Rebuilding Broken Japanese Consumer Trust : Applying the EU's Privacy Impact Assessment to a Japanese Context

Tomas Dexters *

Introduction

While for the average consumer data and especially personal data is little more than a by-product of their everyday lives, it is hard to understate its importance for some actors. Many of the larger tech companies rely heavily on advertisement as a source of revenue, the personalization of which relies on personal data. Companies thus have a motivation to gather as much personal data as possible to enhance accuracy in targeted advertising. This runs counter to the interests of many consumers, who are usually forced to put up with personal data processing to make use of various services. Legal frameworks are the main means of protecting consumers. But that is not to say that consumers themselves have no means to alter the equation to their advantage. Voting with your wallet, as well as limiting participation are proactive means of consumer protection. For larger tech companies like Google or Apple, consumers are left with little choice but to sacrifice their personal data for using various services they cannot receive elsewhere. Companies that do not dominate a market, however, are likely to be more wary of consumers not wanting to give up their personal information.

If consumers don't trust a service provider and the service offered is not seen as critical, consumer trust suddenly becomes important. Simply not infringing on data protection laws may not be enough to win consumer trust. Companies involved in personal information processing in Japan face such a problem of low degrees of consumer trust regarding data protection. This applies not only to the legal protection, but also the processing. This paper explores what the dangers of low consumer trust could mean for a company in its first part. The second part looks at the legal backgrounds of both regions and how they relate. The third part explores various Data Privacy Impact Assessments (DPIA frameworks) from both the

* University of Tokyo, Graduate School of Interdisciplinary Information Studies, IT-ASIA D3.

Key Words : Personal Data Protection, Privacy Impact Assessment, GDPR, Act on the Protection of Personal Information.

EU and Japan, In particular the DPIA methodology by Constantina Vemou and Maria Karyda. The fourth part applies the DPIA to the Japanese context. The fifth and final chapter gauges how a DPIA solves the relevant issues. Overall, this research will gauge what the dangers of low consumer trust mean for an entity processing personal information, and whether the proposed methodology can tackle the various challenges from both a consumer and a producer perspective.

1 Consumer Trust and Why it Matters

A cursory search on Google for "consumer trust" will lead to several articles on how it is important to cultivate for brand loyalty for companies. For academic research, such articles won't adequately define what consumer trust is. Rousseau et al. define trust as willingness to take on risk based on their expectations or the behavior of another (Rousseau 1998, 395). In the context of digital privacy, this translates to trusting someone with your personal information.

1.1 The Issue

However, Japan has an issue regarding public trust in data protection: 53% of poll respondents do not trust public entities' handling of personal data, and 55% feel the same about private entities. 73% of respondents even considered existing data protection regulations insufficient (Muneo 2022, 12-13). Legally, a business handling personal information in Japan does not require the consent of an identifiable person for the processing of their personal data. This is outlined in Japan's Act on the Protection of Personal Information article 18. There, personal information not handled beyond the scope necessary for achieving a clearly outlined purpose of use does not require consent. Handling personal data beyond this purpose of use would require consent. This contrasts with the EU, where consent or a limited range of requirements must be fulfilled to legally process personal data.

Data on similar concerns in a region such as the EU are inconclusive (Bauer 2022, 2113). A polled 65% of respondents to a special Eurobarometer poll felt that they had at least some degree of control over their personal data (EC 2019). This indicates that the various rights such as data retention and data portability are at least satisfactorily implemented. Furthermore, the legal culture surrounding personal data protection in both regions is different (Orito 2005, 1). For instance, Japanese citizens tend to accept access by the government to their

personal data, provided said information is managed properly (Luther 2012, 263).

Keeping this in mind, 233 verified cases involving the leakage of personal data of 46 million identifiable persons in Japan from entities including public bodies were catalogued on the portal site CyberSecurity-jp.com would do little to bolster trust (Cyber 2024). One similar statistic across both regions is made apparent in a study by Verizon; consumers across both Japan and various EU countries consider past cybersecurity breaches and data mismanagement a good reason to suspend further utilization of services (Verizon 2019a). In Japan, only 5% of users would overlook such issues (Verizon 2019b, 3), with about an average of 11% across the countries of the UK, France, Germany, Italy, The Netherlands and Sweden (Verizon 2019c, 4). This underlines the statement from several of the largest consulting companies such as Deloitte (Deloitte 2024), McKinsey (McKinsey 2020) and PwC (PwC 2014) that refer to robust data privacy practices to achieve a competitive advantage.

1.2 Why it Matters

But to what degree is trust a factor of importance to begin with? In the case of public entities, identifiable persons have no alternatives if they disagree with the entities' data protection policy. In the case of private entities, this lack of competition occurs as well. Social media platforms, search engines and operating services for hardware usually have competitors. If consumers want user friendly and ethical terms and conditions with regards to data processing, however, not much choice remains. When viable competitors are added to the equation, the situation changes.

This occurred in Toronto, for example, where the Sidewalk Labs smart city project was ultimately canceled. The reason for this was opposition from its citizens over a personal data processing proposition. Sensors and surveillance data from inside and outside residences would be collected and transferred to third parties including Google. A lack of trust cancelled the project (Bennat 2020). After all, when personal data gathering turns into a fear of surveillance, it can quickly become a cause of worry (Zoonen 2016, 475). Without trust, it is hard to acquire acceptance or cooperation from citizens and ultimately leads to opposition (Shimizu 2021, 1). While Sidewalk Labs ultimately failed at the start of the Covid pandemic, a lack of trust or social acceptance is attributed as one of the fundamental reasons for its failure. Writing for the MIT Technology Review, Karrie Jacobs stated that the "lack of seriousness about the privacy concerns of Torontonians was likely the main cause of its demise" (Jacobs 2020). When asked for one lesson to learn from the failure of Sidewalk Labs, Josh O'Kane who wrote a book on the project mentioned respect

for data privacy as a fundamental example (McDonald 2022). This pitfall is identified in case studies for Toyota's Woven City project; data is clearly noted to belong to users and society, rather than a transferrable commodity (Sakuma 2020, 37).

1.3 Does it Matter in Japan?

Looking at industry actors, the idea of trust with regard to data privacy is common. Consulting companies such as Deloitte (Deloitte 2023), PwC (PwC 2014), and McKinsey (McKinsey 2020) regard data privacy as the key to building consumer trust. At the same time, these actors emphasize several methods to build trust, such as education (Deloitte 2023) and cooperation (Morey 2015) with consumers. Then there is the Japan Institute for Promotion of Digital Economy and Community (JIPDEC). This non-profit organization provides accreditation services for various IT and management processes, including but not limited to APPI compliance. A JIPDEC DPIA methodology mentions losing stakeholder trust as one of the basic criteria for defining risk factors (JIPDEC 2020).

One major academic issue when it comes to trust or social acceptance is that it is a nebulous concept. When it comes to smart cities academia, citizen participation and social acceptance are very common and emphasized concepts. This field of research however lacks studies to flesh out these theoretical concepts (Meijer 2016, 404). Furthermore, research by Granier and Kudo points out that participation and trust concepts function differently in the Japanese context. They point out that Japanese smart city initiatives such as the Kitakyūshū Smart Community project simply expected citizens to "cooperate" and not much more (Granier 2016, 70). This same research however accentuates the merits of citizen cooperation and active participation in a co-production scheme (Granier 2016, 61). This indicates that Japan is not immune to the dangers of low consumer trust. And by extension the lessons to be learned from cases such as the Toronto Sidewalk Labs incident are an ever-present warning.

2 The Legal Background

One of the main reasons why the General Data Protection Regulation (GDPR) is relevant, is due to the influence EU data protection laws have on the corresponding Japanese legal framework. A first legal influence on Japan's Act on the Protection of Personal Information (APPI) was the EU's GDPR predecessor, Directive 95. This directive featured an adequacy

clause, which had an influence on what would become the APPI (Terada 2020, 174-178). Following this directive, the EU's GDPR would have a significant influence on further developments of the APPI, notably on the APPI's 2015 amendment (Katsuya 2021, 118-122). Especially the establishment of the Private Information Protection Commission (PPC) in 2016 was crucial. This agency was created as a third party, as opposed to the centralized cabinet structure commonly seen in Japan. The PPC would not only receive the mandate for overseeing personal data protection in 2016 (PPC 2024), but even receive the authority to provide guidance and conduct on-site inspections where necessary.

Further amendments included: rules for cross-border data transfer were established, the introduction of the concept of anonymously processed personal data, and establishing rules for sensitive types of personal data (EC 2019a). A final amendment concerns various fines and punishments under the APPI. Companies could see fines from ¥300,000 to ¥100,000,000 if decided on by the PPC, with a possible increase from ¥500,000 to ¥100,000,000 for illegal provisions of personal data to third parties, or fraud. This brought the severity of personal information processing fines closer to the GDPR. Under the latter, fines can be either a maximum of € 10,000,000 or two percent of the companies' entire global annual turnover, whichever is highest. In the case of severe violations, these amounts can be doubled.

2.1 Legal Convergence

The establishment and amendments of the APPI brought it closer to the GDPR. Observing the timeline of negotiations between Japan and the EU for the Economic Partnership Agreement provides an explanation for this convergence. When negotiations were completed in December 2017, Japan was not on the EU's whitelist for possessing an adequate level of protection. In July 2018, this had changed and Japan's APPI was considered adequate by the EU (EC 2019b). The APPI amendments that introduced the concepts of sensitive personal information and the PPC are to be seen as amendments in line with the negotiations with the EU (Itakura 2018, 159). But besides this, the concept of legal diffusion provides additional explanation. Japan being a trade partner of the EU which possesses a robust data protection framework and can be regarded as the 'leading regulator' (Bradford 2019, 176). This phenomenon results in the legal convergence discussed above (Bradford 2023, 56), though this can also be seen as the EU partaking in "regulatory imperialism" (Bradford 2023b,17).

3 The Legal Tools: Privacy Impact Assessments

This convergence presents opportunities for GDPR-related concepts to be applied to the Japanese context. In the GDPR, Data Protection Impact Assessments (DPIA) are the main features of article 35.

3.1 Tools of the EU

DPIA focuses on risk management, with privacy by design being a major objective (Oetzel 2014); hoping to achieve the trust of consumers and citizens (Wright 2012). A DPIA becomes necessary based on one important condition: there must be a high risk involved in a particular project involving the processing of personal information (DPC 2023, 11). This risk can be interpreted either as a potential risk of scale or of types of personal data. On one hand, a doctor managing their own private business does not need to create a DPIA for the processing of clients' personal information. On the other hand, a smart city featuring several sensors can easily lead to the involvement of numerous individuals. The EU's guidelines on DPIA mention: "For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore, require a DPIA" (WP 2023, 10).

However, guidelines published by Data Protection Authorities (DPA) often lack practical guidelines (Meis 2016), not featuring templates for a DPIA. Only objectives are mentioned in section 7 of article 35 of the GDPR:

1. A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
2. An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
3. An assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1;
4. And the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned;

This led to the development of DPIA models by various actors, such as Roger Clarke (Clarke 2009) and organizations such as ISO's 29134 model (ISO 2017). Further models of DPIA focused on integrating with the existing EU framework. Wright et al, argue for an EU DPIA framework, comparing guidelines originating from several EU countries (Wright

2013a). Notario et al. analyze DPIA methodologies (Notario 2015) in the EU, based in the context of an existing specific EU DPIA template (EC 2014). Van Puijenbroek and Hoepman would in turn focus on practical examples of DPIA which are in use in businesses in The Netherlands.

3.2 Tools of Japan

Various frameworks have also been proposed by Japanese actors, such as PwC (PwC 2024) and JIPDEC. JIPDEC's recommendations align with Toyota's Woven City guidelines for personal data protection as protecting individuals rather than processing data properly. Theirs is a system which closely follows the methodology which this paper suggests and gives a solid starting point for any businesses handling personal information wanting to perform a DPIA (JIPDEC 2020). Under the influence of various industry and academic actors, many DPIA methodologies go beyond compliance, with JIPDEC regarding it as a helpful tool for achieving privacy by design and due diligence (JIPDEC 2020).

3.3 The Tool of this Research

A more in-depth DPIA methodology was proposed by academics Vemou and Karyda (Vemou 2019). Their model builds on a library of existing DPIA methodologies from a variety of sources. Academic sources feature Wright (Wright 2013b), Oetzel and Spiekermann (Oetzel 2014), and Bieker et al. (Bieker 2016) Industry standards include ISO 29134, and finally legal standards derive from Canada's legal framework (TBCS 2010) and several policies, including two (CNIL 2019) of which based in the European framework (UK ICO 2014). Vemou and Karyda's Comprehensive Privacy Impact Assessment (CPIA) is made up of 6 steps, following most other existing models.

Step 1: The CPIA starts with a preliminary threshold analysis. This step confirms the requirements for a DPIA and the necessary resources for its relevant project. Essentially, whether article 35 of the GDPR applies to this project is analyzed. This analysis should ideally take place after senior management greenlights the project but preceding the budget and timetable finalization by the companies' Data Protection Officer. This step ends in a short report featuring the motivation behind the creation of the DPIA. This entire step should ideally be taken in parallel with the relevant project.

Step 2: This step features the planning and organization of the PIA project at the same time as the system implemen-

tation project. The output of this step includes a scope, roles for PIA implementation and PIA team, an overview of internal and external stakeholders including method of consultation, and the PIA plan implementation. The stakeholders -internal and external- are either involved actors, or actors that would be impacted by the project. External stakeholders can include industry experts and consumer groups (Wright 2013; Bieker 2016). The methods of involvement of these stakeholders can include but are not limited to surveys, interviews, and focus groups (Bieker 2016; ISO 2017). Vemou and Karyda place emphasis on the selection and inclusion of DPIA team members which are representatives of relevant business units (Oetzel 2014), business analysts, risk assurance and internal audit staff, communications advisers, and specialists of technology (Vemou 2019, 45). This step finally features setting milestones parallel to implementation phases of the new project. The final DPIA outcomes can be analyzed to mitigate and cover possible newly discovered risks (Oetzel 2014; Vemou 2019, 45).

Step 3: Here, models of personal data flows of the intended project are created. This includes details such as: the types, sensitivity, sources, method of collection and processing, purpose, main actors involved, data retention periods and transfers to third parties of personal data. Furthermore, the existing security and privacy controls of the company are also analyzed. Finally, the expected behavior of identifiable persons should be incorporated in the model. Following this, data protection targets require defining. These privacy requirements become the basis of risk analysis and should be sourced from a variety of sources such as legal frameworks, user expectations and general literature (Vemou 2019, 46).

Step 4: Next up is the identification of possible risks. This is defined as "a hypothetical scenario of describing how risk sources could exploit vulnerabilities of supporting assets, in a context of threats and allow feared events to occur on personal data, thus generating impacts on the privacy of data subjects (CNIL 2019)."

This process consists of 3 parts: the identification of risk sources, the definition of threats as possible events that would lead to the harm of one's data privacy, and the identification of threat scenarios through linking risk sources with outcomes. These scenarios are mainly to be performed from the point of view of the identifiable persons. From this, the scope of personal data breaches and an overview of the possible consequences

become visible. Finally, the risk is defined as the likelihood of a threat scenario taking place, multiplied by the impact of said threat scenario. As a result, the organization has an overview of possible threats and their relative scope and whether the possible results of incidents can be avoided, or its impacts lessened (Vemou 2019, 47).

Step 5: From step 4's risk evaluation, risk mitigation can be performed through organizational and technical controls. This would ideally reduce the likelihood of risks by adjusting the project or redesigning the method of personal information processing. For this method redesign, the risk evaluation provides numerical data on potential risks of personal data processing, aiding reevaluation (Vemou 2019, 49).

Step 6: The previous steps' outputs are tallied for the privacy impact assessment process. This report should report the following information: "the project owner, project description, information flows and processing purposes, privacy risks, privacy controls to mitigate risks, action plan for recommendations implementation (along with responsible/accountable for implementation), residual risks and sign-off information." Compounded with risk mitigation decisions turns a CPIA into a valid compliance report for GDPR article 24 (Vemou 2019, 49).

These 6 steps form the body of Vemou and Karyda's CPIA methodology, though some adjustments are possible when applying it to a Japanese context.

4 DPIA in the Japanese Context

While being a legal requirement strictly under the GDPR, a DPIA performed in a Japanese context would be completely optional. The GDPR condition where a possible high risk of personal data processing requires a DPIA similarly does not apply to Japan. As a methodology however, a DPIA offers several potential benefits, along the lines of best practices. An inherent benefit of a DPIA is being part of a privacy by design philosophy. Previously mentioned section 7 of article 35 of the GDPR lists the objectives to be met with a DPIA. The first of these objectives is the purpose of the data processing, which is the same as the APPI's article 17's definition of the "purpose of use". This definition is critical, as a clearly outlined purpose of use is important under Japanese law. Article 18 of the APPI adds the requirement of consent from identifiable persons in cases of personal data processing beyond the scope of this purpose of use from the preceding article. Subsequent objectives include the ne-

cessity and proportionality of the processing, assessment of the risks and rights and freedoms of identifiable persons, and the measures to address these risks and safeguard rights.

4.1 Link with Trust

These objectives in a Japanese context are appealing in the context of risk management and avoiding the gathering of superfluous personal data. One important question that rises from these best practices and risk management is the influence it would have on trust. Consumer trust or acceptance with regards to new technology are often measured through Technology Acceptance Models (TAM). A TAM developed by Al Abdali et al found that "the privacy lifecycle protection, privacy controls, impact assessment, and personal information monitors significantly influence the service trust." (Al Abdali 2021, 129-130). The various benefits of a DPIA can therefore have a direct impact on consumer trust. Though a study that gauges the impact of implanting a DPIA in a method consistent with its objectives would provide a clearer link. Regrettably, such a study has not yet been done to this researcher's knowledge.

4.2 Building Data Privacy

The introduction and methodology to DPIA's from JIPDEC affirms many of these benefits. Privacy by design through DPIA implementation, engagement of the stakeholders and due diligence are the three core ideas brought up by this organization. Their method follows the basic outline of the CPIA method: implementation decision, stakeholder involvement, implementation flow planning, risk analysis and mitigation (JIPDEC 2020).

Vemou and Karyda's CPIA method goes further, especially in the context of further risk management and identifiable person trust management. Particularly, all steps of the CPIA besides the first step play an important role in providing a solid methodology to waterproof personal data processing by businesses handling personal information. The second step is interesting for building up consumer trust, since various methods of consumer integration are introduced to fit various situations (Vemou 2019, 45). Besides integrating external stakeholders such as customers or consumer groups, the method of involvement is also varied. Building on other models, the CPIA suggests surveys, focus groups, interviews, or workshops as implemented in other models (Bieker 2016; ISO 2017). Going even further, Delphi Consensus as a consultation method was tested in the European BIRO project (Di Iorio 2019).

This last specific example illustrates the major difference to JIPDEC methodology, where

the same objectives are proposed, but differ in level of detail and methodology. JIPDEC only underlines the need of stakeholder involvement and consultation on feedback (JIPDEC 2021). While such consultations of stakeholders -especially consumers- is optional, it is recommended by both the CPIA and JIPDEC. The question of how far a business handling personal information involves consumers depends on how far a company is willing to go to perfect their data privacy practices. But considering the earlier mentions by consulting groups that see data privacy as a potential for competitive advantages, there are advantages for consumer consultation.

Companies such as Japan's JCB already carry out DPIA's for customers from the EU. They also apply risk analysis methods for tackling risks in personal data protection or even broader information security matters (JIPDEC 2022, 8;32). Having a more robust and detailed methodology in place for Japanese markets is beneficial in terms of best practices and can be used for compliance should data processing include or begin to include EU citizens. Various good practices for data privacy collected by a JIPDEC survey point out DPIA related efforts from notable Japanese companies. Having the various details and methodologies present in CPIA would improve these good practices or make it easier for other businesses handling personal information to perform their own DPIA (JIPDEC 2022, 32-33).

5 Rebuilding Consumer Trust

5.1 A Solution to the Problem?

When looking at solving the issue of low consumer trust, a study by McKinsey presents a few usable data for comparison. For proactive steps businesses handling personal information could take, data mapping, operations, infrastructure, and customer-facing best practices are listed (McKinsey 2020). Data mapping envisions the data maps of collected personal information, with special care taken to not gather unnecessary data. This is featured in the CPIA's third step for data flows, with additional parameters on top (Vemou 2019, 47). Operations and infrastructure are similarly featured in steps 3, 4 and 5 of the CPIA, seeking to properly plan the internal management of personal data processing. Looking at the data from Japan's Network Security Agency, only 20.3% of personal information processing incidents involve outside attacks. Insider human errors such as misplaced data and mismanagement together account for 50.6% of logged incidents (JNSA 2019, 7). Data from the portal site Cybersecurity Japan for the years 2023 and 2024 saw a similar trend towards insiders rather than outsiders as the ori-

gin for verified incidents (Cyber 2024).

This is further mirrored in a comparative study where the biggest worries regarding data protection for Japanese citizens were the mismanagement of personal data by internal actors (Cullen 2010, 112). Steps 3, 4 and 5 seek to streamline internal management and correct mistakes during the implementation phase of a project. This further synergizes with reaction speed during incidents when roles and responsibilities are clearly defined. Finally, customer-facing best practices can otherwise be summed up with privacy by design which is a key focal point for DPIAs in general. Further keywords include transparency and user experience, balanced with security and privacy (McKinsey 2020). The CPIA's methodology's third, fourth and fifth steps all include reviews of the security and privacy controls. These can be evaluated based on consumer input gained from stakeholder consultation from the second step (Vemou 2019, 45-47). Including consumers in the process or publishing DPIA findings can directly appeal to consumers, the latter measure promoted by JIPDEC (JIPDEC 2021).

5.2 Further Building Blocks

Finally, the McKinsey study also interviewed consumers for various business practices and how these practices correspond to their trust. Topping this list was limiting the usage of personal data to what is purely necessary, and a quick response to hacks and breaches (McKinsey 2020). These coincide with the attention given to operations and infrastructure on the business side in the previous paragraph and steps 3, 4 and 5 by the CPIA. Note that this report was based on the North American market and may not translate precisely to the Japanese context, though various points of concern for the consumer coincide with the findings from Cullen (Cullen 2010). Though any possible inconsistencies on this front further underlines the CPIA's method of consumer involvement to address the largest concerns of identifiable persons as ideal.

Conclusion

Companies can have a variety of reasons for managing consumer trust, which has been shown to be low among Japanese consumers concerning data privacy, according to polls. Technology acceptance models identify a clear link between respect for data privacy and risk impact assessment, and consumer trust. From a business perspective, most of the largest consulting firms identify data protection as an important tool for gaining trust. Alternatively, de-

pending on the product or service provided, a lack of respect for the consumer's need for data privacy can have catastrophic consequences, as seen with the Sidewalk Labs smart city project. Consumer trust can thus be said to matter in the framework of data privacy. Private and public entities in Japan are faced with low levels of consumer trust for data privacy. Borrowing from the EU's General Data Protection Regulation, the Comprehensive Privacy Impact Assessment by Vemou and Karyda is a fleshed-out methodology that can alleviate many data privacy-related worries. Compatible with Japan's legal framework, the appeal of this methodology is that it borrows from the EU's stricter data protection law. This strictness has led to the development of more robust and waterproof Systems. Furthermore, it corresponds to best practices for personal data processing management, with consumer consulting mechanisms. These advantages would put it above alternative privacy impact assessments that are recommended by Japanese organizations such as JIPDEC. This research has shown that practical solutions can be found in theoretical concepts such as legal diffusion. Japanese entities processing personal information can implement a myriad of solutions to the problem of social acceptance and trust. Methodologies that have been refined further already exist and are available for implementation to rebuild some of the lost trust of Japanese consumers.

Bibliography

AlAbdali,Hilal, Mohammed AlBadawi, Mohamed Sarrab, and Abdullah AlHamadani. 2021. "Privacy Preservation Instruments Influencing the Trustworthiness of e-Government Services." *Computers* 10, no. 9: 114-134.

Bauer, Paul C., Frederic Gerdon, Florian Keusch, Frauke Kreuter, and David Vannette. 2022. "Did the GDPR Increase Trust in Data Collectors? Evidence from Observational and Experimental Data." *Information, Communication & Society* 25, no. 14: 2101-2121.

Bennat, Berger. 2020. "Sidewalk Labs' Failure and the Future of Smart Cities." *Triple Pundit*.

Bieker, Felix, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost. 2016. "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation." edited by Stefan Schiffner, Jetzabel Serna, Demosthenes Ikonomou, and Kai Rannenberg. *Privacy Technologies and Policy*, Cham: Springer International Publishing: 21-37.

Bradford, Anu. 2019. "Digital Econonomy, The Brussels Effect: How the European Union Rules the World." *Oxford Academic*.

Bradford, Anu, Adam Chilton, and Katerina Linos. 2023 "The Gravity of Legal Diffusion." *Rochester*, NY, July 5.

Bradford, Anu. 2023. *Digital Empires: The Global Battle to Regulate Technology*. Oxford University Press.

Clarke,Roger. 2009. "*Privacy Impact Assessment: Its Origins and Development.*" *Computer Law & Security Review* 25: 123–135.

Commission Nationale de l'Informatique et des Libertés. 2024. "Privacy Impact Assessment (PIA)."

Cullen, Rowena. 2011. "Privacy and Personal Information Held by Government: A Comparative Study, Japan and New Zealand." Edited by Assar, Saïd Assar, Boughzala, Imar, and Boydens, Isabelle. *Practical Studies in E-Government: Best Practices from Around the World* 93–112.

Cybersecurity.com. 2022. "Kojinjōhō rōei jiken – higaijirei ichiran." Last Accessed September 18, 2024, https://cybersecurity-jp.com/leakage-of-personal-information#content2022.

Cybersecurity.com. 2024. "Kojinjōhō rōei jiken – higaijirei ichiran." Accessed September 18, 2024, https://cybersecurity-jp.com/

leakage-of-personal-information.
Data Protection Commission. 2023. "Guide to Data Protection Impact Assessments ¦ Data Protection Commission."
Deloitte. 2024. "Consumer Privacy: A Business Imperative in the Digital Age." *Deloitte Middle East ¦ ME PoV 42*.
Di Iorio, C.T., Carinci, F., Azzopardi, J., Baglioni, V., Beck, P., Cunningham, S. and Federici, M.O. 2009. "Privacy impact assessment in the design of transnational public health information systems: the BIRO project." *Journal of Medical Ethics* 35, No. 12: 753-761.
European Commission. 2014. "2014/724/EU: Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems."
European Commission, Directorate-General for Justice and Consumers. 2019. "Special Eurobarometer 487a: The General Data Protection Regulation."
European Commission. 2019. "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)."
European Commission Press Release Database. 2019. "The European Union and Japan agreed to create the world's largest area of safe data flows."
Granier, Benoit, and Hiroko Kudo. 2016. "How Are Citizens Involved in Smart Cities? Analysing Citizen Participation in Japanese 'Smart Communities'." Edited by Hans Jochen Scholl. *Information Polity* 21, no. 1: 61-76.
Itakura, Yoichirō and Terada, Mayu. 2018. "Ōshūrengōinkai jūbunseikettei no tenbō to kitai." *Jōhōshorigakkaikenkyūhōkoku* 2018-EIP-79 No.2: 156-183.
International Standardisation Organisation. 2017. "ISO/IEC 29134:2017(E): Information technology - Security techniques – Guidelines for privacy impact assessment."
Luther, Catherine, and Radovic, Ivanka. 2012. "Perspectives on Privacy, Information Technology, and Company/Governmental Surveillance in Japan." *Surveillance & Society* 10, no. 3: 263-275.
Jacobs, Karrie. 2022. "Toronto wants to kill the smart city forever." *MIT Technology Review*. https://www.technologyreview.com/2022/06/29/1054005/toronto-kill-the-smart-city/
Nihonnettowākusekkyuritikyōkai. 2019. "2018 nen jōhōsekkyuriti inshidento ni kansuru chōsakekka."
Nihonjōhōshorikaihatsukyōkai (JIPDEC). 2020. "Puraibashīeikyōhyōka (Privacy Impact Assessment)] ～ ISO/IEC29134:2017 no JIS-ka ni tsuite ～." Accessed September 20, 2024, https://www.jipdec.or.jp/library/report/2020721.html
Nihonjōhōshorikaihatsukyōkai (JIPDEC). 2021. "PIA to ha? PIA no susumekata to pointo wo kaisetsu." Accessed September 20, 2024, https://www.jipdec.or.jp/library/report/20210225-2.html.
Nihonjōhōshorikaihatsukyōkai (JIPDEC). 2022. "Puraibashīgabanansu ni kansuru chōsakekka (torikumijōkyōrei)." Accessed September 20, 2024, https://www.jipdec.or.jp/news/news/htpisq0000002w03-att/20220318_case_study_privacygovernance_research.pdf.
McDonald, Jordan. 2022. "What cities can learn from Sidewalk and Toronto's failed city of the future." *Tech Brew*. Accessed September 19, 2024, https://www.emergingtechbrew.com/stories/2022/09/21/how-miscommunication-derailed-sidewalk-s-usd1-3-billion-city-of-the-future.
Muneo, Kaigo, and Pang, Natalie. 2022. "Smart Cities and Data Privacy Concerns in Japan." Edited by Echle, Christian, and Naumann Katharina. *Data and Innovation in Asia-Pacific* 12.
Katsuya, Uga and Shishido, Jōji. 2021. "Jichitaishokuin no tame no kojinjōhōhogohōkaisetsu." *Dai-Ichi Hōki*.
McKinsey. 2020. "The consumer-data opportunity and the privacy imperative." Accessed September 21, 2024, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative.
Meijer, Albert, and Manuel Pedro Rodríguez Bolívar. 2016. "Governing the Smart City: A Review of the Literature on Smart Urban Governance." *International Review of Administrative Sciences* 82, no. 2: 392-408.
Meis, Rene, and Heisel, Maritta. 2016. "Supporting Privacy Impact Assessments Using Problem-Based Privacy Analysis." Edited by Lorenz, Pascal, et al., *Software Technologies*. Cham: Springer International Publishing: 79–98.
Morey, Timothy, Theodore "Theo" Forbath, and Allison Schoop. 2015. "Customer Data: Designing for Transparency and Trust." *Harvard Business Review*.
Nicolás Notario et al. 2015. "PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology." *2015 IEEE*

Security and Privacy Workshops, San Jose, CA, USA: 151-158,

Oetzel, Marie, and Spiekermann, Sarah. 2014. "A Systematic Methodology for Privacy Impact Assessments: A Design Science Approach." *European Journal of Information Systems* 23, no. 2: 126–50.

Orito, Yohko, and Murata, Kiyoshi. 2005. "Privacy Protection in Japan: Cultural Influence on the Universal Value." 2005 ETHICOMP.

PricewaterhouseCoopers. 2014. "Build customer trust through data privacy." *R&C Outlook June 2014*.

PricewaterhouseCoopers. 2024. "Puraibashīeikyōhyōka (PIA) kōchikushien." Accessed September 21, 2024, https://www.pwc.com/jp/ja/services/assurance/governance-risk-management-compliance/privacy-impact-assessment.html.

Kojinjōhōīnkai. 2024. "「Kojinjōhōīnkai」he no kaiso (heisei 25 nen 1 gatsu tsuitachi nit suite)."

Rousseau, Denise et al. 1998. "Not So Different After All: A Cross-discipline View of Trust." *The Academy of Management Review*: 395.

Sakuma, Daisuke, and Katō Kazuhiko. 2020. "Jidōuntengyōkai no sumātoshiti senryaku to haikei to TA（Winner Takes All: shōhaishasōtori）no kōzai". *Kaihatsu Kōgaku*, no. 1: 37-40.

Shimizu, Yuho, Shin Osaki, Takaaki Hashimoto, and Kaori Karasawa. "The Social Acceptance of Collecting and Utilizing Personal Information in Smart Cities." *Sustainability* 13, no. 16: 9461.

Terada, Mayu. 2020. "EU to nihon ni okeru kojinjōhōhogohōsei no hikaku to kadai." *Hikakuhōkenkyū* 81: 174-178.

Treasury Board of Canada Secretariat. 2022. "Directive on Privacy Impact Assessment."

UK Information Commissioner's Office (ICO). 2014. "Conducting privacy impact assessments: code of practice."

Vemou, Konstantina, and Karyda, Maria. 2019. "Evaluating Privacy Impact Assessment Methods: Guidelines and Best Practice." *Information & Computer Security* 28, no. 1: 35–53.

Verizon. 2019. "What customer experience do consumers REALLY want?" Accessed September 21, 2024, https://www.verizon.com/about/news/what-customer-experience-do-consumers-really-want.

Verizon. 2019. "APAC: The CX Optimists." Accessed September 21, 2024, https://www.verizon.com/business/resources/reports/2019/apac_the_cx_optimist.pdf.

Verizon. 2019. "Europe: High-stakes CX." Accessed September 21, 2024, https://www.verizon.com/business/resources/reports/2019/europe_high_stakes_cx.pdf.

Working Party on the Protection of Individuals with Regard to the

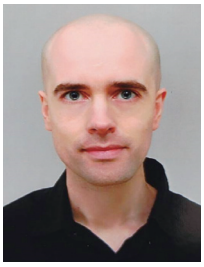
Processing of Personal Data. 2017. "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679."

Wright, David, and De Hert, Paul. 2012. "Introduction to Privacy Impact Assessment." *Law, Governance and Technology Series* 6: 3–32.

Wright, David. 2013. "Making Privacy Impact Assessment More Effective." *The Information Society* 29, no. 5: 307–15.

Wright, David, Finn, Rachel, and Rodrigues, Rowena. 2013. "A Comparative Analysis of Privacy Impact Assessment in Six Countries." *Journal of Contemporary European Research* 9: 160–80.

Zoonen, Liesbet van. 2016. "Privacy Concerns in Smart Cities." *Government Information Quarterly* 33, no. 3: 472-480.



Tomas　Dexters（トーマス・デクスターズ）

［**専門**］日本と EU の情報法・日本学 (EU and Japanese Information Law・Japanese Studies)

［**主たる著書・論文**］

Dexters, Tomas. 2019. "The adequacy of the adequacy of the GDPR and the APPI." MA Thesis, Kyushu University.

Dexters, Tomas. 2018. "Inoue Kowashi – Constitutional Entrepreneur of the Meiji Period." MA Thesis, KU Leuven.

［**所属**］東京大学大学院学際情報学府博士課程
ITASIA プログラム博士課程 3 年生

［**所属学会**］社会情報学会 (The Society of Socio-Informatics)

Rebuilding Broken Japanese Consumer Trust : Applying the EU's Privacy Impact Assessment to a Japanese Context

Tomas Dexters *

For personal data processing, there is a balance between how far a company can push what degree of processing is possible through technology, and what consumers are willing to put up with to access a product. In Japan, companies can gather and process personal information with no consumer consent if said personal data is necessary for the utilization of a business purpose. Additionally, there is a low degree of public trust among the Japanese public for data protection. The former fact means that companies are relatively free to gather personal information if legally justifiable. The latter means that consumer participation can be reluctant, or that consumers choose to opt out of a service or product entirely. This incentivizes companies or public organizations to exceed the strict legal requirements to prevent consumers deciding not to utilize their product or service.

Looking at the evolution of Japan's data protection law through the framework of Legal Diffusion, the influence of the EU's GDPR is plain to see. This research takes this one step further and looks to the GDPR for solving the issue of low consumer trust. One of these would be Data Privacy Impact Assessments (DPIA), originating from GDPR article 35. Specifically, there are various academic templates for these DPIAs, since article 35 only provides a set of objectives rather than a methodology. This paper will look at a DPIA method from Constantina Vemou and Maria Karyda, which includes provisions for transparency and integrates consumers as a stakeholder.

While DPIAs are not required under the Japanese Act on the Protection of Personal Information, this implementation has plenty of benefits in the vein of good business practices. The DPIA is a method compatible with the Japanese legal framework and the specific methodology analyzed corresponds to various consumer concerns and problems for personal data processing entities.

* University of Tokyo, Graduate School of Interdisciplinary Information Studies, ITASIA D3.

Key Words：Personal Data Protection, Privacy Impact Assessment, GDPR, Act on the Protection of Personal Information.