noting ongoing, increasing monetary investments in cybersecurity of financial sector actors). For other undesirable market obstacles or inefficiencies that are liable to be introduced by IS, see Eli Dourado & Jeremy Brito, *Is There a Market Failure in Cybersecurity?*, MERCATUS CTR. GEO. MASON U., no. 6, Mar. 6, 2012, https://www.mercatus.org/system/files/Cybersecurity_DouradoBrito_MOP_Final.pdf; Amitai Etzioni, *The Private Sector: A Reluctant Partner in Cybersecurity*, 15 GEO. J. INT'L AFF. 69 (2014); Gordon, Loeb & Lucyshyn, *Sharing Information on Computer Systems Security: An Economic Analysis*, JOURNAL OF ACCOUNTING AND PUBLIC POLICY, 22, 461-485; CYBER THREAT ALLIANCE, *supra* note 47.

- *Lack of transparency regarding the robustness and confidentiality of IS platforms*, including the possible use of shared data by any participating government agencies for non-cybersecurity purposes such as tracking of individuals for immigration control or unauthorized surveillance;[50]

- *Regulatory redundancy*, where other, possibly competing IS formats are mandated and may complicate efficient IS;[51]

Two of the **normative-substantive disincentives** for non-governmental entities (and some governmental entities) to fully adopt and internalize IS are:

- The *potential exposure of protected personal data held by the organization*, including a lack of statutory limitation on the purposes of the government regulator's use of such data; non-transparent sharing via government channels with agencies and actors that have not been vetted by participants;

  The *potential exposure of organizational IP*, with potential chilling effects on organizational innovation; and possible implications for corporate market value.[52]

Taken together, both the operative and substantive-normative disincentives to IS help to explain why some cyberspace actors are reluctant to fully adopt and internalize IS as part of their overall cybersecurity strategies on their own initiative; and may participate less than optimally including in situations where required to do so by regulators.[53] Even when such safeguards are in place, potential exposure of protected data may occur through the "bottoming out" of trusted platforms, as seen in the repeated breaches of the US National Security Agency cyber weapons cache.[54]

[50] *See* NIST, *supra* note 1, at 4–5.

[51] One example can be seen in the United States, where the financial sector is defined as one of the sixteen included under the aegis of DHS and also subject to the directives of the US Department of Treasury. *See* Melissa Knerr, *Password Please: The Effectiveness of New York's First-in-Nation Cybersecurity Regulation of Banks*, 1 Bus. Entrepreneurship & Tax L. Rev. 539 (2017) at 550, 553. *See also* Neil Robinson, *Information Sharing for CIP: Between Policy, Theory, and Practice*, *in* Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection 324 (Christopher Laing, Atta Baadi & Paul Vickers eds., 2013).

[52] The risks associated with IP aspects of cyber threat vectors are growing and becoming more transparent. *See* Riley Walters & Michael Maher, *Why Chinese IP Theft is a Concern for National Security*, Heritage Found. (Apr. 4, 2019), https://www.heritage.org/asia/commentary/why-chinas-intellectual-property-theft-concern-national-security.

[53] David Sutton, *Trusted Information Sharing for Cyber Situational Awareness*, 132 E & I Elektrotechnik und Informationstechnik 113–16 (2015); Paul Barford et al., *Cyber SA: Situational Awareness for Cyber Defense*, *in* Cyber Situational Awareness, Advances in Information Security 3–13 (S. Jajodia et al. eds., 2010).

[54] Swati Khandelwal, *Shadow Brokers Leaks Another Windows Hacking Tool Stolen from NSA's Arsenal*, The Hacker News (Sept. 7, 2017), https://thehackernews.com/2017/09/shadowbrokers-unitedrake-hacking.html.

We focus our analysis here on the first of the substantive-normative disincentives, that of the potential exposure of personal data in the context of information sharing. The case study we will examine is that of the July 2020 ruling of the Court of Justice of the European Union (CJEU) in the case of *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ("Schrems II").[55]

3.2 Substantive rights protections for IS of sensitive data: the case study of the Schrems II ruling of the CJEU

The CJEU ruling

On July 16, 2020, the CJEU handed down its ruling on the Schrems II case, drawing attention among regulators and private companies around the globe for its controversial, immediate annulment of the arrangement between the United States and the European Union for the exchange of personal data – the so-called Privacy Shield framework.[56] The case was brought against Facebook by the Austrian attorney Max Schrems, in his second round of litigation against that company.[57] His personal data, as well as that of many other European users of Facebook, was regularly transferred from Facebook servers in Ireland to that company's servers located in the US, ostensibly protected by Privacy Shield and its safeguards that had been determined as "adequate" by both countries upon its establishment in 2016. Schrems claimed that Facebook's use of his data on its US servers does not offer sufficient protection of his data privacy rights under EU data protection law, and the Court supported his claim.

The CJEU ruling has manifold ramifications for the transfer of personal data by private organizations between these two entities, as well as beyond their bilateral interactions, which are still being clarified at the time of this writing.[58] In the context of information sharing, the legal and regulatory situation has changed radically: governments and private companies may no longer share cybersecurity-relevant information that contains the personal data of EU data subjects, unless certain express conditions for the legality of data transfer are met.[59] Specifically, the Court found that "…the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States… are not circumscribed in a way that satisfies requirements that are essentially

[55] Judgement of the Court, Case C-311/18,16 July 2020, http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=9791227 (herein, "Schrems II Judgement").

[56] See the full description of this arrangement at the Privacy Shield website, https://www.privacyshield.gov/welcome.

[57] Hannah Kuchler, "Max Schrems – the man who took on Facebook - and won", *Financial Times*, April 5, 2018, https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544.

[58] European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 10 November 2020 (version for public consultation).

[59] Schrems II Judgement, *supra* note 55.

equivalent to those required…under EU law."[60] The reference here is to US federal statutes that allow for data surveillance programs such as those based on Section 702 of the FISA and on Executive Order 12333 and which, in the eyes of the Court, are neither proportional to the compromise of data subject rights nor allow a sufficient level of redress for EU data subjects.[61] The Court therefore annulled the Privacy Shield framework that had been in force since July 2016, revoking the recognition by the EU's personal data protection regime that US safeguards of data privacy are adequate for EU data subjects' rights protections.

The global scope of the Schrems II ruling

Moreover, the CJEU emphasized that its ruling is not US-specific. Any jurisdiction to which EU personal data is transferred from any one of the 27 European Union member states must uphold an "adequate" level of data privacy protection – otherwise such transfer is unlawful. Any country that permits access to personal data by public authorities or does not provide sufficient redress for EU data subjects regarding such access will not meet the adequacy test set by the Court in its interpretation of EU data protection law.[62] This global scope of the Schrems II ruling is an outcome of the regulatory reach of the EU's General Data Protection Regulation, or GDPR,[63] which came into force in May 2018 and has garnered global attention for its impact on data protection regimes and corporate activities as they interact with data subjects in every context.[64] Although the present article cannot encompass a full review of the extraterritorial application and implementation of the GDPR, it is important to touch upon several points that are relevant for the information sharing of personal data.

The GDPR governs the processing of "personal data", which is defined broadly to include any piece of information that might reasonably identify a living individual who is a data subject of an EU country. It aims to protecting his or her fundamental rights and freedoms, and in particular the right to protection of personal data, irrespective of the geographical location of the data processing – which means that the GDPR is inherently extra-territorial and extra-jurisdictional in its applicability.[65] Robust enforcement of the GDPR on the part of European regulators both within the EU and outside of their strictly territorial jurisdiction has contributed to the effectiveness, influence and regulatory impact of this regime in initial the two-and-a-half years of its existence.[66]

[60] *Id*., at §185.

[61] *Id*., at §178-184.

[62] *Id*., at §189.

[63] General Data Protection Regulation, https://gdpr-info.eu/.

[64] Colin Bennet, "The European General Data Protection Regulation: An instrument for the globalization of privacy standards?", *Information Polity* 23 (2018), 239-246.

[65] GDPR Article 3.

[66] Benjamin Greze, "The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives", *International Data Privacy Law* 9 (2019) 109-127,

The processing of data under the GDPR, which includes any activity for its gathering, use, transmission and storage), must be carried out by organizations "lawfully, fairly, and in a transparent manner";[67] and the requirement of a "lawful basis" for processing personal data in the context of cyber threat IS means that the sharing and receiving parties must both be able to demonstrate that they have legitimate grounds for use of the data. These grounds are enumerated in Article 6 of the GDPR and include explicit consent of the data subject, performance of a contract, compliance with a legal obligation to which the organization is subject, protection of vital interests of the data subject and a defined public interest. The final legal ground, most relevant to information sharing, is that of legitimate interests of the organization undertaking the data processing: for our purposes – information sharing to bolster cybersecurity. These legitimate interests may serve as a basis for IS, "…except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject".

This is precisely the challenge to IS thrown up by the Schrems II ruling. The CJEU has determined that these fundamental rights and freedoms override any legitimate interests of organizations using the personal data belonging to EU subjects unless those organizations can demonstrate an EU-adequate level of data protection. Information sharing to bolster cybersecurity is undoubtedly a legitimate interest, but Schrems II calls into question the use of personal data by IS platforms – whether its source is the EU or elsewhere.

The use of personal data by cyber information sharing platforms

The types of data that are shared by IS platforms include a wide array of indicators, as reviewed in Part 2 above. A majority of these do not include identifiable personal data, and are more readily characterized as TTPs (tactics, techniques and procedures), IOPs (indicators of compromise) and other technical specifications. Yet there are also instances in which personal data is in fact shared as part of the threat mitigation information: email addresses, IP addresses, names, bank account numbers and credit card information of victims, and sometimes the names of threat actors themselves.[68] Borden, Mooney, Taylor, and Sharkey classify shared personal data into three categories: falsified personal data (when an identity, or a partial identity, is created by a data subject and used to hide his or her identity); stolen or victim personal data (when a third party has stolen the personal data of an actual data subject), and personal data of threat actors (which is the personal data of individuals committing fraud and other cybercrime).[69] They add the following example.

> Sharing certain personal data (such as IP or email addresses) can prove to be "essential" in rapidly identifying and preventing security breaches or the exploitation of discovered vulnerabilities. It also may prevent further crime. For instance, the processing of Threat Actor Personal Data relating to an unsuccessful cyber incident against one [information sharer] can help [others] secure their systems against cyber threats from that same

[67] GDPR Article 5, https://gdpr-info.eu/art-5-gdpr/

[68] Borden, Mooney, Taylor & Sharkey, *supra* note 47 at p. 2

[69] *Id*.

> individual. In addition, sharing Stolen/Victim Personal Data within the member community is the quickest and most efficient and effective way for members to prevent a data subject from being a victim of further fraud or criminal activity. In addition, any attempt to remove personal data from the threat information that is shared, would be disproportionately onerous and would undermine the value and effectiveness of the threat information; thereby debilitating the very purpose of threat sharing and making network security more unfeasible.[70]

Other researchers have noted the difficulty of scrubbing private personal data from real-time cybersecurity alerts when these include mobile phone data such as phone numbers and locations associated with an individual data subject;[71] application-level data that is shared;[72] personal data of contributing sharers;[73] and technical data that may be readily correlated with specific individuals.[74]

Thus, although cyber information platforms may not actively encourage or support the sharing of personal data, it is inevitably an inherent element of the overall information shared. Real-time use of threat information, especially when automated processes are used, may not allow for timely anonymization or restraint on the part of stakeholders.

Ramifications of Schrems II for cyber information sharing

Regulators and practitioners are currently in limbo with respect to the full ramifications of the Schrems II ruling for personal data protection when it is transferred outside of the European Union. At the formal, bilateral level, the EU and the US are attempting to renegotiate Privacy Shield or the framework which will replace it; and the European Data Protection Board has issued guidelines for public input.[75]

With respect to cyber IS platforms' use of personal data, whether intentional or inadvertent, the full ramifications of the Schrems II ruling are still unclear. We propose that the following three paths, although difficult, might allow the continued sharing of cyber threat information in a way that shields organizations from regulatory exposure for violating data protection laws, and specifically the GDPR. The first is a regulatory guideline on the part of the European Data Protection Board for the application of the GDPR that explicitly permits IS of personal information for cybersecurity as "the performance of a task carried out in the public interest" Article 6(1)(e) of the GDPR. The second is an explicit exemption from regulatory liability and individual claimant standing with respect to the use of private data for suitably vetted IS platforms. Such an exemption would most likely need to be

[70] *Id.* at p.4.

[71] Thomas Wagner, Khaled Mahbub, Esther Palomar, Ali Abdallah, Cyber threat intelligence sharing: survey and research directions, *Computers and Security* 87 (2019).

[72] Vinod Sharma, Genevieve Bartlett, Jelena Mirkovic, "Critter: Content-Rich Traffic Trace Repository", *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*,

[73] *Id.*, at p. 15.

[74] *Id.*

[75] European Data Protection Board, *supra* note 58.

legislated in the national laws of all sharing parties. A third development depends upon technological tools that might be applied to information sharing in order to identify and scrub protected personal data, even at the cost of lessening the added value of IS.

3.3 Incentivizing IS to safeguard personal data through a polycentric approach

The Schrems II ruling and its ramifications for the sharing of information that includes protected personal data poses important regulatory challenges. One regulatory response to be considered in mitigating this risk for organizations is the incorporation of a polycentric approach to IS.

Polycentricity may be defined as the exercise of governance functions on the part of several stakeholders as they address a defined, collective problem in order to achieve a defined, collective goal.[76] A polycentric approach recognizes that diverse actors working at multiple levels and from different bases of legitimate regulatory authority can increase levels of cooperation and compliance, enhancing "flexibility across issues and adaptability over time."[77] Such an approach also incorporates the conceptualization of cybersecurity threats and cyberattacks as collective action problems that require coordination of a multiplicity of actors for their effective mitigation.[78] The particular suitability of polycentric governance for bolstering cybersecurity because of its multiplicity of actors, regulatory aspects and jurisdictions in cyberspace is noted by several scholars.[79] In the context of IS, such polycentric regulatory mechanisms can be highly beneficial because of the explicit acknowledgement of the complex interdependencies of all actors in cyberspace, [80] and the recognition that more diversity within the participant pool for information sharing can bring a broader array of the types of information that are available to mitigate cyber risk.[81]

[76] *See also* ERIC WINDHOLZ, GOVERNING THROUGH REGULATION: PUBLIC POLICY, REGULATION AND THE LAW (2017); OECD, REGULATORY POLICY OUTLOOK 2018, OCT. 10, 2018, https://read.oecd-ilibrary.org/governance/oecd-regulatory-policy-outlook-2018_9789264303072-en#page1 (on regulatory trends generally); Shackleford, *supra* note **Error! Bookmark not defined.**XX at 1283.

[77] Scott Shackelford, *Toward Cyberpeace: Managing Cyberattacks Through Polycentric Governance*, 62 AM. U. L. REV. 1273, 1284 (2013) at 1284.

[78] *Id.* at 1351 ("[W]without innovative institutional efforts at multiple scales it may be impossible to learn which combined sets of actions are the most effective in mitigating collective action problems like cyberattacks.").

[79] *Id.* at 1284 ("Polycentric regulation is . . . a multifaceted approach in keeping with the complexity of the crises in cyberspace."). *See also* ANDREW D. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT (2006); ROBERT K. KNAKE, INTERNET GOVERNANCE IN AN AGE OF CYBER INSECURITY (2010).

[80] *See* SHACKELFORD, SCOTT J., MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014), 99-100.

[81] Specifically, key parameters include the explicit inclusion of a multiplicity and diversity of trusted participants, and a range of regulatory incentives, tools, measures employed for IS. These might encompass, *inter alia*, national laws, sectoral self-regulation, best practices, guidelines, standards, international agreements, public-private partnerships, academic and consulting reports, and other types of regulation through information sharing. On the other hand, some drawbacks to the polycentric approach include fragmentation, "gridlock," inconsistency, and "the difficult task of getting diverse stakeholders to work well together across sectors and borders." Shackelford, *supra* note 76 at 1351-52.

For example, a cyber IS platform might incentivize information sharing for a broad diversity of sharers:

- *Government regulators and agencies* - which may legislate IS requirements and share cyber risk information under separate arrangements and protocols, including international agreements;

- *Sectoral actors* that may share information informally, as they are targeted simultaneously by malicious cyber actors;

- *Umbrella groups* formed within the sector for formal and informal IS;

- *Individual technical experts*:

- *Academic and consulting actors* providing external assessments of IS models and their effectiveness; and

- *Private individuals* who may share information through governmental, sectoral or organizational channels, or through informal channels such as social media, when they experience compromised cybersecurity through their personal internet use.

In the context of the issues raised for IS by the Schrems II ruling discussed above, stemming from the increased enforcement of data privacy rights in the EU and in many domestic law jurisdictions, it is worth examining further whether polycentricity may in fact augment regulatory supervision of the safeguarding of substantive legal rights through the inclusion in IS platforms of more gatekeepers of these rights, thus enabling greater transparency for their oversight.

4. Selected regulatory dilemmas

questions for discussion in Ostrom Workshop on November 16

We note here three of the theoretical dilemmas for regulators, both governmental authorities and sectoral self-regulators, as they promote information sharing is an exercise in trust building. These are presented below as questions for discussion:

- How should regulators weigh the question of whether to require IS or to offer it as a voluntary measure – including support for sectoral IS that does not include governmental entities?

- Does a sectoral basis for IS encourage more or less trust than a more generic approach?

- How does the increased automation of IS, greatly contributing to rapidity of its distribution and its implementation by organizations, affect trust-building in the sharing community?

5. CONCLUSIONS AND ISSUES FOR FURTHER STUDY

This article has aimed to show that information sharing is critical to cybersecurity, despite the current regulatory challenges associated with its optimal use. IS can serve to promote the exchange of cyber expertise; the sharing of critical technical data; real-time coordination of defensive actions; and, perhaps most importantly, the development of trust among key stakeholders in cybersecurity, whether for a particular sector or more generically. There is, overall, robust support among regulators and practitioners for IS: the potential advantages of increased cyber situational awareness outweigh the disincentives. As well, technological developments such as standardized reporting of cyber threat indicators, the use of TLP and STIX and TAXII architectures is leading to more automated IS - and thus its commoditization for an increasing pool of users outside of the traditional governmental and private sector stakeholders.

We have also argued, albeit briefly, that a polycentric approach to IS will augment the levels of cybersecurity that sharing platforms may be able to achieve. The more diverse the stakeholder pool for information sharing, the broader the types of information that are available to mitigate cyber risk. This advantage needs to be weighed against the necessity of trust-building within the sharing community, which may become more challenging as the IS community expands. The interesting issue of whether polycentricity may augment regulatory oversight of the safeguarding of substantive legal rights by enabling greater transparency requires further exploration and research.

The July 2020 Schrems II ruling of the CJEU poses difficult questions for IS at the level of safeguarding the substantive rights of individuals for protection of their personal data, as well as the resulting regulatory exposures of sharing organizations that are liable to inhibit IS. The current limbo with respect to the clarifications needed around the ruling aside, sharing organizations will need explicit guidance from regulators on their use of personal data that is either intentionally or inadvertently shared. We have proposed three ways forward out of the current limbo, albeit arduous ones.

Other issues that have been left open for further work include the quantification of success indicators for information sharing in bolstering cybersecurity; the effect of commoditization of threat data on trust-building, and the need to gain insights from information sharing in regulatory frameworks for collective action problems other than cybersecurity such as public health, environmental quality, and the elimination of debris in outer space). The need for regulatory attention to these and other aspects of IS becomes increasingly acute as the financial, reputational and other costs of cybersecurity escalate.

***