National Institute of Informatics News ISSN 1883-1966 (Print) ISSN 1884-0817 (Online)

NII Today

92
Sep. 2021
National Institute of Informatics News

Interview | **Protecting Privacy**
Perspectives on Data Security Control in Academic Research: SHISHIDO, George

Q&A | What is Required of Academia Under the Amended Personal Information Law: SATOH, Ichiro

Roundtable | Enhancing Competitiveness through Stronger Governance: DOI, Miwako; HIOKI, Tomomi; SATOH, Ichiro

Contribution | Personal Information Protection in Academic Research and Foreign Data Protection Laws: ITAKURA, Yoichiro

Essay | A Town Where Everyone Knows Everyone and a World in which People Chat Intimately with Electronic Devices: OKADA, Hitoshi

Feature

From Personal Information to Privacy

The Amended Personal Information Law and Privacy Governance

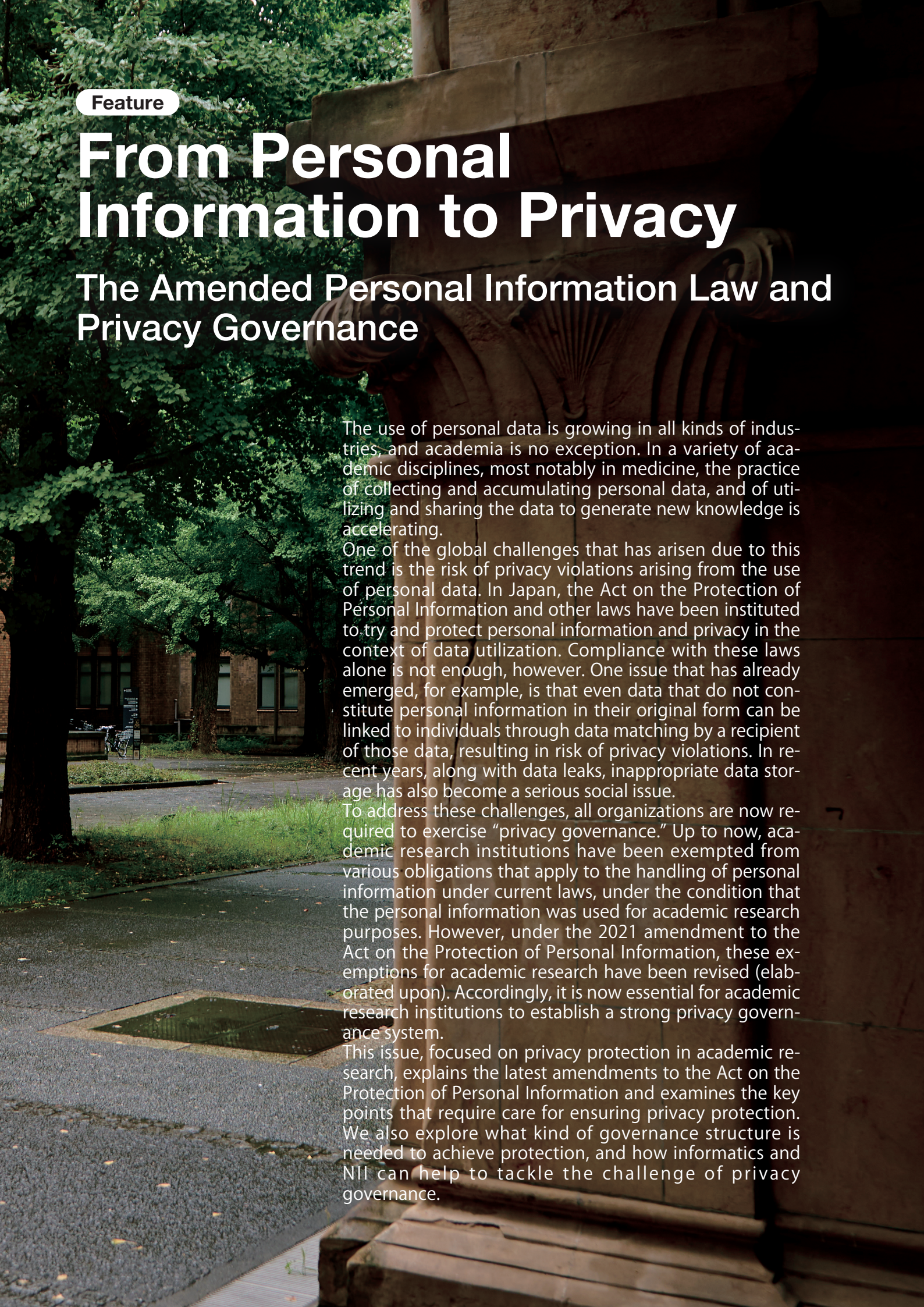
This English translated version NII Today corresponds to No. 92 of the Japanese edition

www.nii.ac.jp/en/about/publications/today/

Feature

From Personal Information to Privacy

The Amended Personal Information Law and Privacy Governance



The use of personal data is growing in all kinds of industries, and academia is no exception. In a variety of academic disciplines, most notably in medicine, the practice of collecting and accumulating personal data, and of utilizing and sharing the data to generate new knowledge is accelerating.

One of the global challenges that has arisen due to this trend is the risk of privacy violations arising from the use of personal data. In Japan, the Act on the Protection of Personal Information and other laws have been instituted to try and protect personal information and privacy in the context of data utilization. Compliance with these laws alone is not enough, however. One issue that has already emerged, for example, is that even data that do not constitute personal information in their original form can be linked to individuals through data matching by a recipient of those data, resulting in risk of privacy violations. In recent years, along with data leaks, inappropriate data storage has also become a serious social issue.

To address these challenges, all organizations are now required to exercise "privacy governance." Up to now, academic research institutions have been exempted from various obligations that apply to the handling of personal information under current laws, under the condition that the personal information was used for academic research purposes. However, under the 2021 amendment to the Act on the Protection of Personal Information, these exemptions for academic research have been revised (elaborated upon). Accordingly, it is now essential for academic research institutions to establish a strong privacy governance system.

This issue, focused on privacy protection in academic research, explains the latest amendments to the Act on the Protection of Personal Information and examines the key points that require care for ensuring privacy protection. We also explore what kind of governance structure is needed to achieve protection, and how informatics and NII can help to tackle the challenge of privacy governance.

Interview

Protecting Privacy

Perspectives on Data Security Control in Academic Research

SHISHIDO, George
Professor, Graduate Schools for Law and Politics,
The University of Tokyo
Visiting Professor, NII

Interviewer: **ASAKAWA, Naoki**
Editor in Chief, Nikkei Computer

In May 2021, the Diet passed and instituted an amendment to the Act on the Protection of Personal Information. In addition to unifying data protection across public and private sectors, the amendment also revises provisions related to academic research, so its impact on research that involves information on individuals will be substantial. In this article, Professor SHISHIDO, George of The University of Tokyo (and visiting professor at NII), an expert on information law, explains the main points that academic institutions and individual researchers need to keep in mind when it comes to handling personal data and the new privacy protection system.

What does privacy protection mean?

In recent years, the Act on the Protection of Personal Information (hereinafter also "personal information law") has been revised several times. I get the impression that it has become more difficult for non-specialists to understand the rules about privacy. To begin with, what exactly does it mean to protect privacy?

SHISHIDO It used to be that privacy meant preserving the peace and quiet of someone's private life. Traditionally, guaranteeing privacy meant keeping a clear dividing line between activities in the public sphere, relating to politics, society, and economics, and activities in the private sphere, such as relaxing at home or engaging in intimate relationships with friends and family, for the purpose of protecting the tranquility of one's private life.

A look back at history shows that the concept of privacy has changed with advances in science and technology. Firstly, the development of portable cameras and newspapers in the late 19th century led to a heightened awareness about privacy protection. Then, as data processing technologies developed in the 20th century, new fears arose about the danger that personal data held by governments and corporations could be combined and matched.

Consequently, there has been a growing concern that even information that is public to some extent can constitute

an invasion of privacy if it is used recklessly or provided inappropriately to a third party. Since the 1960s, the concept of a right to control information about yourself, the right of "informational self-determination," has emerged strongly in Europe and the U.S. It is the idea that it would be very difficult to live our lives securely and freely as individuals without this new right that has led us to today's debates about privacy protection.

The development of information technology in recent years has enabled companies to collect huge amounts of data about consumer behavior. By collecting information tied to the consumption of their goods and services, companies have come to hold far more personal information than governments. And these data may be distributed across multiple companies. Furthermore, if governments get access to these data from companies and link it to information they possess, they can gain a very detailed understanding of how individuals live their lives.

The personal information law alone does not ensure privacy protection

In Japan, the personal information law was first enacted in 2005 in response to growing concerns about data privacy. Since then, multiple amendments have been made, specifically, in 2015, 2020, and 2021.*1 What role do these personal information laws play in the context of privacy protection?

SHISHIDO Let's start with the premise that there is some overlap between privacy protection and the personal information laws, but also some misalignment. Privacy protection is the subjective right of individuals to demand that governments, companies, and other entities not disturb the peace and quiet of their private lives or use their personal data in any way that violates their privacy in this sense.

On the other hand, the personal information law is premised on the fact that there is value in distributing and making use of information about individuals, or so-called "personal data," within society. Accordingly, the law is designed as a broad framework for ensuring that the rights and interests of individuals, including privacy, are not violated in the process of using personal information.

Depending on whether the held information is scattered, or if it is personal data managed in a database, or retained personal data, the law defines obligations such as "to specify the purpose of use and to limit the use of information to that scope"; "in principle, to obtain the consent of the data subject when providing information to a third party";*2 and "to respond to a request for disclosure from the data subject." The law formally distributes rights and powers between the data subject and the entity handling the data, according to the form of the information.

The personal information laws undoubtedly serve to protect privacy to a certain degree, but in terms of the right of "informational self-determination," they fall short of allowing total control by the individual.

Aside from the personal information law, there are other privacy protection mechanisms, based on the content and nature of data and on the degree of potential harm to the individual. In the medical field, there is doctor-patient confidentiality,*3 as defined by the Medical Practitioners Act, and telecom carriers are subject to the "secrecy of communications"*4 rule.

Even in academia, a researcher might formally comply with the personal information law, thinking, "Well, I got consent for this, so everything's OK." But that might not be enough, actually.

The 2021 amendment will significantly impact academic research

In the May 2021 amendment, the protection standards of private and public hospitals were brought into alignment and exceptions for academic use were revised. (See Fig. 1.)

SHISHIDO Private academic institutions were previously exempted from the mandatory provisions that applied to other entities handling personal information, based on the principle of academic freedom. Or else, the Personal Information Protection Commission would refrain from exercising its authority over such institutions.

I think that this was reasonable up to a point for the legislation of the time. However, research today is much more dependent on data than it was. Plus, making personal information handling in research safer and more secure should promote rather than discourage research. With the 2021 amendment, there is a shift away from a blanket exemption for private-sector research to the application of nuanced rules.

Whereas national university corporations and public research institutions have been subject to personal information rules, these rules did not apply to the private sector. With the 2021 amendment, the rules apply to both, making it easier to distribute personal data for research purposes between public and private entities. In effect, it's no longer necessary to worry about differences in rules, so you can pass on your data with confidence, knowing that the recipient will be implementing the same security control measures as your own organization.

At the same time, when academic research is supervised by the government, there are potentially very serious implications for academic freedom and university autonomy. The 2021 amendment has considered this point carefully by applying the same rules

about security control measures and requests for disclosure of personal data, etc., for protecting the rights and interests of individuals that private companies are subjected to, while still allowing some exemptions from restrictions on purpose of data use and on the sharing of personal data. This represents a rethink of the balance between academic freedom and personal data protection.

Developing security control systems and a pile of other issues

The most laborious task for academic institutions is probably the development of a security control system. Private companies too struggle with this. How should they set out to tackle this task?

SHISHIDO In short, developing a system of security control measures is all about establishing and operating a data governance system. This applies to all entities, companies and academic institutions alike.

In the case of universities and research institutions, you start by taking stock of the situation, answering questions like, "What kind of research are we doing?", "What data are we holding for our research?", "How are we using it?" and "Who can access it?"

Then, based on this itemization, you bring to light the content and nature of the data handled by the research institution and the risks faced by the individual data subjects. In accordance with the risks, you can then formulate suitable security control measures.

Obviously, this can be a very challenging task for individual researchers and research institutions. I think that the academic community will need to collectively create a voluntary code of practice, guidebook, checklists, and that sort of thing.

At the same time, there are two other points that the broader academic community needs to discuss.

One is the issue of cross-border personal data transfers. Examples of this are receiving data from an external source, storing data on an external server, and outsourcing data handling to an external research institution. If the data transfers are only within Japan, there are far fewer problems, but for research activities aimed at universal knowledge creation, it is inevitable that data will cross international borders.

Research universities often host foreign researchers, graduate students, and young researchers from abroad, to collaborate on research. This is where a variety of risk challenges that go beyond personal data protection in its original narrow sense enter the picture simultaneously, including discussions of economic security and other matters.

Rules that restrict research in terms of data handling cannot be implemented solely in a domestic context. Even while setting up domestic rules, it is necessary to keep an eye on trends in overseas rules. This is an issue that should be tackled by the whole academic community in the wake of this amendment.

Another point relates to industry-academia collaboration. As soon as researchers generate universal knowledge through their research, their findings are employed to develop new products and services through industry-academia collaboration. There are even situations where the findings impact either the individual subjects whose personal data were collected or the clusters (groups) to which the individuals belong in some way.

Under the 2021 amendment, private-sector research institutions are also judged to be academic research institutions if their main purpose is academic research, which reflects the growing importance of industry-academia collaboration in today's research environment. However, from the point of view of the data provider or data subject, acceptability will vary depending on how the data are used, for example, whether for knowledge creation, for social benefit through drug design after deeper research, or for further use in marketing without consent. Separate to the legal requirements for industry-academia collaboration, academic institutions will be required to ensure transparency and governance by formulating rules and explaining them to data providers and the public.

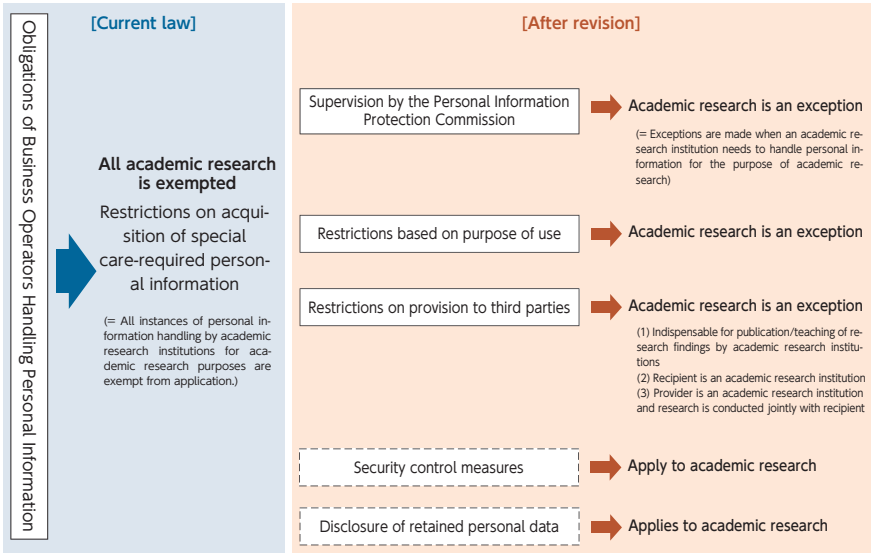


Fig. 1 Excerpts from "Revision (Elaboration) of Exemptions for Academic Research"
Created based on the diagram on page 26 of the "Act on the Protection of Personal Information: Proposed Amendments in 2020 and 2021" (May 7, 2021, Personal Information Protection Commission).https://www.meti.go.jp/shingikai/sankoshin/shomu_ryutsu/bio/kojin_iden/life_science/pdf/001_03_02.pdf

SHISHIDO, George
Graduated from the Faculty of Law of The University of Tokyo in 1997. After working as an assistant at The University of Tokyo Graduate Schools for Law and Politics, he was appointed as a professor there in 2013. He served as a member of the "Personal Data Study Group" of the IT Strategic Headquarters of the Cabinet Secretariat (2013-2014) and a member of the "Personal Information Protection System Review Study Group" of the Cabinet Secretariat (2020). His fields of specialization are constitutional law and information law. He is the author of numerous books, including "New Handbook of Precedents: Information Law" (editor and author, Nippon Hyoron Sha, 2018) and "Transformation of the Laws under Society with Artificial Intelligence" (co-editor and co-author, Yuhikaku, 2020).

Industry-academia collaboration and cross-border data transfers

According to the interpretation of the current Personal Information Protection Commission,*5 when personal information is handled for the purpose of product development, it is not considered to be "for academic research purposes," even for academic institutions. Is there some confusion around the interpretation of this point in industry-academia collaboration?

SHISHIDO This could become an issue in the future. Up to now, I don't think that either the industry people or researchers who are committed to industry-academia collaboration have been deeply concerned about this point. If we can't sort out this issue properly, we'll have a very big problem on our hands.

In some cases of industry-academia collaboration, data are used for purposes that cannot be considered academic research at all, while in other kinds of R&D collaboration, it is hard to distinguish between research and development. Medicine is a typical example of the latter. In view of this, it would be better to properly rethink data handling for each specific research field, including industry collaborations.

Cross-border data transfers involve even more difficult issues. Some politicians believe that due to China's National Intelligence Law, any data transfer to China constitutes a violation of security control measures. At the same time, the U.S. and China are pursuing joint research very actively and data sharing in academic disciplines is likely to continue growing. So, hopefully internationally acceptable rules will be formulated soon.

SHISHIDO There is a short-term problem, as well as a medium to long-term problem. Firstly, the short-term issue is that departments and labs conducting research that relates directly to national security need to create clear rules for security control.

Over the medium to long term, researchers need to carefully and deeply rethink the importance and value of publishing and sharing their academic research findings with the whole world. On this basis, we should then consider national security-related rules for each field of research and seek political responses within international frameworks, like Japan-U.S.-Europe, or Japan-China.

Academic research aims to contribute to the development of all humanity, transcending divisions between countries. I believe that collaboration between academic institutions, including cross-border data transfers, joint research, and personnel exchanges, should ideally contribute to the peace and welfare of all humankind, in a different way than the high politics of short-term international politics (a policy area of high importance). The way the world has collaborated on research through the COVID-19 crisis shows the significance of such cooperation and hints at the kind of problems that may arise if things don't work well.

Fields that will require rules and the role of NII

Other than medicine and psychology, which have handled personal data, what other fields will be required to establish personal data handling rules?

SHISHIDO One is so-called social surveys: political surveys and public opinion polls, for example. Recent research has made it possible to conduct micro-analysis on these surveys, with findings like, "sending this message to this age group in this income bracket in this electorate is likely to change their voting behavior." If deeper research makes increasingly fine-grained analysis like this possible, it will be necessary to revise the rules relating to personal information laws.

Another field is research that aims for "total knowledge." Comprehensive universities, in particular, are not just

delving deeply into specific research fields, but also pursuing interdisciplinary and synthetic research aimed at achieving a total understanding of the whole of society.

An example of this might be medical economics, which studies preventive medicine and the rational management of health insurance. In both these interdisciplinary research fields, a wide range of information and wisdom must be gathered from a variety of sources. In cohort studies,*6 the objective is to obtain knowledge by collecting all kinds of data on individuals, from vaccination status to lifestyle attitudes.

This kind of interdisciplinary data movement seems ideal for a data-driven society. On the other hand, it is possible that gathering such varied data in one place in the name of research could result in a situation where specific individuals are identifiable from a dataset that was originally anonymous. We need to start thinking hard about how to address such risks.

—— How can informatics and NII help in formulating rules?

SHISHIDO Themes such as "What are data?" and "What is knowledge about data?" are at the frontiers of informatics. Informatics is becoming a core discipline that plays a very vital role in the whole of academic research.

Universities and research institutes all have their own departments of informatics or related disciplines. NII brings together researchers that straddle the boundaries of humanities and sciences. In addition to developing the field of informatics itself, I believe that NII has a role to play by contributing, through informatics, to the overall development of academic research in Japan. Without being bound by the framework of informatics, NII should strengthen its role as a platform or coordinator for enabling researchers to gather, discuss, and disseminate information.

Photography by FURUSUE, Takuya

[Glossary]

***1 = Amendment of the Act on the Protection of Personal Information:** The Act on the Protection of Personal Information was enacted in 2003, with provision for review, in principle, every three years, based on the assumption that the scope of personal information protection would expand with advances in information technology. The current law (as of September 2021) was enacted in 2015 and came into effect in 2017. It was amended further in 2020 and 2021.

***2 = Provision to third parties:** Provision of personal data held by a business operator to another party. As a rule, provision to a third party is not permissible without the consent of the data subject.

***3 = Doctor-patient confidentiality:** The obligation of a doctor not to divulge to anyone any confidential information about a patient obtained through the doctor-patient relationship.

***4 = Secrecy of communications:** Article 21, Paragraph 2 of the Constitution of Japan guarantees the confidentiality of communications between individuals (e.g., by letters, telephone calls, radio, email). Additionally, Article 4 of the Telecommunications Business Act stipulates: "(1) The confidentiality of communications handled by a telecommunications carrier must not be violated," and "(2) A person employed with a telecommunications carrier must not disclose any confidential information about another person acquired in the course of their employment. This obligation applies even after the person has ceased to work for the telecommunications carrier."

***5 = Personal Information Protection Commission (PPC):** An independent regulatory body established in 2016 to ensure the proper handling of personal information (including Specific Personal Information), taking into consideration its proper and effective use. The duties of the PPC include formulating and promoting basic policies for the protection of personal information, supervising personal information, and administrative tasks related to authorized personal information protection organizations.

***6 = Cohort study:** A longitudinal study in which two groups of people are tracked, one with and one without a defining characteristic associated with the hypothesis being tested. Typically, the morbidity and mortality of the two groups are compared.

A Word from the Interviewer

Academic institutions will be required to implement the same security control measures for personal data as private companies. This sounds like a tricky challenge for researchers. The current "no obligation" policy is an obstacle to collaboration with EU research institutions that are subject to the General Data Protection Regulation (GDPR), so this revision was inevitable. On the other hand, there are growing concerns that restrictions on data distribution on the grounds of national security, such as those arising from the recent U.S.-China conflict, will hinder international collaborative research. Keeping in mind Professor SHISHIDO's words, "Academic research aims to contribute to the development of all humanity, transcending divisions between countries," we need to continue watching critically for excessive restrictions.

ASAKAWA, Naoki Editor in Chief, Nikkei Computer

Joined Nikkei BP after earning an MSc in Physics from The University of Tokyo in 2003. In 2010 he earned an MBA from Bond University in Australia. Prior to assuming his current position, he worked as a reporter for Nikkei Electronics and Nihon Keizai Shimbun.

Q&A

What is Required of Academia Under the Amended Personal Information Law

Promoting academic research based on trust

SATOH, Ichiro
Professor, Information and Society Research Division, NII
Professor, School of Multidisciplinary Sciences, The Graduate University for Advanced Studies (SOKENDAI)

Since heading the technical working group within the Cabinet Secretariat's "Personal Data Study Group" at the time of the 2015 revision of the Act on the Protection of Personal Information, law Professor SATOH, Ichiro has been involved in almost all the major working groups that have examined amendments to the law. We asked him about the essential points to keep in mind when using personal information for academic research, with a particular focus on the 2021 amendments to the law, which will significantly impact the academic world.

Q1

What are the key points in the latest amendments to the Act on the Protection of Personal Information (hereinafter also "personal information law")?

A The current law is a revision passed in 2015, with further amendments made in 2020 and 2021. Some of the 2020 and 2021 amendments will come into effect in April 2022. The 2015 amendment introduced individual identification codes*1 for biometric data and for some identifiers; anonymously processed information,*2 which is a new data type for providing data to third parties without consent; and regulations on cross-border data transfers to other countries. Previously, a specific ministry had jurisdiction over each industry sector, but private businesses are now under the unified jurisdiction of the Personal Information Protection Commission (PPC). This is a major shift.

The 2020 amendment represented a minor change to the 2015 amendment. It mostly tightens up details. At the same time, it introduces a new system for handling pseudonymously processed information,*3 which enables more relaxed restrictions about processing data in certain ways, as long as the data are not provided to a third party.

There are changes that affect academic institutions. The right to request disclosure and cessation of use has been expanded to include not only some legal violations, such as unauthorized acquisition, but also risks of harm to the rights or legitimate interests of an individual, as well as disclosure and cessation of use of data that are only held for a short time, meaning data that need to be erased within six months. With the introduction of "personal-related information" as a data type, it became clear that even data that do not qualify as "personal information" at the premises of the data provider should be treated in the same way as prescribed for the provision of personal information to third parties if the data can be matched with personal information held by the recipient at the recipient's premises.

Q2

What amendments were made to the personal information law in 2021?

A This revision impacts significantly on the academic sector. Before the 2021 amendment of the personal information law there were different laws for the private sector, administrative agencies (central government ministries and agencies), and independent administrative corporations. Now, all these different personal information rules are integrated into a single law. Under this integrated law, the personal information protection systems of local government bodies will be subject to common nationwide rules. Overall jurisdiction for personal information protection will also be unified under the PPC. The definition of personal information is now also unified with that of the private sector.

So, what about the impact on the academic sector? To unify regulations across medicine and academia, national and public hospitals and universities, Inter-University Research Institute Corporations, and National Research & Development Agencies,

will, at least in theory, be subject to the same regulations as private universities and hospitals. National university corporations, for example, were subject to the "Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc." From now on, though, they will be subject to the same personal information law that was applied to the private sector. The blanket exemption from protection obligations that applied to personal information for academic research under the current law has also been scrapped. However, there are provisions for exemptions to specific obligations under certain conditions.

Q3

What will be the impact of all this legal unification in the 2021 amendment?

A Up to now, there were differences between the legal systems of private businesses, administrative agencies, independent administrative corporations, and local government bodies. Private universities, national universities, and public universities even used different definitions of personal information, for example. As a result of these differences, sharing data between organizations was difficult. With this unification, most of the barriers caused by such legal differences should be eliminated, for example when data are shared between national and private universities. Still, national and public university corporations, Inter-University Research Institute Corporations, and National Research & Development Agencies will need to revise their respective personal information protection regulations by April 2022, when the amendment takes effect.

Q4

How will the use of personal information for academic research change under the 2021 amendment?

A The changes will be different for private universities and national and public universities. Under the current law (2015 amendment), private universities and other private-sector academic research institutions enjoy a blanket exemption from protection obligations when handling personal information for academic research purposes. With the 2021 amendment, private-sector academic research institutions will need to implement security control measures (Article 23 of the amendment) and respond to requests from data subjects for data disclosure, etc. Independent administrative corporations, local government bodies, and local independent administrative agencies (including public universities) that conduct academic research will be subjected to the same rules that apply to private-sector academic research institutions. However, the public sector rules about data disclosure, etc., and provision of anonymously processed information will continue to apply to them. Note also that both private and public-sector academic research institutions are now required to formulate and publish their voluntary codes of practice to ensure that research involving the use of personal information is conducted appropriately.

When personal information is handled for the purpose of academic research, there may not be restrictions based on purpose of use, restrictions on the acquisition of "special care-required" personal information,*4 restrictions on provision to third parties, or other such obligations. But this is only on condition that there is no risk of illegitimate violation of individual rights or interests. When I participated in cabinet study groups and committees working on the 2021 amendment, I made the point that academic freedom should be respected, which is not to say that anything goes, as long as it's for academic purposes. I clearly stated that a proviso, such as "except if there is a risk that the rights or interests of an individual are illegitimately violated," should be included. A proviso to this effect was included in the text of the revised law. There are multiple reasons behind this inclusion: (1) certain restrictions were needed to address the "adequacy decision" requirement of the EU's GDPR (General Data Protection Regulation), which applies to academic research; (2) there had been cases of careless regard for individual rights and interests on the grounds of academic research; (3) the increasing sophistication of technology for personal data use.

Q5

What will the voluntary codes look like?

A Under the 2021 amendment, academic research institutions need to comply with the provisions of the law in relation to personal information handling for academic purposes. They need to take all measures necessary to ensure that they handle personal information appropriately. For this, they need to create and publish a voluntary code of practice. This might seem to be a new obligation for academic research institutions, but in reality, it allows for and respects the autonomous judgment of universities and other academic research institutions. As long as the institutions handle personal information in accordance with their voluntary code, their autonomy is respected. The PPC will exercise its oversight authority only when there is a risk of illegitimate violation of individual rights or interests.

Thus, academic research institutions are required to create a suitable voluntary code of practice and comply with it. Suppose that an academic research institution uses personal information for an academic purpose. Even in the case that it is permitted to use the information beyond the specified scope of use, the voluntary code will impose certain restrictions on use outside the specified purpose and the institution will need to take care to ensure that individual rights and interests are not violated illegitimately.

Some care is needed here about the interpretation of cases where there is a risk that the rights or interests of individuals are unfairly violated. Such a case could be interpreted within the narrow scope of claims for damages under civil law, but it might also be interpreted in the context of a constitutional violation. Institutions that create

a voluntary code need to understand these conditions, to ensure that the code is appropriate to their needs.

Q6

Is creating voluntary codes of practice good enough?

A

Up to now, academic research institutions have formulated codes of conduct for personal information protection and privacy as part of research ethics guidelines. But it's not enough to just establish a code; it must be followed too. The point is that personal and private information is a complex subject. So, it is difficult for an individual researcher to determine whether their research infringes on someone's rights or interests. The range of information that can be considered private is so broad that academic research would be impossible if we avoided using all such information. Therefore, as we use information that may have privacy implications, we are required to prevent or minimize privacy infringements by restricting the ways that the information can be used.

Voluntary codes of practice may inhibit research, but since the main purpose of research institutions is to perform research, they tend to prioritize research over such codes. That is why voluntary codes alone are never going to be sufficient. The time has come for academic research institutions to also develop mechanisms, including organizational governance, for monitoring and supervising the compliance of their activities with their codes of conduct and practice. Otherwise, they will struggle. So far, however, few academic research institutions have established the governance systems needed to ensure compliance with voluntary codes.

Q7

What are the key points to keep in mind regarding academic use of personal information?

A The reason behind the relaxation of some obligations relating to the academic use of personal information is that the public trusts academic research institutions and expects them to use data for the benefit of society. If that trust and hope are betrayed in any way, these relaxations may disappear. Every academic researcher needs to use data appropriately, keeping this point in mind.

Note that a detailed explanation about the academic use of personal information under the latest amendments is offered in "Big Data Pioneers Medical AI" (a new book; see p.19 of this issue).

[Glossary]

***1 = Individual identification code:** A code obtained by digital conversion of any feature of a specific individual's body, such as fingerprints, palm prints, DNA, face, finger veins, gait, and voice print, and specified by Cabinet Order as an identifier for use in personal identification, e.g., for the My Number system, passports, medical insurance, pensions, or driver's licenses.

***2 = Anonymously processed information:** Information that has been processed in accordance with standards based on laws and regulations to delete any descriptions or individual identification codes that could be used to identify specific individuals, such that it is impossible to determine the subject of the information. Such information can be freely used without specifying the purpose of use or obtaining the consent of the data subject.

***3 = Pseudonymously processed information:** Information about individuals obtained by processing personal information according to standards based on laws and regulations, such that the subject of the information cannot be identified without cross-referencing with other information. Such information can be used solely for data analysis within an organization; it cannot be provided to a third party.

***4 = Special care-required personal information:** Any description that requires special care in handling to avoid unfair discrimination, prejudice, or other disadvantage to an individual. This can include race, beliefs, social status, criminal history, the fact of having been the victim of a crime, and medical history.

SATOH, Ichiro

Involvement in the Act on the Protection of Personal Information

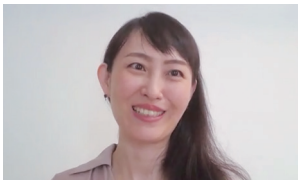
Professor SATOH, Ichiro is a system software specialist, but in 2015 he became involved in the process of revising the Act on the Protection of Personal Information as a member and leader of Cabinet Secretariat working groups. Later, he participated in the main working groups tasked with revising personal information laws for administrative agencies and independent administrative corporations, as well as on the 2021 amendment of the Act on the Protection of Personal Information. "I was the only person involved in almost all the major working groups, including legal scholars. This was a very valuable experience for me, although I felt the weight of my responsibility keenly," he said. Some of the details of Prof. SATOH's involvement in these legal amendments are recounted in the book "Fighting GAFA's Expansion: Digital Defeat, What did Kasumigaseki do?" by WAKAE, Masako (editorial board member of the Yomiuri Shimbun), published by Chuokoron Shinsha.

Roundtable

Enhancing Competitiveness through Stronger Governance

Studying with the “Guidebook on Corporate Governance for Privacy”

DOI, Miwako
Auditor, National Institute of Information and Communications Technology (NICT) / Executive Vice President, Tohoku University / Executive Director, Nara Institute of Science and Technology



HIOKI, Tomomi
Lawyer, Miura & Partners / Auditor, The Information Network Law Association

SATOH, Ichiro
Professor, Information and Society Research Division, NII / Professor, School of Multidisciplinary Sciences, The Graduate University for Advanced Studies (SOKENDAI)

Interviewer:
MURAYAMA, Keiichi
Commentator, Nikkei Inc.

As data utilization becomes increasingly important for social and economic innovation, a move has emerged to compel companies and research institutions to create a privacy governance system for handling data. The Corporate Privacy Governance Model Study Group of the Data Distribution Promotion Working Group under the IoT Acceleration Consortium of the Ministry of Economy, Trade and Industry (METI) and the Ministry of Internal Affairs and Communications (MIC), chaired by Prof. SATOH, Ichiro of NII, has prepared a guidebook about privacy governance, to urge industry to address this challenge proactively. How should privacy governance be understood and tackled?

The reason privacy governance is necessary

—— Why do we need privacy governance now?

SATOH The data that companies use for business include a massive amount of privacy-sensitive information. The Act on the Protection of Personal Information (hereinafter also “personal information law”) protects privacy indirectly, but this Japanese law is quite loose by global standards. Compared to the EU’s GDPR (General Data Protection Regulation) and the legal framework of the U.S. state of California, it has a narrow scope of data protection. Overseas, various types of personal data*1 are protected, including the “cookies” used to temporarily store connection-related information about individual website visitors, but protection in Japan is more limited. In today’s world, companies need to think of doing more than just complying with the personal information law. Furthermore, data use is very central to the business of many companies, so if left unchecked, they would end up using more and more private information. A method of putting a brake on this tendency is therefore required.

The method our study group proposed for this function is called the “Guidebook on Corporate Governance for Privacy in Digital Transformation (DX)”*2 (hereinafter also “privacy guidebook”). The intention was to offer guidelines on how to securely utilize privacy-sensitive data and set up data protection systems for this purpose. This solution requires an officer to take responsibility for data privacy within each company, along with appropriate allocation of human and budgetary resources. Since an internal perspective alone is inadequate, we want companies to set up third-party committees and a system for communicating with the public.

However, we wanted to provide a minimal set of requirements that even small companies can implement easily. The numerous companies that don’t handle any personal information except for employee data can adopt our system with ease. Still, we hope that every company will implement the system in the way that best fits their situation.

The role of the privacy guidebook

—— Are some companies struggling to understand the extent to which they are allowed to use data because of privacy protection?

DOI I see a gap between companies that want to utilize data for generating profit and those that don’t. The first type needs to comply not just with domestic rules, but also with overseas

mechanisms like the GDPR. They also need to think about appropriate data storage and cloud use. There's a lot to worry about.

Corporate governance and personal information protection are just two of things that crop up. Many companies can barely keep up as one thing after another needs to be addressed. Although we've published a privacy guidebook, it will be tough to see how many companies will get onboard with it. Larger companies with plenty of human resources will be conscious of their reputation, but small companies, on the other hand, may not even be fully aware of whether they have usable data. We need to start thinking from these basics.

Risk management is essentially about anticipating and preparing for problems that might arise in the course of business. In Japan, though, too many companies and universities still engage in "follow-up" risk management, which means setting things right after the event. It is vital to create a risk map and conduct anticipatory risk management. For privacy governance too, it's important to get companies to recognize that following the guidebook will benefit their management.

——Is this viewpoint that "it's positive for business" reflected in the guidebook?

HIOKI We want to take privacy governance initiatives to the point where they are not a cost, but rather something that makes a company stronger and more competitive. The idea is that a company that can't be trusted will not find customers for its products and services, or business partners for collaboration. For start-ups, data handling could even affect their ability to raise funds.

Discussions of internal controls in companies tend to focus on information security, with privacy taking a back seat. Of course, you could run a negative campaign, saying "If you don't take action, your executives will be held accountable," but that doesn't provide a positive incentive. This guidebook is designed to increase corporate value.

From risk avoidance to risk reduction and acceptance

—— Maybe compliance with laws and regulations alone is not enough. Is a larger framework needed?

SATOH The scope of personal information is fixed, so it's clear what needs to be handled in accordance with laws and regulations. In contrast, privacy is a highly subjective concept, with a broad and vague scope. Every company needs to think about what kind of privacy-sensitive information it possesses and determine how it should be used. Privacy is decisively different from personal information in the sense that businesses need to independently assess a much wider scope of information. I want to see privacy governance practiced as a way of effectively conducting these kinds of assessment.

The guidebook urges companies to pay attention to privacy risks and to address them. When it comes to risk, Japanese companies tend to focus on "avoidance" or "transformation," whereas overseas companies tend to reduce risks by adapting the way they use data. They often maintain their existing business practices after obtaining the understanding of consumers through effective communication. Or in other words, they resolve the problem through "acceptance." This tendency is one of the underlying reasons that Japanese companies have fallen behind foreign companies in business. They tend fall into one extreme or another, either giving up on data utilization altogether, or else insisting that privacy-sensitive information should be used without restrictions for research purposes, because of, for example, the need to combat COVID-19. In reality, data use and data protection can coexist. It is up to researchers to think of ways to achieve both. Privacy governance should help with this.

HIOKI In the past, the main concerns of companies were probably compliance with laws and regulations and dealing with flaming risks, but with advances in data utilization and the digital transformation of society, these concerns have expanded to include the trust and loyalty of consumers. A strong governance structure is now a vital element in fostering trust. When a problem arises, the legal department may not be able to resolve it alone, or it may be totally unaware of something that the business unit is pursuing. And this situation could lead to a PR issue.

DOI, Miwako

As a specialist in human interfaces, she has engaged in research and development into Japanese-language word processing, machine translation, VR, gesture interfaces, wayfinding services, wearable computers, and network robots. She currently serves as an auditor at the National Institute of Information and Communications Technology (NICT); Executive Vice President at Tohoku University; Executive Director of Nara Institute of Science and Technology; professor in residence at Osaka University; visiting professor at Tokyo University of Agriculture and Technology; and a visiting professor at Osaka University of Arts.

HIOKI, Tomomi

As part of the National Strategy Office of Information and Communications Technology (Cabinet Secretariat), she led the effort to draft the 2015 amendment of the Act on the Protection of Personal Information. Currently, she works as a lawyer in business and regulatory practices relating to data. She is involved in the Data Governance Research Unit at The University of Tokyo's Institute for Future Initiatives as a researcher. She is also a member of the Corporate Privacy Governance Model Study Group of the Data Distribution Promotion Working Group under the IoT Acceleration Consortium of the Ministry of Economy, Trade and Industry (METI) and the Ministry of Internal Affairs and Communications (MIC).

With this kind of broader perspective, interest in privacy governance seems to be growing.

Indicators as a tool to enhance corporate value

Do you have any tips on how to accelerate this shift?

DOI In the past, environmental issues were really of interest only to companies that directly discharged pollutants or emitted carbon dioxide (CO2), but with the goal of carbon neutrality, more and more companies need to concern themselves with the topic. A key point here is that environmental commitments can be formulated as quantitative goals or KPIs (Key Performance Indicators), at least to some extent, as in, "We can become carbon neutral if we meet this target." It's possible, for example, to calculate the reduction in CO2 emissions when fluorescent lamps are replaced with LEDs. This is the level at which management needs to confront the challenge.

It would be easier to tackle privacy governance if we could use indicators like KPIs to tell us how to handle data. Using indicators would help everyone to think positively about how to treat the data they possess.

Against the backdrop of economic security discussions, storing data in overseas clouds, which was previously acceptable, is no longer permitted. This means that we cannot use risk maps created in the past to deal with a current situation. Imagine if a consulting firm came up with a way of supporting privacy governance in combination with security. That idea could be a useful tool for increasing corporate value. If privacy becomes a business opportunity for consulting firms, like the environment has become, incentives would work. So, why not bring together companies capable of exploring this idea?

Academic research institutions and privacy governance

The concept of privacy governance is also very important for academic research institutes and universities.

SATOH There was a time when research on privacy-sensitive information was concentrated in particular disciplines, such as medicine. More recently, though informatics and sociology are also dealing directly with privacy and personal information. Think, for example, of using sensors to study human movement. A wide variety of privacy-sensitive information is being used across all of academia.

The 2021 amendment of Japan's personal information law has brought significant changes to the rules for academic use of personal information. Academic research institutions will be required to formulate and publish voluntary rules, and even academic use will now be subject to a prohibition on illegitimately violating the rights or interests of individuals. Many research institutions in Japan have created personal information protection regulations and ethical guidelines, which are typically used to screen research projects before they begin. After a project is approved, though, it is not adequately monitored. Like companies, academic research institutions now need to create a system to ensure that they follow their voluntary rules and ethical guidelines. So, the guidebook should be of value to academic institutions too.

Challenges in establishing systems in academia

Do you see any momentum toward building governance systems?

DOI The National Institute of Information and Communications Technology (NICT) has set up a committee on the handling of personal data, made up of lawyers and experts, which advises us on every study we work on. Although moves like this are afoot, universities need to catch up. Given that subsidies for operating expenses are declining, it's not easy to address this need, which requires the allocation of human resources. At large universities, each department has its own unique character, so a top-down approach tends to be ineffective. Up to now, they have been able to use data for academic purposes very freely. There has probably been a lack of re-education about this impending change.

SATOH From the standpoint of researchers who use data to generate findings, restrictions on data use amount to impediments to research activities. Some researchers even regard such restrictions as violations of academic freedom. The free use of data for academic research is also supported by public expectations of academia. Or in other words, data use is considered permissible for research that benefits the world. However, if researchers do not handle personal data appropriately, or if they look on any data use as an inherent right, they will lose public trust, making their research activities impossible. It is important for researchers to discipline themselves on the issue of privacy.

For about six years, I was in charge of ethically screening research projects at NII. Any restrictions on the acquisition and use of data arising from personal information laws or ethical considerations were met with strong opposition and resentment. Any system that requires researchers to review the data handling of other researchers will have limits. NII's research ethics review process is rigorously implemented, and if there is a problem the project is not allowed to proceed. However, in light of the growing intensity of data use, I

think the organization now needs to establish a privacy governance system, investing sufficient amounts of money, time, and effort to make it work effectively.

HIOKI It's difficult to exercise control uniformly over a whole university, because every department and section tends to deal with problems differently. Even within a single medical faculty, arguments vary widely, from "why can't we use data for the advancement of medicine" to views that stress the importance of privacy. Everyone has their own opinion. Under these circumstances, risk management will be difficult.

We also need to keep an eye on international trends. If Japan is the only country that cannot access databases created in collaboration by overseas research institutes, that is a problem. If our privacy policy is at odds with the policies of other countries, researchers may get messages like, "this dataset was not collected properly, so it cannot be used." Is it enough to have a domestic standard of privacy in Japan? This is a serious question.

To change attitudes, a mechanism and business use are needed

How can we change the attitude of research institutes and universities?

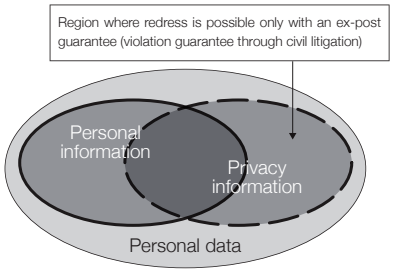
SATOH Even if we ask universities and research institutions to work on privacy governance, they will refuse to restrict their own research. Therefore, we need some way to get the parties that finance research to impose certain restrictions. When the global genome research project was conducted, a few percent of the research budget was reserved for ethics and data protection. If companies adopt privacy governance, they can then compel universities to take appropriate action when working with them on joint research. We need to do something before we lose public trust.

DOI One approach to building trust is to go beyond academia and think about commercial data use. If a company achieves commercial success by using data from a university, a privacy policy could be imposed on them as a condition of use. If best practices like this emerge, they can be widely shared. If we create a model that benefits all three sides—data providers, researchers, and industry— that would be a great start.

HIOKI We have the example of Osaka University*3 too, which pays careful attention to privacy risks when it makes databases available to companies, as part of its goal of implementing its research findings for social benefit. In fields of data utilization, research and development are closely linked with social implementation. Research institutes can tackle privacy governance with a view that data will eventually be used commercially. This is one approach I think.

[Glossary]

***1 = Personal data:** Includes information about personal attributes, movement/behavior/purchase history, and personal information collected from wearable devices. Also includes people flow information and product information processed so that specific individuals cannot be identified, based on anonymously processed information as provided for under the latest amendment of the Act on the Protection of Personal Information. In addition to personal information, this term also refers to a wide range of information that can be correlated to individual persons, including information that may vaguely be considered to constitute personal information.



***2 = Guidebook on Corporate Governance for Privacy in Digital Transformation (DX) (Ver. 1.0):** https://www.meti.go.jp/pre

***3 = Initiative for Life Design Innovation (iLDi):** https://www.ids.osaka-u.ac.jp/ildi/

A Word from the Interviewer

As the use of personal data for online advertising has been put on hold, our data-intensive society is at a turning point. As this roundtable discussion shows, there are thorny questions to face. It would be ideal if trustworthy companies and research institutions were free to collect data and generate genuine value from it. Thus, as an essential precondition for a more competitive and vigorous society, we need to build a system for fairly evaluating organizations that are serious about privacy governance.

MURAYAMA, Keiichi Commentator, Nikkei Inc.

Graduated from the School of Law at Tohoku University in 1992 before joining Nikkei Inc., where he has covered IT, electronics, automobiles, healthcare, and other fields as a reporter in the Industry Department. After stints studying at Harvard University and working in the Nikkei's Silicon Valley Bureau, he became a member of the editorial board in 2012 and has also served as an editorialist since 2015. He has been in his current position since 2017. His main focus is IT and startups. Recent publications include "STARTUP – The Reality of Entrepreneurs."

Contribution

Personal Information Protection in Academic Research and Foreign Data Protection Laws

ITAKURA, Yoichiro
Lawyer, Hikari Sogoh Law Offices / Visiting Professor, NII

1 Introduction

The protection of personal information in the field of academic research is causing academic research institutions many headaches. In particular, the public-sector research institutions that were hit directly by amendments in 2020*1 and 2021*2 to the Act on the Protection of Personal Information (Act No. 57 of 2003, hereinafter also "personal information law") are currently scrambling to adapt to new rules. On top of this, academic research institutions engage in many international activities. Despite the curtailment of physical movement during the COVID-19 crisis, online academic activities continued vigorously. Consequently, international data exchanges may be happening more than ever before.

This article discusses the issues of personal information protection in academic research, focusing on the points to keep in mind in relation to foreign data protection laws.*3

2 Situations to be careful about in connection with foreign data protection laws

1 Introduction

There are basically two kinds of situations to be careful about when it comes to foreign data protection laws, whether in academic research or other fields. The first is when the data protection laws of a foreign country apply to academic research institutions not located in that country (e.g., a university in Japan). (This is known as "extraterritorial applicability.") The other situation is when data are transferred from a country to an institution located in a different country or region (e.g., Japan). (This is known as "cross-border data transfer.") Now, since there are countless foreign data protection laws in existence, which ones should you worry about?

Basically, you need to be aware of all the data protection laws of the countries you interact with, but the most useful one to know about is the EU's General Data Protection Regulation (GDPR*4), which is known for its heavy financial penalties. The GDPR also applies to academic research institutions in many cases*5 and it has served as the model for data laws in other countries (e.g., Switzerland, Thailand). It may also be worth paying attention to U.S. data protection laws, although the U.S. does not have comprehensive data protection laws at the federal level.*6 At the state level, the California Consumer Privacy Act (CCPA*7) is important, with more and more states adopting laws similar to the CCPA. However, we hear little about the international application of these state laws. In the following discussion, I will take up the GDPR as an example to outline the main points to keep in mind regarding extraterritorial applicability and cross-border data transfers.

2-1 Extraterritorial applicability

Article 3(2)(a) and (b) of the GDPR stipulate that the GDPR applies to a controller or processor not based in the EU in two cases: (a) when goods or services (whether paid or unpaid) are offered to a data subject in the EU and (b) the monitoring of a data subject's behavior when this takes place within the EU. In both cases, the key question is whether the data subject within the EU is targeted. This is known as the "targeting criterion."

For example, if an academic research institution in Japan organizes an online information session about study abroad in German for students in Germany, this would fall under (a). Any personal data of students collected for such an information session need to be handled according to the GDPR rules. The applicability of (a) is judged not only based on whether a service is offered, but also on whether there is an intention to offer one. This means that if such an event were held in English for a worldwide audience, the GDPR would not be applicable. It does apply, however, if a specific country in the EU is "targeted." Now consider the case of an app that is distributed from Japan and used for an experiment in which the location and health information about EU data subjects is collected on an ongoing basis. This would fall the under monitoring of behavior in (b).

As soon as the GDPR applies extraterritorially, all relevant personal data must comply with all the rules of the GDPR. These include obligations relating to the exercise of specific rights such as the right to erasure ("right to be forgotten") and the right to data portability, both of which are well known in Japan. There is also an obligation to have an EU representative.

2-2 Are there any exceptions to the GDPR rules?

Even if the GDPR is applicable, we should know if there are any kinds of exceptions for academic research. Even under Japan's personal information law, when an academic research institution handles personal information for academic research purposes, some obligations are not applicable, out of consideration for academic freedom. (The 2021 amendment modifies this exemption somewhat.) There are two provisions in the GDPR that allow exceptions for academic research.

One is Article 85 ("Processing and freedom of expression and information"), which states in paragraph 1 that "Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression." More specifically, paragraph 2 states that "For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from CHAPTER II (principles), CHAPTER III (rights of the data subject), CHAPTER IV (controller and processor), CHAPTER V (transfer of personal data to third countries or international organisations), CHAPTER VI (independent supervisory authorities), CHAPTER VII (cooperation and consistency) and CHAPTER IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information." Here, it is basically saying that member states must establish exceptions or special provisions to reconcile academic freedom of expression with the GDPR.

The other provision relating to exceptions is Article 89 ("Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes"), which states in paragraph 1 that "Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner." Then, more specifically, paragraph 2 states, "Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes." Thus, the EU or a member state "may" provide for special exceptions to provisions relating to the rights of data subjects under the GDPR "where personal data are processed for scientific or historical research purposes or statistical purposes."

Like this, EU member states can establish necessary exceptions relating to the processing of personal data out of consideration for academic freedom of expression, e.g., to publish academic research. Even if no act of expression is involved, if personal data are processed for scientific or historical research purposes or statistical purposes, the EU or member states may establish exceptions in relation to the rights of data subjects under the GDPR. And, more specifically, any exception established in a member state on the grounds of freedom of academic expression or for scientific research purposes must be examined to check whether it applies extraterritorially.

For example, in Article 43(1) of the Irish Data Protection Act*8 the requirement for exemption on the grounds of academic freedom of expression is qualified with the words, "where, having regard to the importance of the right of freedom of expression and information in a democratic society, compliance with the provision would be incompatible with such purposes." Thus, a specific comparative consideration is required. Article 42 also allows for exemptions from the provisions of the GDPR relating to the processing of personal data for the purposes of scientific or historical research or for statistical purposes, but qualifies this with, "Where the purposes […] can be fulfilled by processing which does not permit, or no longer permits, identification of data subjects, the processing of information for such purposes shall be fulfilled in that manner." (paragraph 3). There is an additional requirement that this is mandatory if the purpose can be achieved even with anonymization.

As explained above, even when the GDPR applies extraterritorially to academic research institutions, exceptions for academic research can be expected. However, it is necessary to check the details of such exceptions in the laws of the relevant EU member states. What's more, if it comes down to a comparative weighing under interpretation of the relevant member state law, it may be difficult to eliminate the risk of noncompliance.*9

3 Cross-border data transfers

While extraterritorial applicability is often an issue when approach is from Japan to a foreign country, cross-border data transfer tends to be an issue when data are transferred from another country to Japan. The GDPR prohibits the processing of personal data and cross-border transfers in principle, adopting a system that requires legitimization (e.g., consent) in both cases. The principal grounds for legitimization

of cross-border transfers under the GDPR is "adequacy decision." This allows bulk cross-border data transfers to countries or territories with an adequate level of data protection measures.

Japan has obtained adequacy certification from EU, but the scope of this certification is constrained by the applicability of Japan's personal information law. The research activities of private universities, which are exempted from provisions of the personal information law, as well as national university corporations, National Research & Development Agencies, and Inter-University Research Institute Corporations including NII, which are not even subject to the personal information law at present (they are instead subject to the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (Act No. 59 of 2003) cannot conduct cross-border data transfers on the grounds of adequacy decision. This point is expected to be resolved with the 2021 amendment to the personal information law, but until the amendment comes into effect in the spring of 2022, the only alternatives are to use the Standard Contractual Clauses (SCC), a model approved by the EU, or to obtain consent for cross-border transfer, which is not recommended for repeated and continual data transfers.

It is up to the EU counterpart to decide grounds for cross-border data transfers, but if a Japanese academic research institution receives data without suitable grounds for legitimization, it may be violating the GDPR. It is therefore necessary to inquire about this issue when examining joint research agreements.

Finally, although it is not an issue with the GDPR, countries with undemocratic data protection or cybersecurity legal systems, such as China, Russia, and Vietnam, may mandate that data and other information about their citizens be stored within the country (data localization rules). This is a more onerous requirement than cross-border data transfer rules, as the grounds for exemption are generally narrow. (Some countries impose both kinds of obligations.) It is important to be very careful when conducting joint research with academic research institutions in one of these countries.

[Glossary]

*1 = The Amendment Act of the Act on the Protection of Personal Information, etc. (Act No. 44 of 2020). This was the first revision based on the so-called "triennial review."

*2 = Amendment based on the Act on Adjusting Laws Related to Forming a Digital Society (Act No. 37 of 2021). Includes unification of personal information protection system between public and private sectors, changes to laws applicable to academic research institutions (basically, they are now subject to the same obligations in relation to handling personal information as business operators), and modifications relating to exceptions for academic purposes.

*3 = For details, please refer to the "Report on a Survey and Analysis of Trends and Future Issues in the Handling of Domestic and Foreign Personal Data by National Research & Development Agencies and National University Corporations for Research Purposes" (March 2021) (an initiative commissioned by MEXT in FY2020) by the National Graduate Institute for Policy Studies.

*4 = GDPR: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).

*5 = An example of Poland's data protection agency imposing a fine on a university for a data breach notification violation (failure to report a breach). https://edpb.europa.eu/news/national-news/2021/polish-dpa-university-fined-lackdata-breach-notifications_en.

*6 = For more details about federal data protection laws in the U.S., see "Federal Trade Commission Privacy Law and Policy," by Chris Hoofnagle, also translated into Japanese by MIYASHITA, Hiroshi et al. (Keiso Shobo, 2018).

*7 = CCPA:California Consumer Privacy Act of 2018.

*8 = Irish Data Protection Act (Act No. 7 of 2018).

*9 = For more details, see the report cited in *3 above; also ITAKURA, Yoichiro and TERADA, Mayu, "Analysis of Academic Research Exclusion Clause in the General Data Protection Regulation (GDPR) of the European Union," IPSJ Research Report on Electronic Intellectual Property and Social Infrastructure (EIP) 2019-EIP-84, Vo. 6, P. 1; ITAKURA, Yoichiro and TERADA, Mayu, "Trends in Academic Research Exclusion of the Implementation Laws of Member Countries in the General Data Protection Regulation (GDPR) of the European Union," IPSJ Research Report, EIP, 2018-EIP-80, Vol. 7, P. 1; and IKEGAI, Naoto, "Exemptions to the EU Data Protection Law for Academic and Research Purposes" (June 16, 2020), [Ref. 1] for the 3rd Conference on the Review of the Personal Data Protection System (June 16, 2020).

ITAKURA, Yoichiro

Graduated from the Faculty of Policy Management of Keio University in 2002, completed a Master's degree program in the Department of Social Informatics at the Kyoto University Graduate School of Informatics in 2004, and graduated from the Keio University Law School in 2007. He began working as a lawyer in 2008 (Hikari Sogoh Law Offices). After assignment to the Consumer Affairs Agency (as a policy planning expert in the Office of Personal Information Protection, Legal System Planning Division), he has served as a partner in the law firm since April 2016. Since May 2018, he has also served as a visiting professor at NII.

NII NEWS TOPICS

News & Topics　　Period: April 1 (Thu.) to August 31 (Tue.), 2021

News Releases

■ July 16, 2021

JDCat, a comprehensive data catalog for the humanities and social sciences, begins operation.

—Humanities and social science data are now searchable for use in research, education, and policymaking.

■ July 13, 2021

“Guerrilla rainstorm” alert system uses “Fugaku” supercomputer

—Real-time verification trial starts in the Tokyo metro area with updates every 30 seconds.

■ July 1, 2021

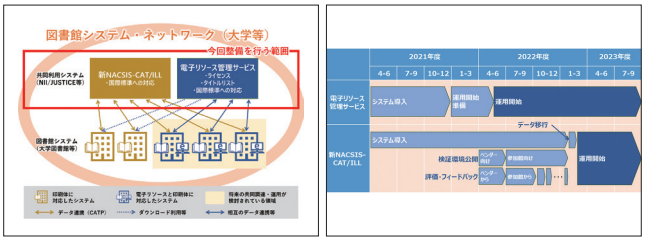
New Global Research Center for Synthetic Media is set up to study AI video and audio.

—Promotes research on AI video creation, fake media detection, and media credibility.

■ June 17, 2021

Academic information system for university libraries has been updated after 36 years.

—Catalog location information services adapted to the increasing digitalization of academic materials to be launched gradually from 2022



New library system network diagram (left) using a cloud environment and a system capable of handling electronic and printed resources without distinction, along with a schedule for the start of operation (right).

■ June 16, 2021

A series of presentations on the use of informatics for COVID-19 research at NII Open House

—NII Open House will be held online on Friday June 18 and Saturday June 19.

■ May 31, 2021

Open House keynote speech by HORITA, Tatsuya (right), Professor, Graduate School of Information Sciences, Tohoku University, with KITSUREGAWA, Masaru (left), Director-General, NII

Online conversation about the challenges of digital transformation in elementary and secondary schools between HORITA, Tatsuya, a professor at Tohoku University, and the Director-General at NII

—Keynote speech for the NII Open House on data-driven education and the GIGA School Concept

■ May 26, 2021

Development of a method for automatically converting control software to ensure safe operation, even when used with sensors that make measurement errors

—Ensuring the safety of real-world systems designed assuming the ideal that “there are no errors”

■ May 25, 2021

Learn programmatic thinking at the NII Open House

—On June 19 “Computer Science Parks” at an online venue and at satellite venues in Toyohashi, Himeji, and Hamamatsu

■ April 27, 2021

New host-switch graph section with more specific condition settings!

—The “Graph Golf” competition to discover network configurations for future supercomputers is being revived.

★ Entries will be accepted until Monday October 11, 2021!

■ April 13, 2021

RIKEN and NII sign collaboration and cooperation agreement.

■ April 12, 2021

Development of technology for automatically finding simulation settings that are difficult to test

—Automates searching of settings for “diverse situations” faced in autonomous driving.

Awards

■ August 3, 2021

SUZUKI, Chikahiko (Project Researcher at ROIS; Project Assistant Professor at Center for Open Data in the Humanities (CODH) Joint Support Center for Data Science Research) received the Yamashita Memorial Research Award 2021 from the Information Processing Society of Japan for his paper.

■ July 22, 2021

KAWARABAYASHI, Ken’ichi (Professor at Principles of Informatics Research Division) and his team’s paper received the Fulkerson Prize.

■ June 21, 2021

IINO, Nami (Project Researcher at Principles of Informatics Research Division) and her team’s paper received the JSAI Incentive Award for 2020 from the Japanese Society for Artificial Intelligence.

■ June 21, 2021

SAKAIDA, Rui (a former Visiting Researcher at NII) received the JSAI Incentive Award at the 89th Special Interest Group on Spoken Language Understanding and Dialogue Processing (SLUD) of the Japanese Society for Artificial Intelligence.

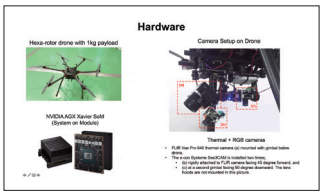
■ June 15, 2021

JI, Yusheng (Professor at Information Systems Architecture Research Division) and her team’s paper received an Outstanding Paper Award from the IEEE Communications Society.

■ June 8, 2021
HASHIZUME, Hiromichi (Professor at Information Systems Architecture Research Division) and his team's paper received the IPSJ Outstanding Paper Award 2020 from the Information Processing Society of Japan.
■ April 30, 2021
KATO, Shuhei (PhD, March 2021, Department of Informatics, SOKENDAI (Yamagishi Lab)) received an Excellence Award in SOTSURON OPEN AWARD 2021 for his doctoral thesis.

NII Information

■ August 30, 2021
Release of "miwo," an AI-based app for recognizing kuzushiji (characters written in cursive style).
■ August 24, 2021
Professor Helmut Prendinger gives a special class for high schoolers.

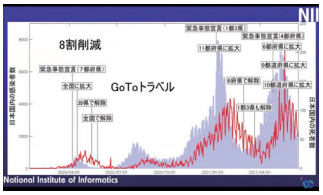



Professor Prendinger (left) gave a special online class at Tokyo Metropolitan Tama High School of Science and Technology, and his lecture slide titled "Drone × AI" (right) shows how AI is used with drones.

■ July 12, 2021
The Japanese Multi-speaker Audio Book Corpus (J-MAC) becomes available.
■ July 28, 2021
NII publishes its FY2021 Overview (Japanese version).
■ June 17, 2021
The "Japanese Kamishibai (storytelling with pictures) and Audiobook Corpus" (J-KAC) becomes available.
■ June 1, 2021
The "Kogakuin University Japanese Sign Language Multi-Dimensional Database" (KoSign) is released.
■ May 6, 2021
PR magazine "NII Today" No. 91 "NII Research Data Cloud Goes Full-Scale" is published.
■ April 9, 2021
NII publishes NII FY2021 Outline (Japanese version).
■ April 7, 2021
"NII SEEDs 2021: Creating Innovation and Future Value Through Informatics" is published.

Events www.nii.ac.jp/event/2021

■ August 20, 2021
The 38th Cyber Symposium on Online Education and Digital Transformation (DX) at Universities and Other Institutions, aka "DX Symposium for Educational Institutions"
■ July 30, 2021
37th DX Symposium for Educational Institutions
■ July 17, 2021
Meeting to commemorate Dr. SAKAUCHI, Masao
■ July 9, 2021
36th DX Symposium for Educational Institutions
■ July 6 to 8, 2021
NII Open Forum for Academic Information Infrastructure 2021
■ June 25, 2021
35th DX Symposium for Educational Institutions
■ June 19, 2021
Information Session for Department of Informatics, School of Multidisciplinary Sciences, SOKENDAI
■ June 18 to 19, 2021
NII Open House 2021 (presentations of research findings, open to the public)



"A Look Back at Human Flows in the Days of COVID-19" by Associate Professor MIZUNO, Takayuki of NII from the "COVID-19-related Research X Rounds" on June 18 (left) and children paying a game of "multiplication table dice" at the "Computer Science Park" for beginners on June 19 (right)

■ June 14-19, 2021
Japan Open Science Summit (JOSS2021)
■ June 11, 2021
34th DX Symposium for Educational Institutions
■ May 28, 2021
33rd DX Symposium for Educational Institutions
■ May 14, 2021
32nd DX Symposium for Educational Institutions
■ April 23, 2021
31st DX Symposium for Educational Institutions

New Publication Guide

"Big Data Pioneers Medical AI"
(NII Series 24)
Medical Bigdata Research Center, NII (ed.)
SATOH, Shin'ichi et al.
Setting up and operating research platforms is important for applying AI to the medical field and maintaining and improving the level of services. This book reviews the history of AI and explains the research platforms in Japan, to present the issues of medical AI and research trends toward their resolution.
ISBN 978-4-621-05390-4 (C0355)
Scheduled for release in October 2021

We want your feedback!

NII Today has been renewed! To help us improve the magazine further, please tell us what you think about the magazine, using the URL below or the QR code on the left. We look forward to hearing from you.

www.nii.ac.jp/today/iken

Bit (NII Character)

Essay

A Town Where Everyone Knows Everyone and a World in which People Chat Intimately with Electronic Devices

OKADA, Hitoshi
Associate Professor, Information and Society Research Division, NII
Associate Professor, School of Multidisciplinary Sciences, SOKENDAI

More than a decade back now, I was doing some research on local currency initiatives, using a participatory fieldwork approach. When I heard about a rural town that was planning to launch an electronic local currency using official ID cards, I immediately headed off to visit the place with a professor from a local university.

The town was rich in natural resources and beauty and surrounded by deep forests. We were guided around by a local. He had grown up in the town and was now in charge of national projects at the town office. We toured some stores that planned to accept the electronic local currency and other facilities that were taking part in the trial. A doubt suddenly struck me. The national government had only just begun issuing official ID cards, even in the big cities. And the adoption rate was still low. I wondered how many people in this town had an ID card.

The answer I got was unexpectedly precise. “Well, there’s the section chief, myself, Kiyotaka-kun, and the cram school teacher. That’s it, I think.” I asked him if this meant that everyone at the town office knew who had a card. “Yes,” he confirmed. “They could also tell you the names of the cows at the farm we just visited. You wouldn’t have any problems around here without a card.”

There was no way to remain anonymous in this little community. People all knew each other and most of the economic activity was done face to face, using real names. Many people even shared the same surname, so everyone knew each other’s full name. When we got back to the town office, I was greeted by the section chief and “Kiyotaka-kun,” two of the reported ID cardholders. Everyone in the office was calling the young guy who took us around by his name in a very friendly manner.

Much time has passed since then. In today’s world we are interacting more and more with devices that we address casually by a nickname. These “electronic friends” know our tastes in music and shopping habit and recommend things that we wouldn’t come up with on our own. All those memories that were once shared within a small, local community are now amassed as data by giant Internet platforms.

Some people think that chatting intimately with a machine is cute. Others see it as an invasion of privacy. In fact, how much we trust others with information about ourselves depends on the context, i.e., on the purpose of collecting the information.

When we choose an action, we subconsciously weigh up multiple factors against each other. There is a technique called conjoint analysis that is used to visualize this kind of process. Studies have revealed that some people do not take part in actions that benefit a particular person, yet they are very willing to cooperate in the public interest.

Who should we trust with information about ourselves? It all depends on our relationships with others. Whereas local communities offer a sense of security with a visible face, the big data platforms are directing a masked theater performance.

Small town life in a rural landscape on one hand, and chatting casually with electronic devices on the other hint at two contrasting possible futures. Current research on the trinity of laws, technologies, and trust is striving to paint a picture of our society a few more years down the road.

(All the personal names in the text are pseudonyms.)

Weaving Information into Knowledge
NII
National Institute of Informatics News [NII Today] No. 92 Sep. 2021
Published by National Institute of Informatics, Research Organization of Information and Systems
Address: National Center of Sciences,2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430
Contact: Publicity Team, Planning Division, General Affairs Department
TEL: +81-3-4212-2028 FAX: +81-3-4212-2150
E-mail: kouhou@nii.ac.jp

Publisher: KITSUREGAWA, Masaru
Editorial Committee Chair: KAWARABAYASHI, Ken-ichi
Editorial Supervisor: SATOH, Ichiro
Editorial Committee Member: IKEHATA, Satoshi; KANEKO, Megumi; KOMIYAMA, Yusuke; TAKEFUSA, Atsuko; MIZUNO, Takayuki
Production: TAINAKA, Madoka; IKEDA, Akiko/ KATAYOSE, Masashi (Sci-Tech Communications Inc.)
Design and DTP: KURAHASHI, Hiro (MATZDA OFFICE CO. LTD.)
Cover illustration: ICHIMURA, Joe