The Rise of "Global Information Law": Centennial Perspectives on the Conceptualization of Japanese Information Law

Itsuko Yamaguchi*

1. Introduction

1.1 Unprecedented challenges of hybrid tradeoffs

Surrounded by the unprecedented uncertainty due to the ongoing coronavirus disease (COVID-19) crisis, digitalization of conventional paper-based processes has been accelerated, thus inducing a wider range of digital transformations in how we communicate, work, and live our daily lives. This raises concerns about some recent trends in global data governance, where flow of data and information is increasingly mediated and controlled by a limited number of multi-country private platform operators and technology companies, and so-called "black-box" algorithmic decision-making systems are gradually implemented for practical uses[1].

While there are pros and cons to tougher regulations on platforms and algorithms, it is extremely difficult for an individual end-user and even for a sovereign state to have a clear overview of what is going on in today's globally connected societies.

How can we know, assess, and verify the unprecedented benefits and risks brought by innovative cyber-physical hybrid technologies, and make laws to meet new challenges in balancing tradeoffs especially relating to civil rights and liberties such as free speech, privacy, data protection, national security, and secret surveillance? What lessons, if any, can be drawn from the Japanese experience from a comparative law perspective?

1.2 Celebrating the 100th issue of the journal

To celebrate the 100th issue of the Journal of Information Studies, whose first issue was published in 1952, this article honors a founding frontier spirit of this journal in responding to new challenges emerging with the latest technologies of the time[2].

This article aims to clarify a strand of intriguing recent phenomena in global data

* Professor of Information Law and Policy, Interfaculty Initiative in Information Studies, Graduate School of Interdisciplinary Information Studies, The University of Tokyo

Key Words : Information, Law, Privacy, National Security, Online Platform, Algorithm, Transparency

governance, which might be broadly conceived as the rise of "global information law". It investigates the global reach of domestic and regional laws that govern transborder flows of data and information. It proceeds with the following four steps.

First, this article starts with terminology of key terms, in particular, "information", which has a connotation of a dynamic "flow" or circulation and underlies the conceptualization of "information law" in Japan in response to the so-called "informatization" of society roughly since the 1960s (Section 2).

Second, it reviews some cases of power struggles relating to transborder data flows, privacy, data protection, national security, and online intermediaries and platforms from comparative perspectives on laws of the United States (US), of the European Union (EU), and of Japan.

These cases highlight the increasing role of online intermediaries and platforms in US government secret surveillance, and concomitant EU judicial and legislative moves to extend the global reach of laws relating to privacy and data protection beyond borders (Section 3).

Third, this article points out another line of recent legislative proposals pertaining to such global reach of the EU laws, which lean toward a more expanding scope of platform regulations, and also takes up "black box" issues of algorithmic decision-making systems in the public sector (Section 4).

Fourth and lastly, it concludes by discussing the potential global reach of Japanese information law as a way of illuminating what we value beyond borders today and tomorrow - a matter requiring further investigation in today's globally connected societies (Section 5).

2. Terminology of Information, Data, and Knowledge

Let us take a brief look at key terms. "Information", "data", and "knowledge" are not always interchangeable terms. "Data" seems to have gained a wide symbolic use in the context of digital technologies including machine learning and deep learning of artificial intelligence (AI) during the last decade, being a vital raw resource to fuel innovation and the digital economy[3]. For example, "data" is said to be one of the "the main elements that compose AI", together with "algorithms", and "[w]ithout data, the development of AI and other digital applications is not possible"[4].

"Information" is typically contrasted with something tangible or physical, but it has been conferred a deeper and richer meaning in Japan. For example, while information is frequently perceived as "equivalent to a mere fragment of 'data'", it can also be understood as one of the "foundational concepts in the Universe" like

"materiality" and "energy."[5]

Furthermore, "information" has been conceived in socio-historical analysis in Japan to be closely associated with the aspect of military "intelligence" during the 1920s and 30s. Later, in the 1960s, its principle area of application shifted from the military to the economy, when people became aware of numerous social changes triggered by the advancement of computing and communication technologies, a phenomenon collectively known as the "informatization" [*Joho-ka* in Japanese] of society or "information society"[6]. It is noteworthy that information is essentially conceived as a dynamic "flow" or circulation, whereas knowledge is rather generally understood as something capable of accumulation or storage, as a static "stock"[7]. This article uses these terms with such connotations, which underly the conceptualization of Japanese "information law", as referred later in Section 5.

3. The Rise of Platform Powers and the Global Reach of EU laws

Since the global proliferation of Internet use, there have been constant power struggles across national borders over who governs, controls and owns information, data, knowledge, and any new intangible form of values.

Yet, as online intermediaries or platform services, such as search engines, social media, and cloud hosting, have grown to be essential societal infrastructure, a nascent ideal of laissez-faire openness and the Internet's democratizing effect have undergone changes, especially in the context of clandestine intelligence surveillance[8].

3.1 Foreign intelligence in corporation with online intermediaries

Particularly since the revelations by Edward Snowden in 2013[9], individual Internet users around the globe who depend upon US-based online services have become alarmed about how far the US National Security Agency (NSA) could go to access bulk telephone meta data and Internet content within and outside the country, how significant a role telecommunication carriers and Internet service providers could play in cooperation with the NSA, and how difficult it is to establish standing to challenge the constitutionality and statutory authorization of certain intelligence-gathering practices by the US government for national security reasons.

For instance, regarding the issue of whether or not the NSA's bulk telephone metadata program for virtually all U.S. citizens constitutes an unreasonable "search" under the Fourth Amendment of the US Constitution, the US federal district court in *Klayman v. Obama* courageously held that it does, whereas the district court in *ACLU* v Clapper did not[10].

Nevertheless, the *Klayman* court flatly refused to address the issue of the NSA's "PRISM" program, which allegedly collected Internet data content of targeted non-US persons located outside the US, pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA) of 1978. This is mainly because the plaintiffs had not alleged sufficient facts to satisfy their burden to establish standing under the standard set by the U.S. Supreme Court's decision in *Clapper v. Amnesty International USA* on February 26, 2013[11].

The same district court in *Klayman v. NSA* revisited this issue on November 21, 2017, added details in the reasoning, but eventually dismissed the plaintiff's challenge to the PRISM program[12].

This inevitably ignited serious transnational privacy concerns for the rest of the world. The US government subsequently introduced legislative amendments, organizational reforms, and strengthened commitments to transparency principles in intelligence communities[13]. Nevertheless, more significant repercussions came from the other side of the Atlantic, as explained next.

3.1.1 The CJEU in *Schrems I*: The "essentially equivalent"

The Court of Justice of the European Union (CJEU) handed down a landmark ruling in *Schrems I* (C-362/14) in October 2015, which invalidated the European Commission's Safe Harbor Decision on transfers of personal data from the EU to the US, pursuant to the "adequacy" requirement of Article 25 of the then-effective Data Protection Directive 95/46/EC.

The original proceeding of this case was based on a complaint by a user of the Facebook social network, who was an Austrian national residing in his home country. This Facebook user asked the Data Protection Commissioner to prohibit Facebook Ireland from transferring his personal data to Facebook Inc. located in the US, claiming that the US did not ensure "adequate" protection of personal data against surveillance activities by public authorities, with reference to the Snowden revelations[14].

In the reasoning, the CJEU took into consideration particularly that US law permits the public authorities to have "access on a generalised basis to the content of electronic communications", without providing "for any possibility for an individual to pursue legal remedies" relating to access, rectification or erasure of personal data. According to the CJEU, the Commission must find that the US ensures a level of protection of human rights "essentially equivalent" to that guaranteed in the EU legal order, but the said Commission Decision failed to do so[15].

3.1.2 The CJEU in *Schremes II*: Mandating a tough assessment job?

After the CJEU ruling in *Schremes I*, a renegotiated framework of the EU-US transfers of personal data, the European Commission's Privacy Shield Decision, was declared invalid by the CJEU in the *Schremes II* (C-311/18) case in July 2020, whereas the validity of the Standard Contractual Clauses (SCC) Decision was maintained by adding up certain stricter requirements[16].

In so doing, the CJEU avoided fatal practical consequences on EU-US data transfers. However, the CJEU still maintains that it is "apparent" that Section 702 of the FISA does not indicate "any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes", and the US Presidential directive issued in 2014 does not grant data subjects "actionable rights before the courts against the US authorities"[17].

Regarding a data transfer pursuant to the SCC, under Article 46(2)(c) of the General Data Protection Regulation (GDPR) enforced in May 2018[18], the CJEU says that the controller or the processor would be required to "verify" on a case-by-case basis whether "the law of the third country of destination" ensures adequate protection, and to provide "additional safeguards" if necessary[19].

It appears that the CJEU mandates a quite tough assessment job for not only the European Commission and the Member States, but also the controllers around the world who transfer personal data pursuant to the SCC to probe into national security laws of the third countries of destination around the globe[20].

3.2 The Global Reach of EU Law: The GDPR and "Adequacy Decision"

3.2.1 The global scalability of EU data protection law

The CJEU rulings in the *Schremes* case is pathbreaking for their global impact on transborder data flows, but this was not the first case. The CJEU ruling in *Google Spain* (C-131/12) in May 2014 was a forerunner that paved the way for a globally scalable reach of data protection laws of the EU and of the Member States.

This case is renowned for recognizing a right to request the search engine operator to delist certain search results or a so-called "right to be forgotten"[21] under the then-effective EU Data Protection Directive of 1995 (95/46/EC) and relevant laws of the Member States, which was later explicitly codified in Article 17 of the GDPR[22].

3.2.2 The CJEU in *Google Spain* under the Directive of 1995

Even under the Directive of 1995, the CJEU in *Google Spain* had already indicated a striking way of scaling up the territorial applicability of the EU data protection law, through an interpretation of a "controller" of the processing of personal data.

According to the reasoning of the CJEU, the operator of the search engine (i.e., the headquarters of Google, Inc. located in the US) must be regarded as the "controller" in respect of the processing of personal data within the meaning of Article of 2(d) of the Directive 95/46/EC, and the activities of Google, Inc. and those of Google Spain are "inextricably linked".

Therefore, Google Inc. would fall within the scope of Article 4(1)(a) of the Directive and the Member States' local laws[23].

3.2.3 A less spatial "territorial" scope: Article 3 of the GDPR

In comparison with Article 4(1)(a) of the Directive 95/46/EC, Article 3(1) of the GDPR delineates the territorial scope of application of EU data protection law in a less spatial sense[24].

For instance, Article 3(1) stipulates that the GDPR applies to the processing of personal data "in the context of the activities of an establishment of a controller or a processor" in the Union, as previously provided in the Directive, with a newly added phrase: "regardless of whether the processing takes place in the Union or not".

Article 3(2) of the GDPR goes further to state that a controller or a processor who is not even "established in the Union" will be covered under certain circumstances. The scope of such coverage is said to be determined by the following two-pronged approach: firstly, whether the processing relates to personal data of "data subjects who are in the Union", and if so, then secondly, whether the processing relates to "the offering of goods or services" or to "the monitoring" of data subjects' behavior in the Union[25].

3.2.4 The EU-Japan Adequacy Decision: An equal footing task for Japan?

Turning back to the issue of the CJEU's requirement of an "adequate" level of protection in the context of transborder data transfers, pursuant to Article 45 of the "adequacy" requirement of the EU GDPR, the European Commission Decision with respect to Japanese information privacy law was adopted in January 2019. The Japanese government adopted supplementary rules complementing the relevant domestic law to ensure the same level of protection as the EU law, applicable only to personal data transferred "from" the EU[26].

The EU-Japan Adequacy Decision after years of negotiation was a relief for Japanese business

operators in the private sector engaging in EU-Japan trade. This illustrates another example of the remarkably scalable reach of the EU data protection law.

However, this created the slightly odd situation, making those who reside in Japan think about a resultant domestic consequence brought about by an international agreement in terms of an equal footing. It would be up to the Japanese government to decide whether or not additional domestic measures should be taken.

4. The Next Agenda of EU Global Law and Algorithmic Systems

The previous section highlighted a set of interrelated phenomena of rising global platform powers and the concomitant global reach and effects of the EU laws relating to privacy and data protection.

4.1 Another global reach: A broader assessment on systemic risks in Article 26 of the proposed DSA

Yet another set of legislative proposals relating to digital intermediaries, platforms, and marketplaces was released by the European Commission: the Digital Services Act (DSA), accompanied with the Digital Markets Act (DMA), in December 2020[27]. As to the risk-based approach under Article 26 of the DSA, "very large online platforms" would be required to "identify, analyse and assess" at least once a year "any significant systemic risks stemming from the functioning and use made of their services in the Union", including:

(a) the dissemination of "illegal content" through their services,

(b) any negative effects for the exercise of the fundamental rights to respect for "private and family life, freedom of expression and information, the prohibition of discrimination and the right of the child", and

(c) "intentional manipulation" of their service, including by means of "inauthentic use or automated exploitation" of the service, with an actual or foreseeable negative effect on the protection of "public health, minors, civic discourse", or actual or foreseeable effects related to "electoral processes and public security".

That could be a strikingly encompassing range of risk assessment, given that Article 1(3) and Article 2(d) of this DSA proposal stipulate a similar kind of less spatial scope of application, like the GDPR mentioned above.

4.2 Public-sector algorithmic systems and due process

In addition to global platform regulatory issues, there is another point of concern on related recent phenomena whereby algorithmic decision-making systems procured from the private sector is gradually expanding in the decision-making of government and the public sector, meeting demands for efficiency, evidence-based practice, outsourcing, privatization, and probably cost-cutting.

For instance, in the United States, there have been relevant litigated cases over the prediction of recidivism in criminal justice, and the evaluation of teachers in public schools relating to the termination of employment, raising significant concerns in terms of due process[28]. If such algorithmic systems were to be implemented in the public sector in a way that unduly restricted access by stakeholders, possibly because of overly assertive private vendors' trade secrets and proprietary information protection, the algorithmic "black box" problem[29] would be exacerbated.

4.3 The Dutch SyRI algorithm on welfare fraud detection and transparency

In this regard, another instructive case is the Dutch district court of the Hague decision on February 5, 2020 on legislation for the Dutch government's use of the *SyRI* (System Risk Indication) algorithm system to detect various forms of fraud, including social benefit, allowance, and tax fraud. The district court assessed closely whether or not the current form of legislation complied with Article 8 of the European Convention on Human Rights (ECHR), which protects the right to respect for private and family life, home and correspondence, and ruled that it did not.

In the reasoning, the court declared that the risk model and risk indicators were "secret", and the application of SyRI was insufficiently "transparent" and "verifiable". The court also mentioned that there is "a risk that SyRI inadvertently creates links based on bias, such as a lower socio-economic status or an immigration background"[30].

This Dutch district court decision provides a good illustration of how prominently the principle of transparency stands out, in combination with other principles, to assess the balance between competing rights and interests, in the case of an application of algorithmic systems in the public sector.

Nevertheless, transparency obligations have a persistent downside of being too instrumental and burdensome for both regulators and regulated with nominal values for remedy. Even in the case of the EU GDPR, according to the two-year assessment report, resource problems for vigorous enforcement remain[31].

Furthermore, besides the data protection issues, the European Commission released the legislative proposal of the Data Governance Act

in November 2020, which facilitates "data sharing" based on "data altruism", particularly relating to re-use of health data held by public sector bodies. The proposed Act is said to be compatible with existing laws of data protection, intellectual property, and trade secrets[32].

5. Conclusion

5.1 Centennial research collaborations

Lastly, coming back to this article's mission to celebrate the 100th issue of the Journal of Information Studies, whose first issue was focused on social science research in the areas of mass communications, newspapers, and journalism[33]. The title of the journal changed twice until the current one was adopted, accompanied by organizational reforms and a broadening of the scope of interdisciplinary research relating to information across the humanities, social sciences, natural sciences and technology studies at the University of Tokyo.

In honoring the founding frontier spirit of this journal, this article has striven to identify through a review of some recent cases a crude but discernable strand of growing phenomena in global data governance, which might be broadly conceived as the rise of "global information law". It has investigated the global reach and effects of domestic and regional laws that govern transborder flows of data and information.

There have already been discussions on the so-called "Brussels Effect", which is the "unilateral regulatory globalization" when a single state is able to externalize its laws and regulations outside its borders through market mechanisms, resulting in the "globalization of standards", whose process is distinguishable from international treaties among states[34]. Still, in consideration of cases taken up in the previous sections in this article, the global reach and practical spillover effects of the EU data protection laws are remarkable[35]. Given that another series of EU legislative proposals relating to data and information are yet to come, such emerging new phenomena of global law are worthy of attention and further investigation.

5.2 The global reach of public-sector access rights in Japan

With respect to Japanese law on information privacy and access rights, and principles of transparency and accountability in the public sector, there has been a robust commitment in Japanese administrative law for several decades, partly because of severe criticisms from overseas against conventional styles of Japanese government administration for being overly opaque and informal. These principles were embodied into the enactment of the

Administrative Procedure Act in 1993, followed by the enactment of a Japanese equivalent of the US Freedom of Information Act (FOIA), information access statutes[36].

As evidence of the effectiveness of remedy in the public sector, it might be useful to share the experience of the Japanese multi-track incentivized mechanism, the Review Board framework as an ADR-type for remedy, in addition to judicial remedy, covering a wide range of appeals under the FOIA and information privacy statutes in the public sector, not even exempting "designated state secret" materials[37].

A disposition by the Review Board is not binding and only advisory in nature. The Review Board system is rather designed to incentivize those who possess a contested material to make it accessible as much and as expediently as possible. The system operates through several means including allocation of a burden of proof, fee-setting, and open reason-giving on the Internet.

Japan's complex multi-track remedy mechanism suffers from its own downside of being invisible and underused, both from overseas and within the country. Nevertheless, combined information access rights, provided by the Japanese FOIA and public-sector information privacy statutes, enable any FOIA disclosure requester or any data subject to seek remedy beyond national borders, without high litigation costs. This kind of global reach of the Japanese information access and privacy laws may be laudable[38].

5.3 Global information law: The next evolutionary step for Japanese information law?

This system design for access and information privacy in the public sector is one manifestation of the underlying conceptualization of "information law", which lays down basic principles and design mechanisms for enforcement and remedy to provide more comprehensive and effective solutions to far reaching and diverse information-related legal issues which crosscut traditional fields of law[39]. Therefore, a concept of information law has been built upon to cover a broad set of values for civil rights and liberties, and any newly emerged form of democratic values as laid out generously in the post-World War II Constitution of Japan, including privacy[40]. The basis of this concept is the social perception of the word, "information" in Japan which is intricately woven with ideas, thoughts, and meanings in a different way from "data" or "knowledge", as mentioned in section 2 of this article. As the nature of information is in dynamic flow, rather than static stocks, information law would have to embrace changes if it is to serve in globalized societies.

In a descriptive sense, there is no statute titled "*Joho-ho*" (information law) in Japan. "Information law" is often defined concisely and broadly as a field of "laws relating to the

production, distribution and consumption of information"[41]. In its essence, information law developed in Japan is the art of illuminating what we value today and tomorrow and designing legal instruments to embody it.

Whether or not such recent endeavors for a global law can meet the challenges presented by the unprecedented scale of systemic power imbalance problems we are witnessing amid the COVID-19 crisis – in particular, shifting the undue burden away from those who are most vulnerable in this globalized society – depends on how we can infuse normative content into the law attractive enough to all stakeholders, wherever they may be.

Notes

[1] This article is partly based on the author's previous works including online presentations at the "Free Speech in the 21st Century" global conference, organized by Alma Mater Europaea international university and the International Association of Constitutional Law (IACL) on July 3, 2020, and the "Centennial Strategic Research Initiatives: A Kickoff Workshop" at the University of Tokyo on December 28, 2020. English translation of Japanese text in this article is provided by the author, unless otherwise specified. Website information cited in the article was last visited on March 8, 2021. This work was partly supported by JSPS KAKENHI Grant Number 17K03501. The author wishes to express gratitude to Professor Emeritus Junichi Hamada for thoughtful comments, Mr. David Buist for carefully proofreading the draft, and all participants of the conferences above and of classes at the University of Tokyo for stimulating discussions.

[2] *See* Yujiro Chiba, *Hakkan ni Saishite* [*Forewords*], and *Gendai no Shinbun-jiyu [Freedom of the Press in Modern Society]*, 1 The Bulletin of the Institute of Journalism, Tokyo University 1-2, 16-30 (1952) [in Japanese]. The Institute of Journalism [*Shinbun Kenkyujo* in Japanese] was established at the University of Tokyo in 1949, and the preceding research organization was established in 1929 at the Imperial University of Tokyo, to conduct social science study with a special emphasis on a typical form of mass communications at that time, i.e., newspaper [*shibun* in Japanese]; *see also* Hideo Ono, *Iwayuru Sekaisaiko no Shuukanshi Aviso no Kenkyu [Study of Aviso, the so-called Oldest Weekly Newspaper in the World]*, The Bulletin of the Institute of Journalism, *supra*, *at* 3-16 [in Japanese].

[3] For example, according to a legislative proposal of the "Data Governance Act" published in November 2020, definition of "data" in Article 2(1) stipulates that "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording". European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act) (Nov. 25, 2020), COM(2020) 767 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN.

Article 4 of the General Data Protection Regulation (GDPR) defines 'personal data' to mean that: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, L 119, Vol. 59 (May 4, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN.

[4] European Commission, WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust (Feb. 19, 2020), COM(2020) 65 final, pp. 8, 16, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-

feb2020_en.pdf. It says that a definition of AI needs to have sufficient flexibility, and provides multiple versions provided by the European Commission. For example, as an initial simpler version of definitions, "Artificial intelligence (AI) refers to systems that display intelligent behavior by analysing their environment and taking actions--with some degree of autonomy --to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)". *See* European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Artificial Intelligence for Europe (Apr. 25, 2018), COM(2018) 237 final, p. 1, https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF.

[5] Toru Nishigaki, *Joho [Information]*, in JOHO-GAKU JITEN [ENCYCLOPEDIA OF MEDIA AND INFORMATION STUDIES] 436 (Takashi Kitagawa et al. eds., 2002).

[6] Shunya Yoshimi (David C. Buist trans.), *Information*, Theory, Culture & Society, Vol. 23, No. 2-3, March-May 2006, at 271-277.

[7] *Id*. at 271-272.

[8] *See, e.g.*, Itsuko Yamaguchi, *Beyond De Facto Freedom: Digital Transformation of Free Speech Theory in Japan*, 38 Stan. J. Int'l L. 109 (2002); Itsuko Yamaguchi, *Kokka Anzenhosho niokeru Algorithm niyoru Kanshi: Kenpo jo no Genron no Jiyu, Privacy to Platform Jigyosha no Yakuwari [Free Speech, National Security, and Privacy under Stress of Algorithmic Surveillance: A Comparative Study of Japan and the United States]*, 3 Kenpo Kenkyu 47-54 (2018) [in Japanese]; Itsuko Yamaguchi (Translated by David C. Buist), *Cyberlaw*, Theory, Culture & Society, *supra* note 6, at 529-531.

[9] *See*, e.g., Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, The Guardian, (June 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Barton Gellman & Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, The Washington Post (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.8aabfe16aa1c; *see also* THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS (Dec. 2013), https://obamawhitehouse.archives.gov/blog/2013/12/18/liberty-and-security-changing-world.

[10] Klayman v. Obama, 957 F.Supp.2d 1 (D.D.C. 2013); ACLU v. Clapper, 959 F.Supp.2d 724 (S.D.N.Y. 2013).

[11] *Klayman*, 957 F.Supp.2d at 8 n.6. Concerning issues of the government surveillance and standing of individual users and their service providers, *see, e.g.*, Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410-414, 422 (2013); *Chapter Two Standing, Surveillance, and Technology Companies*, 131 Harv. L. Rev. 1742 (2018); Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 Stan. L. Rev. 99, 132, 156-157(2018).

[12] Klayman v. Nat'l Sec. Agency, 280 F. Supp. 3d 39, 55–58 (D.D.C. 2017), *aff'd sub nom*. Klayman v. Obama, 759 F. App'x 1 (D.C. Cir. 2019).

[13] *See, e.g.*, Office of the Director of National Intelligence, Statistical Transparency Report: Regarding the Use of National Security Authorities, Calendar Year 2019 (Apr. 2020), https://www.odni.gov/files/CLPT/documents/2020_ASTR_for_CY2019_FINAL.pdf.

[14] The CJEU, Case C-362/14, Maximillian Schrems v Data Protection Commissioner (*Schrems I*), at paras. 26-30 (Oct. 6, 2015), ECLI:EU:C:2015:650, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362.

[15] *Id*. at paras. 74-75, 94-98.

[16] The CJEU, Case C-311/18, Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (*Schrems II*) (July 16, 2020), ECLI:EU:C:2020:559, http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=8483023. *See also* Hendrik Mildebrath, European Parliamentary Research Service, *At A Glance: The CJEU Judgment in the Schrems II case* (Sept. 2020), https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf. Regarding the SCC, *see* Article 26 of Directive 95/46/EC, and Article 46 of the GDPR.

[17] The CJEU, *Schrems II*, at paras 180-181. *See also* Recent Cases, 134 Harv. L. Rev. 1567, 1570-1572 (2021).

[18] Regulation (EU) 2016/679 [GDPR], *supra* note 3.

[19] The CJEU, *Schrems II*, at paras. 134-149; *see also* European Data Protection Board (EDPB), Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (July 24, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTS, INFORMATION PRIVACY LAW 1291-1295 (7th ed. 2021).

[20] SOLOVE & SCHWARTS, *supra* note 19, at 1292-1294.

[21] *See, e.g.,* THE RIGHT TO BE FORGOTTEN: A COMPARATIVE STUDY OF THE EMERGENT RIGHT'S EVOLUTION AND APPLICATION IN EUROPE, THE AMERICAS, AND ASIA (IUS COMPARATUM - GLOBAL STUDIES IN COMPARATIVE LAW, vol. 40) (Franz Werro ed., 2020).

[22] The CJEU, Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (*Google Spain*), (May 13, 2014), ECLI:EU:C:2014:317, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131.

[23] The CJEU, *Google Spain*, at paras. 55-56. *See*, Dan Jerker B. Svantesson, *Article 3. Territorial scope*, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 79-81 (Christopher Kuner et al. eds., 2020).

[24] Svantesson, *supra* note 23, at 81-96.

[25] EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3),Ver. 2.1 (12 Nov. 2019), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf; Svantesson, *supra* note 23, at 88.

[26] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (Text with EEA relevance), Official Journal of the European Union, L 76, Vol. 59 (Mar. 19, 2019), at 1–58, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0419&from=EN; European Commission, EU Japan Adequacy Decision, Fact Sheet (Jan. 2019), https://ec.europa.eu/info/sites/info/files/research_and_innovation/law_and_regulations/documents/adequacy-japan-factsheet_en_2019_1.pdf. *See also* Masao Horibe & George Shishido, *Daiikki Kojinjohohogo-iinkai wo Furikaeru*, 1534 Jurist, at ii-v, 52-63 (2019) [in Japanese]; Shizuo Fujiwara et al., *Special Feature, 2020 Kojinjohohogoho Kaisei*, 1551 Jurist 13-53 (2020).

[27] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (Dec. 15, 2020), COM(2020) 825 final, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72148; European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act)(Dec. 15, 2020), COM(2020) 842 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en. *See also* European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, On the European democracy action plan (Dec. 3, 2020), COM(2020) 790 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790&from=EN. *See, e.g.,* Ryoji Mori et al., *Special Feature, Platform-kisei no Genzaichi,* 1545 Jurist 13-44 (2020) [in Japanese]; George Shishido et al., *Special Feature, Internet-jo no Hibochusho-mondai*, 1554 Jurist 13-52 (2021) [in Japanese].

[28] *See, e.g.,* State v. Loomis, 881 N.W.2d 749, 761 (Wis. 2016); Houston Fed'n of Teachers, Local 2415 v. Houston Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1171, 1175-1180 (S.D. Tex. 2017).

[29] *See, e.g.,* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 3-18, 216-218 (2015); Deven R. Desai & Joshua A. Kroll, *Trust but Verify: A Guide to Algorithms and the Law*, 31 Harv. J.L. & Tech. 1 (2017); Hannah Bloch-Wehba, *Access to Algorithms*, 88 Fordham L. Rev. 1265, 1279-1295 (2020); Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 Yale J. L. & Tech. 103, 122-131, 153-159 (2018); Cary Coglianese & David Lehr, *Transparency and Algorithmic Governance*, 71 Admin. L. Rev. 1 (2019).

[30] Rechtbank Den Haag, *SyRI legislation in breach of European Convention on Human Rights*, Feb. 5, 2020, ECLI:NL:RBDHA:2020:1878, C-09-550982-HA ZA 18-388 (English), https://www.escr-net.org/sites/default/files/caselaw/ecli_nl_rbdha_2020_1878.pdf.

[31] European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation (June 24, 2020) ,COM(2020) 264 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN.

[32] *See* the proposed Data Governance Act, *supra* note 3.

[33] Chiba, *supra* note 2, at 1-2.

[34] Anu Bradford, *The Brussels Effect*, 107 Nw. U. L. Rev. 1, 3-4 (2012).

[35] *See, e.g.,* ELAINE FAHEY, THE GLOBAL REACH OF EU LAW (2017); MARISE CREMONA & JOANNE SCOTT, EU LAW BEYOND EU BORDERS: THE EXTRATERRITORIAL REACH OF EU LAW (2019).

[36] HIROSHI SHIONO, GYOSEIHO I [ADMINISTRATIVE LAW, Vol. 1] 76-95, 292-403 (6th ed. 2015) [in Japanese]. *See also* Koichi Akasaka, *Koukenryoku no Toumeisei to Riyukaiji,* 27 Quarterly Jurist 139-150 (2018) [in Japanese]; about open reason-giving by the administrative remedy system in general, *see, e.g.,* Yoichi Ohashi, *Gyoseifufukushinsakai-toushin no Hougaku-kenkyu no Hitsuyousei to Igi,* 32 Quarterly Jurist 90-98 (2020) [in Japanese].

[37] KATSUYA UGA, KOJINJOHOHOGOHO NO CHIKUJOKAISETSU [COMMENTARY ON PERSONAL INFORMATION PROTECTION LAWS] 26, 466-476, 578-585, 662-665 (6th ed. 2018) [in Japanese]; UGA, *NEW COMMENTARY, infra* note 38.

[38] *See* KATSUYA UGA, SHIN JOHOKOKAIHO NO CHIKUJOKAISETSU [NEW COMMENTARY ON INFORMATION DISCLOSURE LAWS] 36-37, 56-58, 66-128, 196-205, 270, 295-296 (8th ed. 2018) [in Japanese]. *See also* Itsuko Yamaguchi, *Protecting Privacy against Emerging "Smart" Big Data Surveillance: What can be Learned From Japanese Law?*, 1 PERCORSI COSTITUZIONALI, at 193, 199-204 (2014).

[39] *See, e.g.,* JUNICHI HAMADA, JOHO-HO [INFORMATION LAW] (1993) [in Japanese]; KATSUYA UGA & YASUO HASEBE, JOHO-HO [INFORMATION LAW] (2012) [in Japanese]; MASAHIRO SOGABE ET AL., JOHO-HO GAISETSU [INFORMATION LAW: AN INTRODUCTION] (2d ed. 2019) [in Japanese]; TARO KOMUKAI, JOHO-HO NYUMON [INTRODUCTION TO INFORMATION LAW] (5th ed. 2020) [in Japanese]; George Shishido et al., *Special Feature 1, Joho-ho toiu Frontier*, 479 Hougaku Kyoshitsu 4-42 (2020) [in Japanese]; YASUO HASEBE ET AL., MEDIA HANREI HYAKUSEN [100 SELECTED CASES IN MEDIA LAW] (2d ed. 2018) [in Japanese]; SHIGENORI MATSUI ET AL., INTERNET HO [INTERNET LAW] (2015) [in Japanese]; NOBUHIRO NAKAYAMA, CHOSAKUKEN-HO [COPYRIGHT LAW] 11-42 (3rd ed. 2020). *See also* ITSUKO YAMAGUCHI, JOHO-HO NO KOZO: JOHO NO JIYU, KISEI, HOGO [THE ARCHITECTURE OF INFORMATION LAW: FREEDOM, REGULATION, AND PROTECTION OF INFORMATION] (2010) [in Japanese].

[40] The current Japanese Constitution (*Nihonkoku Kenpo*) was promulgated in 1946. For the English translation, *see* National Diet Library, *The Constitution of Japan, based on the English Edition by Government Printing Bureau*, https://www.ndl.go.jp/constitution/e/etc/c01.html. For a brief overview of development of privacy and data protection laws in Japan, *see, e.g.,* Itsuko Yamaguchi, *A Japanese Equivalent of the "Right to Be Forgotten" : Unveiling Judicial Proactiveness to Curb Algorithmic Determinism,* in THE RIGHT TO BE FORGOTTEN, *supra* note 21, at 291-310, https://link.springer.com/chapter/10.1007/978-3-030-33512-0_15.

[41] For an influential definitions of "information law" and a concept of "right to information" in Japan, *see* Junich Hamada, Joho-ho [*Information Law*], in JOHO-GAKU JITEN, *supra* note 5 [in Japanese], at 473; Junichi Hamada, *Joho-media-housei [Information Media Law],* 60 Koho Kenkyu 25, 39-42 (1998)[in Japanese]; Junich Hamada, *Joho-tsushin Seisaku no Aratana Dankai ni Mukete [Toward a New Stage of Information and Communications Policy Research],* 1 Journal of Information and Communications Policy 3-8 (2017) [in Japanese], https://www.jstage.jst.go.jp/article/jicp/1/1/1_3/_pdf/-char/en.

Itsuko Yamaguchi

［専門］Information Law and Policy

［主たる著書・論文］

Itsuko Yamaguchi, *A Japanese Equivalent of the "Right to Be Forgotten" : Unveiling Judicial Proactiveness to Curb Algorithmic Determinism*, in THE RIGHT TO BE FORGOTTEN: A COMPARATIVE STUDY OF THE EMERGENT RIGHT'S EVOLUTION AND APPLICATION IN EUROPE, THE AMERICAS, AND ASIA (IUS COMPARATUM - GLOBAL STUDIES IN COMPARATIVE LAW, vol. 40) 291-310 (Franz Werro ed., 2020)

Itsuko Yamaguchi, *Hyogen no Jiyu to Chosakuken: AI Jidai no "User Rights" Gainen to sono Check Kino [Freedom of Expression and Copyright: A Concept of "User Rights" and its Checking Function in the Age of Artificial Intelligence]*, 25 Quarterly Jurist 61-67 (2018) [in Japanese]

ITSUKO YAMAGUCHI, JOHO-HO NO KOZO: JOHO NO JIYU, KISEI, HOGO [THE ARCHITECTURE OF INFORMATION LAW: FREEDOM, REGULATION, AND PROTECTION OF INFORMATION] (University of Tokyo Press, 2010) [in Japanese]

［所属］

Professor of Information Law and Policy
Interfaculty Initiative in Information Studies
Graduate School of Interdisciplinary Information Studies
The University of Tokyo

［所属学会］

Japan Public Law Association
Japanese American Society for Legal Studies
Japan Society for Studies in Journalism and Mass Communication
The Society of Socio-Informatics

The Rise of "Global Information Law": Centennial Perspectives on the Conceptualization of Japanese Information Law

Itsuko Yamaguchi*

How can we know, assess, and verify the unprecedented benefits and risks brought by innovative cyber-physical hybrid technologies, and make laws to meet new challenges in balancing tradeoffs especially relating to civil rights and liberties such as free speech, privacy, data protection, national security, and secret surveillance? What lessons, if any, can be drawn from the Japanese experience from a comparative law perspective?

To celebrate the 100th issue of the Journal of Information Studies, whose first issue was published in 1952, this article honors a founding frontier spirit of this journal in responding to new challenges emerging with the latest technologies of the time.

This article aims to clarify a strand of intriguing recent phenomena in global data governance, which might be broadly conceived as the rise of "global information law". It investigates the global reach of domestic and regional laws that govern transborder flows of data and information. It proceeds with the following four steps.

First, this article starts with terminology of key terms, in particular, "information", which has a connotation of a dynamic "flow" or circulation and underlies the conceptualization of "information law" in Japan in response to the so-called "informatization" of society roughly since the 1960s.

Second, it reviews some cases on power struggles relating to transborder data flows, privacy, data protection, national security, and online intermediaries and platforms from comparative perspectives on laws of the United States, of the European Union, and of Japan. These cases highlight the increasing role of online intermediaries and platforms in US government secret surveillance, and concomitant EU judicial and legislative moves to extend the global reach of laws relating to privacy and data protection beyond borders.

* Professor of Information Law and Policy, Interfaculty Initiative in Information Studies, Graduate School of Interdisciplinary Information Studies, The University of Tokyo

Key Words: Information, Law, Privacy, National Security, Online Platform, Algorithm, Transparency

Third, this article points out another line of recent legislative proposals pertaining to such global reach of the EU laws, which lean toward a more expanding scope of platform regulations. It also takes up "black box" issues of algorithmic decision-making systems in the public sector.

Fourth and lastly, it concludes by discussing the potential global reach of Japanese information law as a way of illuminating what we value beyond borders today and tomorrow - a matter requiring further investigation in today's globally connected societies.