The Era of Privacy Governance

The State of Legal Reform and Privacy Investments Towards GAFA Regulation

Shintaro Kobayashi

Nomura Research Institute, Ltd.

September, 2022

NRI

Share the Next Values!

About Me

Shintaro Kobayashi

Public Policy Group Manager | ICT Media Consulting Department | Nomura Research Institute

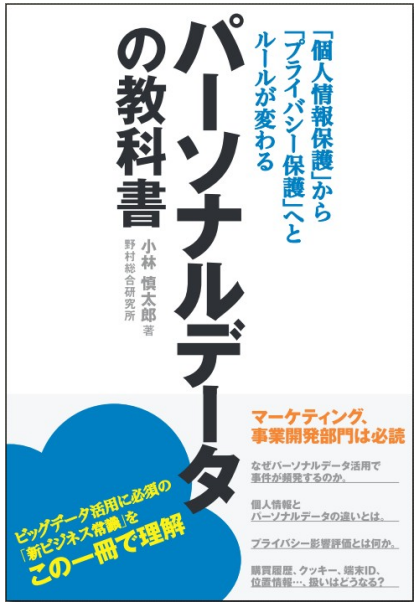
I specialize in ICT public policy and management. I am engaged in research and consulting for government agencies and the information and telecommunications industry. I am exploring mechanisms to create a society where everyone can live in peace while information distribution is lively, with protection of personal information and privacy, promotion of secondary use of copyrighted works, and the like.

(Committee Member)

- Member of ”Corporate Privacy Governance Model Study Committee,” Ministry of Internal Affairs and Communications/Ministry of Economy, Trade and Industry (2019-present)
- Member of ”Privacy Impact Assessment (PIA) Study Committee”, JIPDEC/Personal Information Protection Commission (2020)
- Member of ”Study Committee on Competition Policy for Data Market”, Fair Trade Commission (December 2020 - June 2021)

(Publications)

- ”Series: Privacy Governance—Essential for DX!” Nikkei Cross Trend (November 2020 - January 2021)
- ”Textbook of Personal Data: Rules Changing from Personal Information Protection to Privacy Protection” Nikkei BP (July 2015)



What I want to convey today

Companies of the future will be required to establish their own privacy governance and will need to make privacy investments to achieve this

- On April 1, 2022, the revised Act on the Protection of Personal Information (”APPI”) came into effect, strengthening the rights of individuals to request the cessation of use or deletion of their own information and the obligations imposed on business operators.
- The background of this revision is the flaming incidents caused by inadequate privacy protection in the handling of personal data, and the global trend toward tighter regulations. It is expected that laws will continue to be revised on a short cycle.
- Meanwhile, GAFA and other mega-platformers are trying to overcome these regulations with their massive financial resources and to collect and utilize personal data not only in the online world but also in the real world.
- In this report, I propose the significance of establishing ”privacy governance,” a mechanism for companies themselves to both protect and utilize personal data, in order to respond flexibly to tighter regulation and avoid being dominated by GAFA, and also suggest how ”privacy investments” should be made for this purpose.

01 Why is the APPI repeatedly amended?

02 Will regulation of GAFA revitalize data distribution?

03 Proposals for necessary ”privacy investments”

Many “flaming incidents” sparking consumer outcry have occurred, and companies and their managers are increasingly being held accountable

Privacy Problems and Their Impacts

Rikunabi	LINE	Yahoo! JAPAN	Benesse	Suica
Improper use/failure to obtain consent	**Poor management of personal data**	**Insufficient explanations**	**Personal information leaks**	**Insufficient explanations**
Provided the unofficial resignation rate to companies listed on Rikunabi without the consent of the individual and provided insufficient explanations.	Enabled access to personal data from Chinese companies more than necessary and without specifying the country to which the data is being transferred.	Explanations for ”Yahoo! Score” were inadequate.	Approximately 29 million sets of personal information were leaked.	Suica rider history data was anonymized before being provided to others, but explanations were inadequate.

- **Consumers’ surprise/unease led to flare-up**
- **Guidance from Personal Information Protection Committee**

Privacy issues **have serious impacts including managerial and legal liability**

Suspension of service	Apology/explanations	Loss of trust	Damages
Sharp drop in share price	Review of internal systems	Review of policies/rules	Establishment of third-party committee

Source: Prepared by NRI based on publicly available information.

In most cases, attempts to use data without adequate personal data management or risk assessment are the cause of the flaming incidents

Structure of a Flaming Incident

Causes

- Failure to manage personal data (how it was acquired, purpose of use, etc.)
- Failure to assess and address privacy risks or inability to do so in the first place
- Utilizing data while neglecting consumer concerns and fears

Result

- Flaming incident

When there is inadequate personal data management, lack of understanding, or inadequate privacy risk assessment, can data be used securely?

Following the GDPR, privacy regulations are tightening across the globe

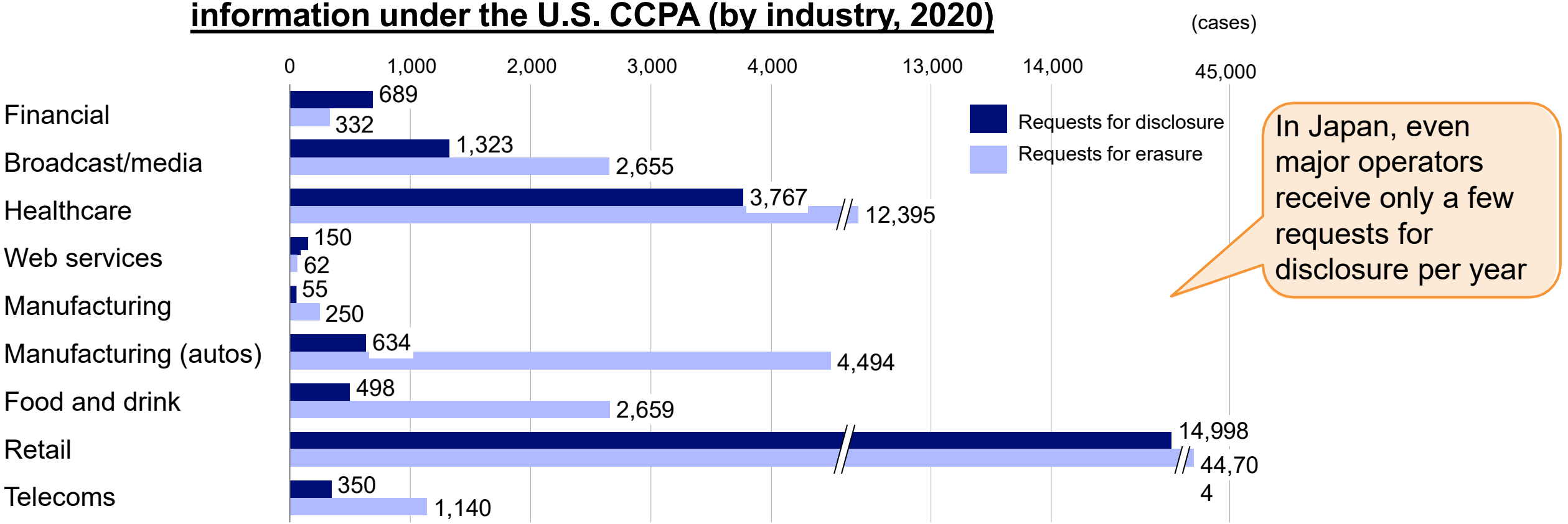
Trends in Legal Regulation in Japan/Europe/United States

Year	Japan	Europe	United States	
			Federal	State (e.g., California)
2012	(2005: APPI comes into effect)	**EU General Data Protection Regulation (GDPR) drafted**	Consumer Privacy Bill of Rights drafted	
2013				
2014				
2015	2015: Revision of APPI **(first revision 10 years after coming into effect)**		Proposed Consumer Privacy Bill of Rights (discussion draft) unveiled	
2016		GDPR adopted	Considered by Congress but not passed	
2017	Revised act comes into effect			
2018		GDPR comes into effect	State laws on privacy in disarray	**Enactment of California Consumer Privacy Act (CCPA)**
2019				
2020	2020: Revision of APPI		**Uniform federal privacy act considered** (Publication of Democratic and Republican party proposals)	CCPA comes into effect Enactment of CPRA, an enhanced version of CCPA
2021				
2022 on	Revised act comes into effect (April 1, 2022) Next revision (2025: three years after coming into effect)	Adoption of ePrivacy rules equivalent to GDPR special act?	Enactment of uniform federal privacy act?	CPRA comes into effect (2023)

Source: Prepared by NRI based on publicly available information.

In the U.S., CCPA enforcement has increased the burden on business operators. The era of individuals monitoring companies is coming

Number of ”Requests for Disclosure” and ”Requests for Erasure” of personal information under the U.S. CCPA (by industry, 2020)



Source: Prepared by NRI based on IAPP ”Data privacy requests metrics: Lessons for your privacy program” (September 16, 2021)

1. Why is the APPI repeatedly amended? | Key points of revised APPI in effect from April 1, 2022

The act was amended to emphasize the rights and interests of individuals

Key Points of the Revised APPI

1. The state of individual rights *Regulations on the obligations required in cases of third-party provision of personal data to a third party without obtaining prior consent from the individual and stopping provision at the request of the individual.	**Strengthened rights to demand cessation of use/deletion etc.**
	Enhancement of disclosure methods for retained personal data
	Mandatory disclosure of records of third-party provision
	Short-term saved data made subject to disclosure etc.
	Enhancement of opt-out regulations*
2. The state of obligations to be upheld by business operators	**Mandatory reporting and notification of individuals for leaks etc.**
	Prohibition of inappropriate use
3. The state of mechanisms to promote voluntary efforts by business operators	Enhancement of the accredited personal information protection organization system
	Addition of public announcements regarding retained personal data
4. The state of data utilization	Creation of pseudonymized information
	Clarification of the application of exceptions for the public interest
	Handling of personal data by recipients
5. The state of penalties	Increased penalties
6. Extraterritorial application of laws and cross-border transfer	Expansion of extraterritorial application
	Enhancement of information provision for cross-border transfers

Source: Prepared by NRI based on "Act for Partial Revision of the Act on the Protection of Personal Information (Summary), June 12, 2020," Personal Information Protection Commission

1. Why is the APPI repeatedly amended? | Issues for next revision in three years

Tighter regulations on privacy-by-design* are expected in Japan going forward

Issues for Next Revision (NRI's predictions)

1. Expanded scope of personal information (Cookies, IP addresses, member IDs etc.)
2. Enhancement of individual rights
3. Enhanced protection of children's data online
4. Introduction of AI/profiling regulations
5. Introduction of surcharge system
6. Enhancement of privacy-by-design (PIA, system development etc.)

Enhancement of privacy-by-design (PIA, system development etc.)

Present

In Japan, an increasing number of companies, especially those promoting DX, have introduced privacy impact assessments (PIA). The government also recommends that companies conduct PIAs.

Future

PIAs or appointment of DPOs (Data Protection Officers)/CPOs (Chief Privacy Officers) may become mandatory as in Europe and the U.S.

* Assessing in advance the risk of privacy violations that may occur when handling personal data, including personal information, and working to avoid or minimize such risks.

Why is the APPI repeatedly amended?

- There has been an endless stream of flaming incidents. In most cases, the attempt to utilize data without adequate implementation of personal data management and risk assessment resulted in the flare-up.

- Following the 2012 draft GDPR, privacy regulations are tightening across the globe. The revised act that came into effect on April 1 was amended to emphasize the rights and interests of individuals.

- With the endless stream of flaming incidents and tightening privacy regulations around the globe, the APPI will continue to be revised in the future. **It is important for companies to work on "enhancing privacy by design" in order to stay ahead of regulations.**

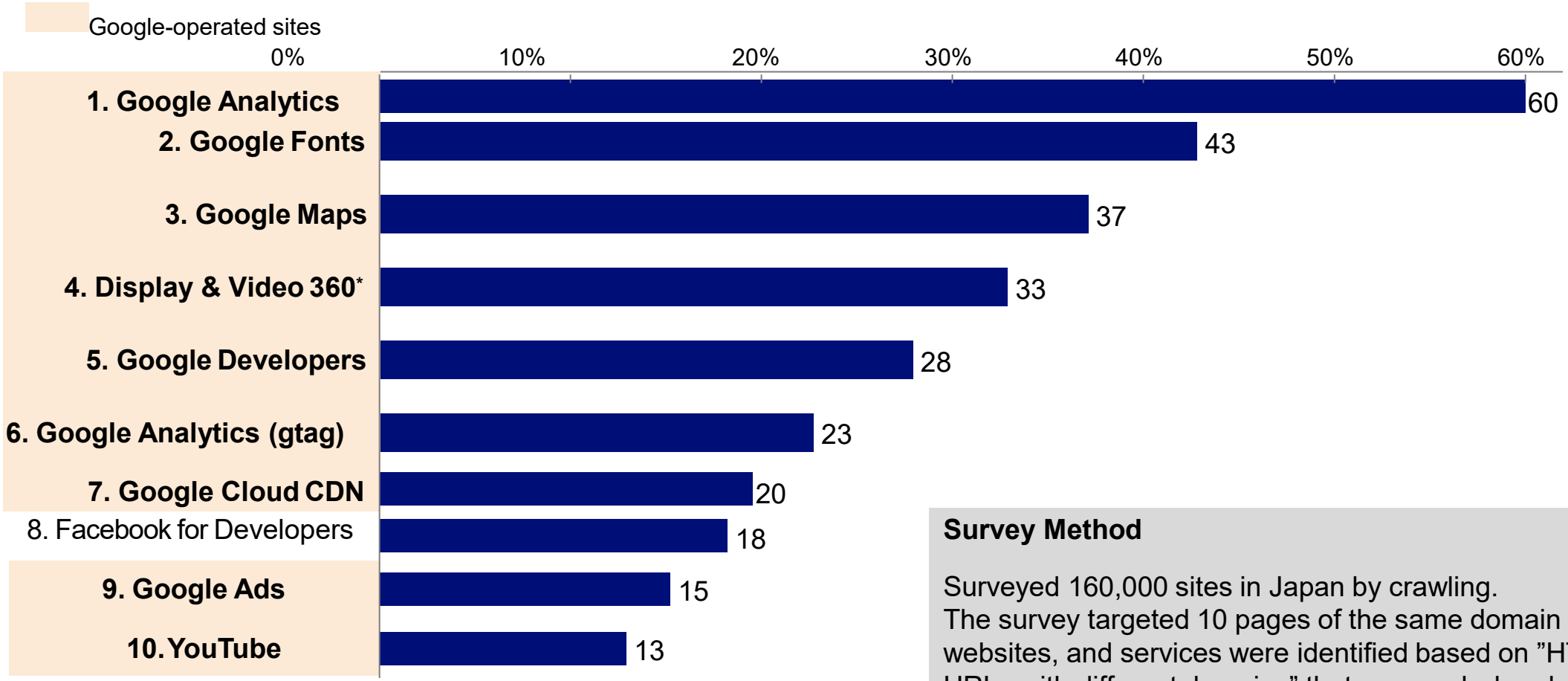
01 Why is the APPI repeatedly amended?

02 Will regulation of GAFA revitalize data distribution?

03 Proposals for necessary ”privacy investments”

Most Web services used on Japanese websites are Google

Adoption Rate of Web Services on Major Japanese Websites (Top 10)



*Module provided by the former Double Click, Inc., which merged with Google in 2018.Source: Prepared by NRI based on ”DataSign Web Services Survey Report 2021.7” DataSign (July 31, 2021)

Survey Method

Surveyed 160,000 sites in Japan by crawling.
The survey targeted 10 pages of the same domain on the surveyed websites, and services were identified based on ”HTTP requests to URLs with different domains” that occurred when browsing the websites.

2. Will regulation of GAFA revitalize data distribution? | Data concentrated in GAFA

GAFA are steadily accumulating IoT data

Autos

Automotive data is starting to become concentrated among Google, Amazon, and Microsoft.

All but German cars and Toyota have Android

In addition to European and US OEMs (Volvo, GM, Ford), Renault-Nissan and Honda are using Google products for infotainment systems and in-car OSs

AWS, Azure on the rise for connected cars

OEMs (BMW, VW, Toyota) that have indicated their intention to produce their own OSs are also adopting Amazon Web Services and Microsoft Azure for cloud computing for connected cars.

Smart Homes

With the entry of Google Home and Amazon Echo, the IoT home market is expanding. Voice data increasingly dominates.

Standardization of communication standards

Google, Amazon, Apple, and Zigbee Alliance (industry association for wireless communication standards) announced the development of a common communication standard for smart home devices (December 2019).

Domination of voice data by Google and Apple

The Connectivity Standards Alliance, which includes Apple, Amazon, Google, and others, has announced a new smart home device connectivity standard called ”Matter” (May 2021). Ensures voice control compatibility.

Wearables

Apple and Google are trying to dominate healthcare data.

Apple Watch

The company boasts an overwhelming market share. Provides hospitals and medical institutions with a clinical research platform (ResearchKit) for R&D.

Fitbit (Google)

Competition authorities in Japan, the U.S., and Europe conditionally approved Google’s acquisition of Fitbit (January 2021). The condition is that Fitbit’s health data will not be used for digital advertising business (for a minimum of 10 years).

2. Will regulation of GAFA revitalize data distribution? ｜Towards opening up data concentrated in GAFA

The “right to data portability” introduced by the GDPR is intended to make it easier for individuals to transfer their personal data accumulated by GAFA

Overview of Right to Data Portability

Significance and Purpose of Right to Data Portability (From European Commission Q&A)

① For individuals, it bolsters their fundamental right to control their personal data.

② For startups and SMEs, it allows them access to a data market dominated by digital giants, enabling them to gain more users.

The GDPR’s Right to Data Portability

Indirect transfer

- The right to receive data from the controller in a machine-readable, generally accessible format and to transfer it to another controller without interference

Direct transfer

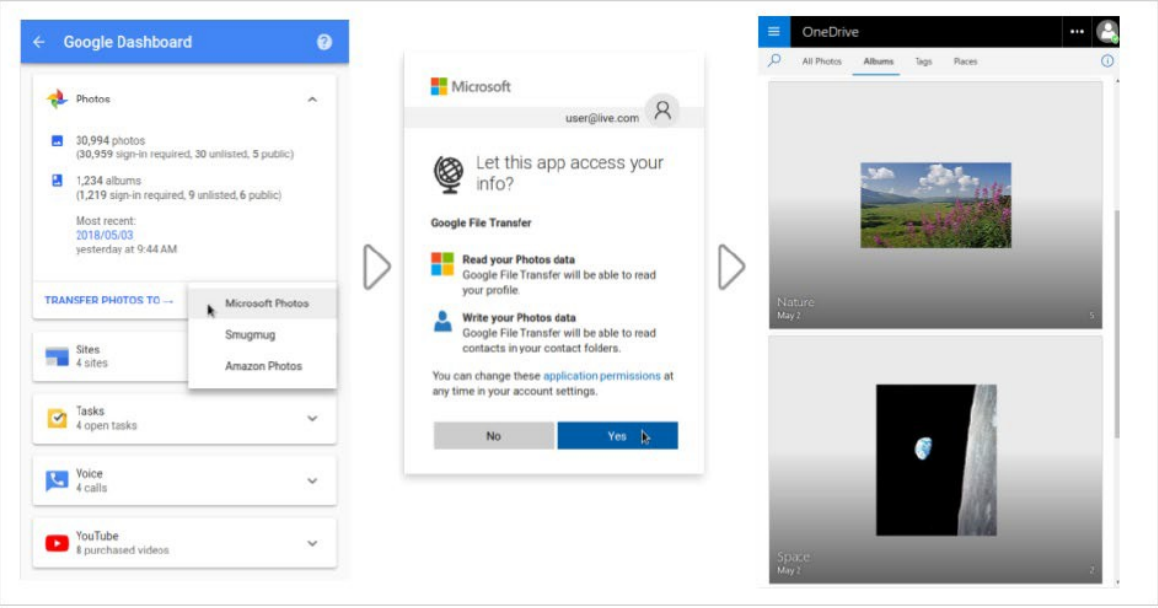
- The right to transfer directly between controllers (not through the principal) where technically feasible

GAFA's measures to address data portability are advancing

- A five-company consortium of Facebook, Google, Microsoft, Twitter, and Apple is working to achieve direct transfer data portability.

Illustration of Data Portability Based on DTP (Data Transfer Project)

Select the data you want to transfer on the Google dashboard → **Transfer data to Microsoft OneDrive**

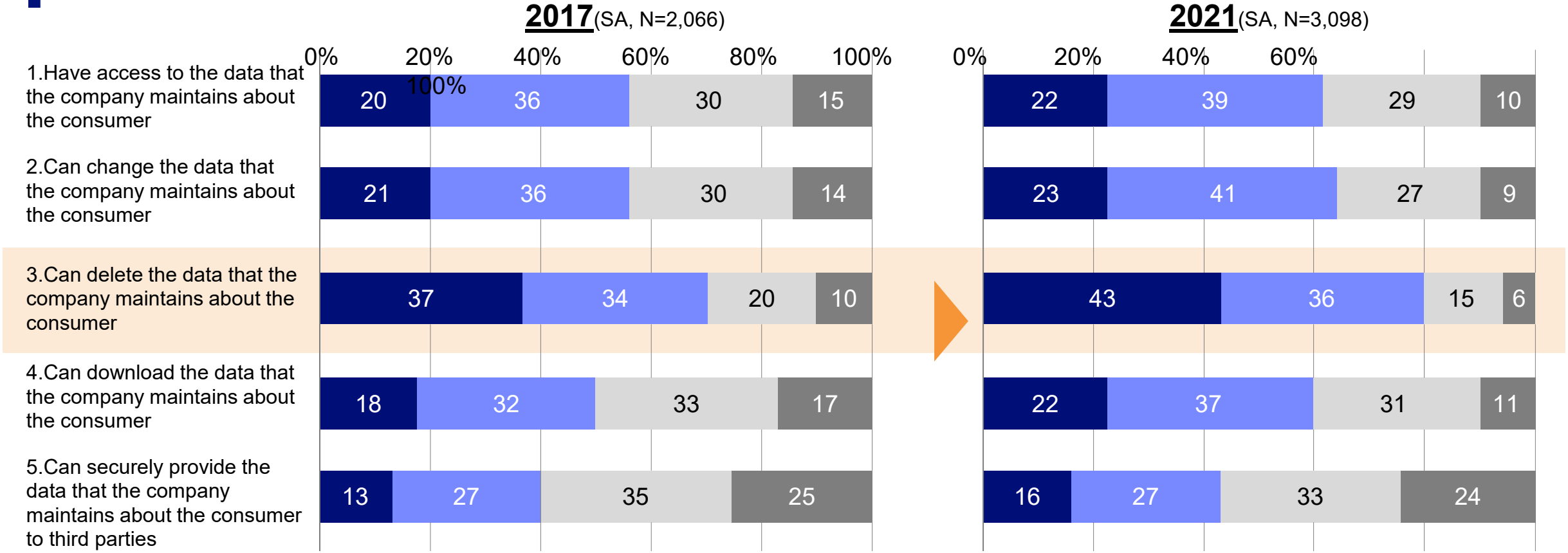


Source: "Data Transfer Project Overview and Fundamentals" (DTP White Paper, July 20, 2018)

2. Will regulation of GAFA revitalize data distribution? ｜Consumer mentality leaning toward “protection” rather than “usage”

Japanese consumers remain wary of data distribution, and there is a strong need to “erase the actual data that companies manage”

Functions/Services Sought by Consumers



Source: NRI ”Questionnaire Survey on Information and Communication Services” (July 2017 and July 2021) Survey method: Web-based questionnaire; survey target: consumers aged 15-69 residing in Japan

Part 2 Conclusion

Will regulation of GAFA revitalize data distribution?

- Data for web services is mostly collected by Google; GAFA are actively collecting IoT data, and data will continue to be concentrated among GAFA.
- Although the right to data portability was established in the GDPR to open up the data gathered by GAFA, it is not currently having the desired effect, as GAFA are responding with concerted efforts.
- **With consumer mentality leaning toward "protection," even if data portability is achieved, there is concern that data will remain with GAFA or be erased without being distributed. Companies need to take action to gain the trust of consumers and get their data back from GAFA.**

01 Why is the APPI repeatedly amended?

02 Will regulation of GAFA revitalize data distribution?

03 Proposals for necessary “privacy investments”

3. Proposals for necessary “privacy investments”

Companies that cannot invest in privacy will be weeded out

- Privacy investments are needed on two fronts: “defensive” for legal measures and “offensive” to use data to counter GAFA.

3. Proposals for necessary “privacy investments” ｜Building privacy governance

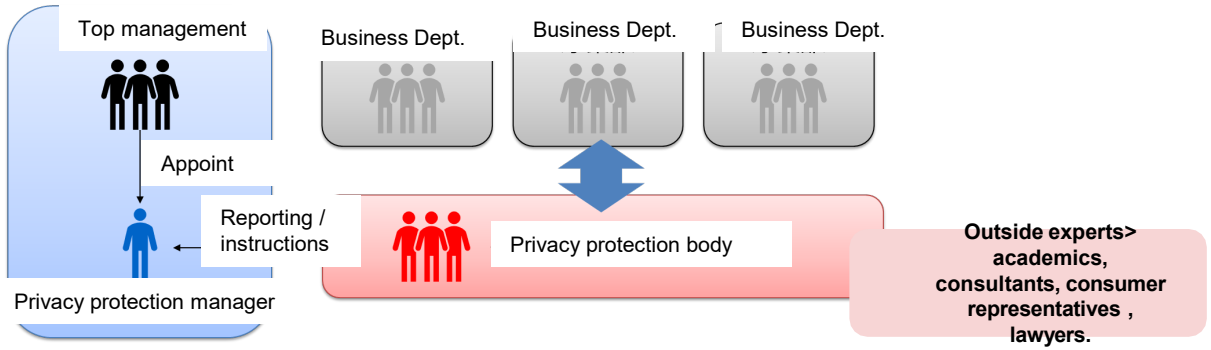
The Government has published a guidebook and recommends building privacy governance

Three commitment requirements for top management

Requirement 1: Put commitments to privacy governance in writing
Top management should put in writing their basic approach and stance on privacy as a key challenge in management strategies, and publicize them among internal and external stakeholders. They must ensure accountability for their actions in accordance with what was put in writing.

Requirement 2: Designate privacy protection manager
Appoint an official responsible for handling privacy issues across the organization and provide the official with both authority and responsibility.

Requirement 3: Allocate resources for addressing privacy
Put sufficient resources (human, physical and financial) in stages to establish a system, and allocate, develop, and secure human resources.



Privacy governance: important items

1. **Establish a system** (internal control, creating a body for privacy protection, collaborating with outside experts)
2. **Formulate and disseminate operation rules** (formulate rules for reliable operation, and publicize them internally)
3. **Foster corporate culture on privacy** (foster corporate culture so that each employee is aware of privacy issues)
4. **Communication with consumers** (publicize the organization’s efforts and stay in touch with consumers)
5. **Communication with other stakeholders** (communication with business partners, group companies etc., investors and shareholders, government agencies, industry groups, and employees etc.)

Enhance enterprise value and gain an edge in business

Gain public trust

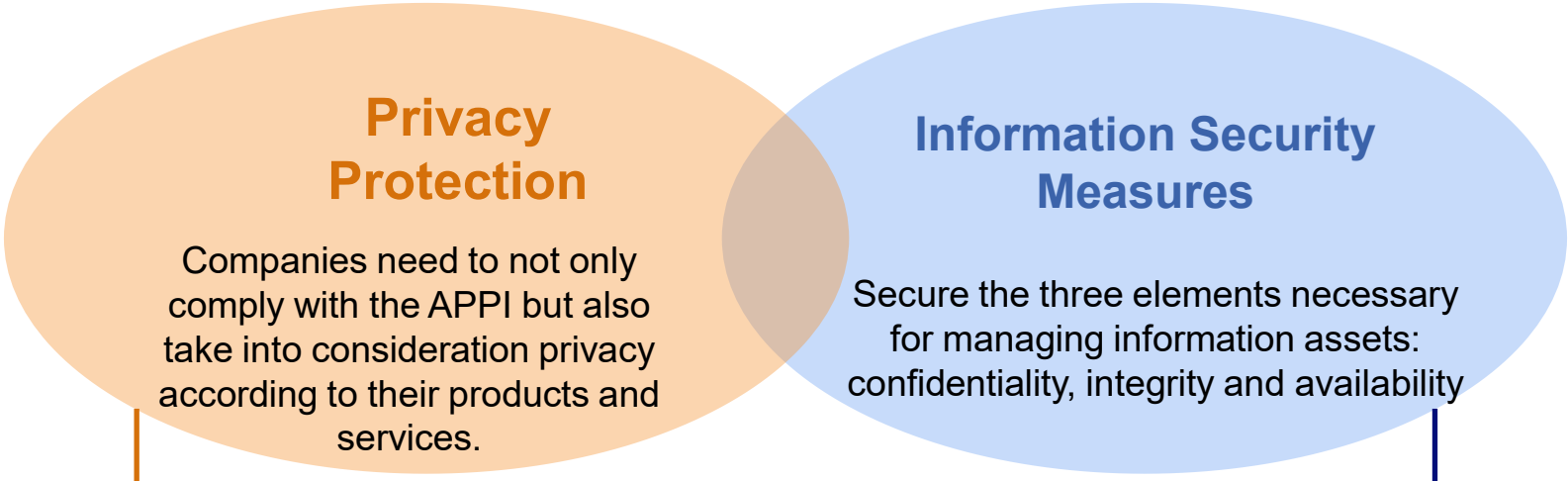
Consumers and other stakeholders

Source: https://www.meti.go.jp/policy/it_policy/privacy/guidebook11gaiyo.pdf
Ministry of Internal Affairs and Communications, and the Ministry of Economy, Trade and Industry; Corporate Privacy Governance Model Meeting, Guidebook on Corporate Governance for Privacy in Digital Transformation (DX) Age ver1.1: Summary (July 2021）

3. Proposals for necessary “privacy investments” | Building privacy governance

Privacy protection and information security measures are fundamentally two different things, and should be handled by separate supervisors and organizations

Relationship between Privacy Protection and Information Security Measures



- Consists primarily of communication with individuals
- Information security is part of protection activities

- Activity closed to business operators
- Personal data is part of information assets

3. Proposals for necessary “privacy investments” | Building privacy governance

Four key questions to ask when establishing an organization for privacy protection

Question	Main points
a. Privacy dept. vs Information security dept.	● In what areas will the privacy department work with the information security department, and in what fashion?
b. Corporate dept. vs business dept.	● Should the corporate and business departments be handled by a single organization, or by separate organizations?
c. Dedicated vs “many hats”	● Perhaps it is possible to maintain the organization for privacy protection by having such back-office departments as legal affairs, information security, and risk control take on additional duties or collaborate with one another? ● If it is difficult to set up a company-wide, dedicated organization from the start, how about having each business dept. designate a privacy protection officer and create a virtual organization consisting of these officers?
d. CPO (Chief Privacy Officer) vs DPO (Data Protection Officer)	● CPOs and DPOs, while both designed to promote privacy management, have significantly different positioning and roles. • CPO: strategic management for a company’s privacy program. May need implement management from a marketing perspective • DPO: executes GDPR-stipulated work ● What qualifications are required of a privacy protection supervisor?

3. Proposals for necessary “privacy investments” | Building privacy governance

Building privacy governance step-by-step

- It would be best to establish organizations for privacy protection, but they cannot be created overnight
- They need to be established step-by-step according to the actual situation of each company

Step 1
Ascertain personal data to be handled

- Through data mapping, take stock of what kind of data is handled by the company’s businesses and whether the company is in compliance with the APPI.

Step 2
Update rules

- Based on the results of data mapping, update rules on data handling.
- Update internal rules so that they are consistent with notices for users.

Step 3
Implement privacy measures

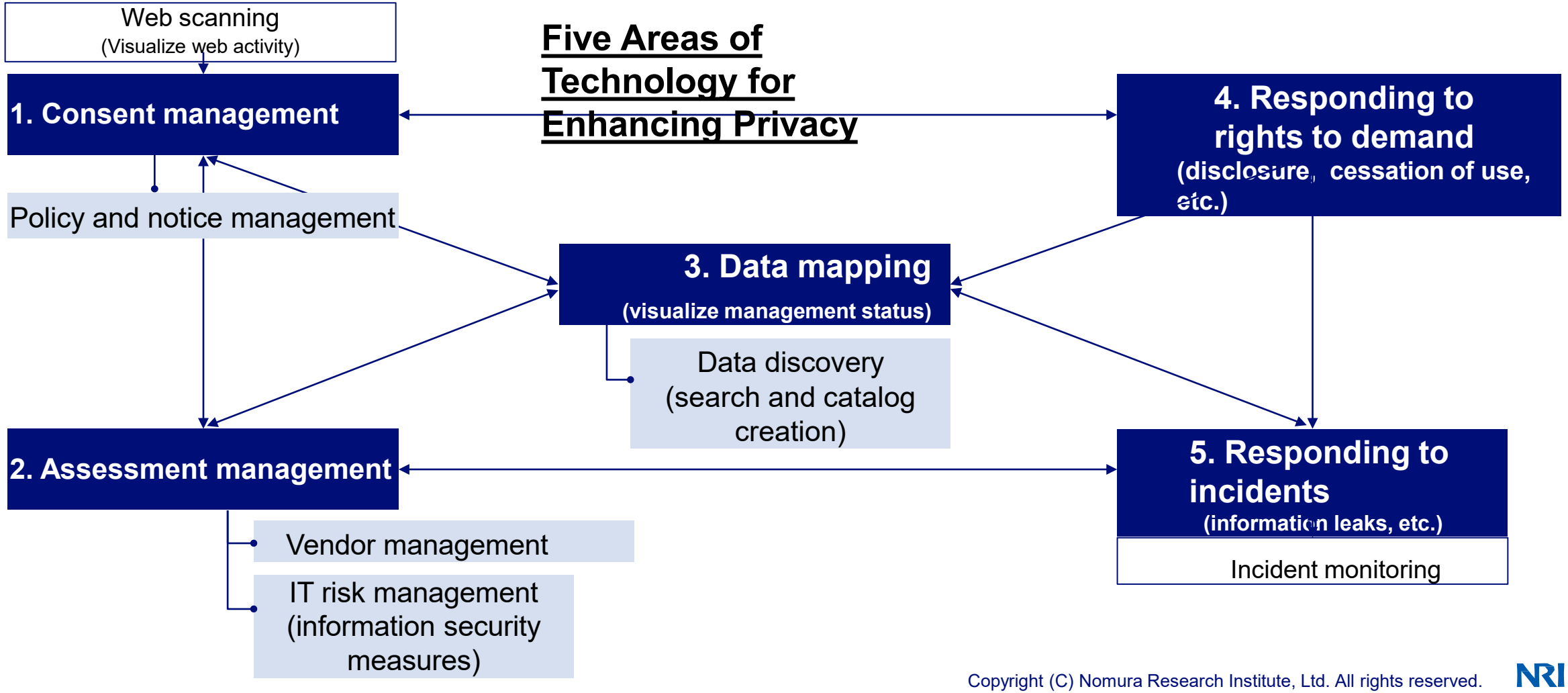
- Establish an organization for privacy protection to work on privacy governance systematically.
- Have the organization chiefly work on privacy impact assessments (PIA).
- Use countermeasures for risk management involving stakeholders to accumulate knowhow in countermeasures.

Step 4
Enhance efficiency & sophistication of privacy measures with technology

- **Manual management** with Excel, etc. **has its limitations; utilize technology for enhancing privacy (or privacy tech; see the next slide)** to implement privacy measures in an easy, reliable, and efficient manner.

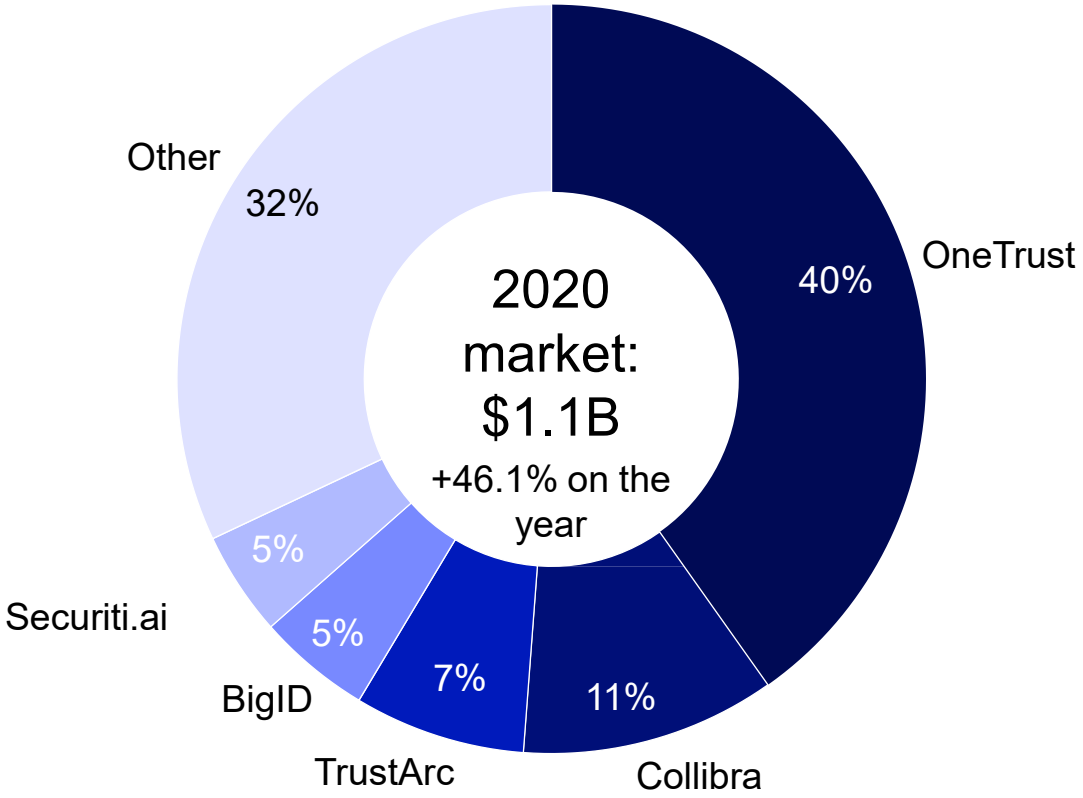
3. Proposals for necessary “privacy investments” | Utilizing technology to streamline and enhance governance

Privacy tech: Visualizes how personal data is stored and used, and enables smoother internal communication about data usage and protection



In the field of privacy tech, start-ups are gaining attention

Privacy management software: market shares



Source: Compiled by NRI, using OneTrust website (source: IDC report)
https://www.onetrust.com/resources/idc-market-shares-2020/

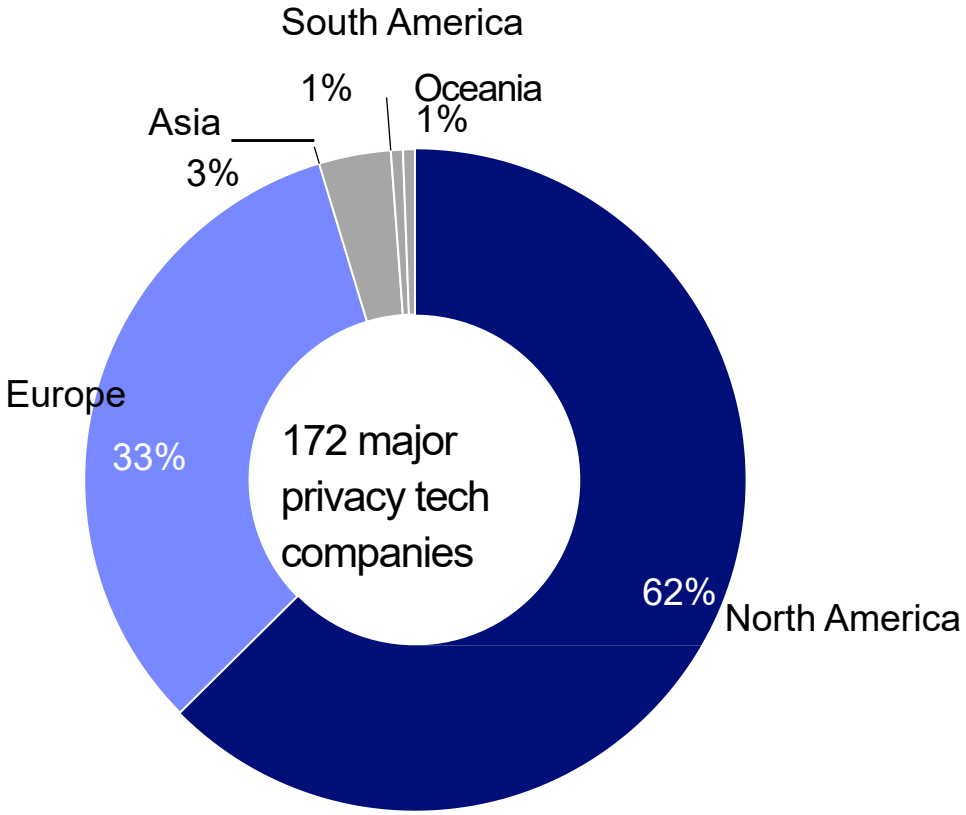
Privacy tech companies (in order of market share)	Profile	
OneTrust	Founded	2016
	Offices	Atlanta, London
	Remarks	Provides several modules ★Partner agreement with NRI
Collibra	Founded	2008
	Offices	New York
	Remarks	Strong in data catalogs that can be linked to privacy policy
TrustArc	Founded	2002
	Offices	Toronto
	Remarks	Strong in regulatory compliance status management and risk control modules
BigID	Founded:	2016
	Offices:	New York
	Remarks	Strong in data discovery, provides consent management and several other modules
Securiti.ai	Founded:	2018
	Offices:	California
	Remarks	Strong in data discovery, enables on-premise cloud data linkage

Source: Prepared by NRI based on the websites.

3. Proposals for necessary “privacy investments” | Utilizing technology to streamline and enhance governance

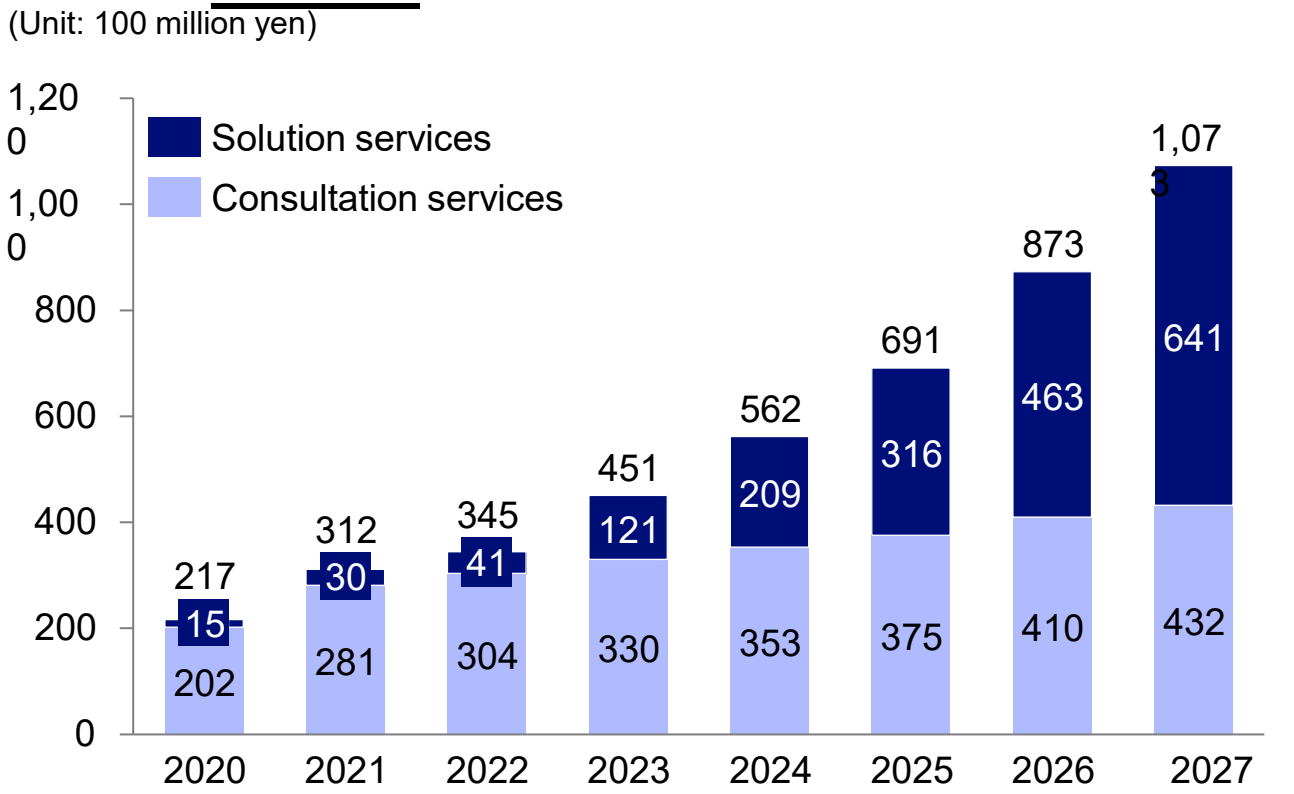
Privacy tech has been adopted chiefly in Europe and the U.S.; going forward, wider use is expected in Japan

Privacy tech companies: headquarters locations by region



Source: Compiled by NRI based on privacy tech companies’ addresses listed in Crunchbase

Privacy-related market in Japan: forecast



Note: FY2020: NRI estimate, FY2021 and beyond: forecast
Source: NRI, IT Navigator 2022 version

In addition to building privacy governance, it is essential to utilize technology for efficiency and sophistication

- The Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry have published a dedicated guidebook and recommend that corporations build privacy governance. Privacy measures are not something that can be undertaken as an extension of security measures. Companies seeking to use personal data must have a dedicated privacy protection organization.

- Privacy governance needs to be built in phases. The first step is to perform data mapping and verify what type of data is handled in company businesses.

- Manual governance has its limits. Privacy technology is increasingly being used in the U.S. and Europe. Privacy technology allows for visualization of personal data storage and usage and enables smoother internal communication on data usage and protection.

Duplicate

3. Proposals for necessary “privacy investments”

Companies that cannot invest in privacy will be weeded out.

- Privacy investments are needed on two fronts: ”defensive” for legal measures and ”offensive” to use data to counter GAFA

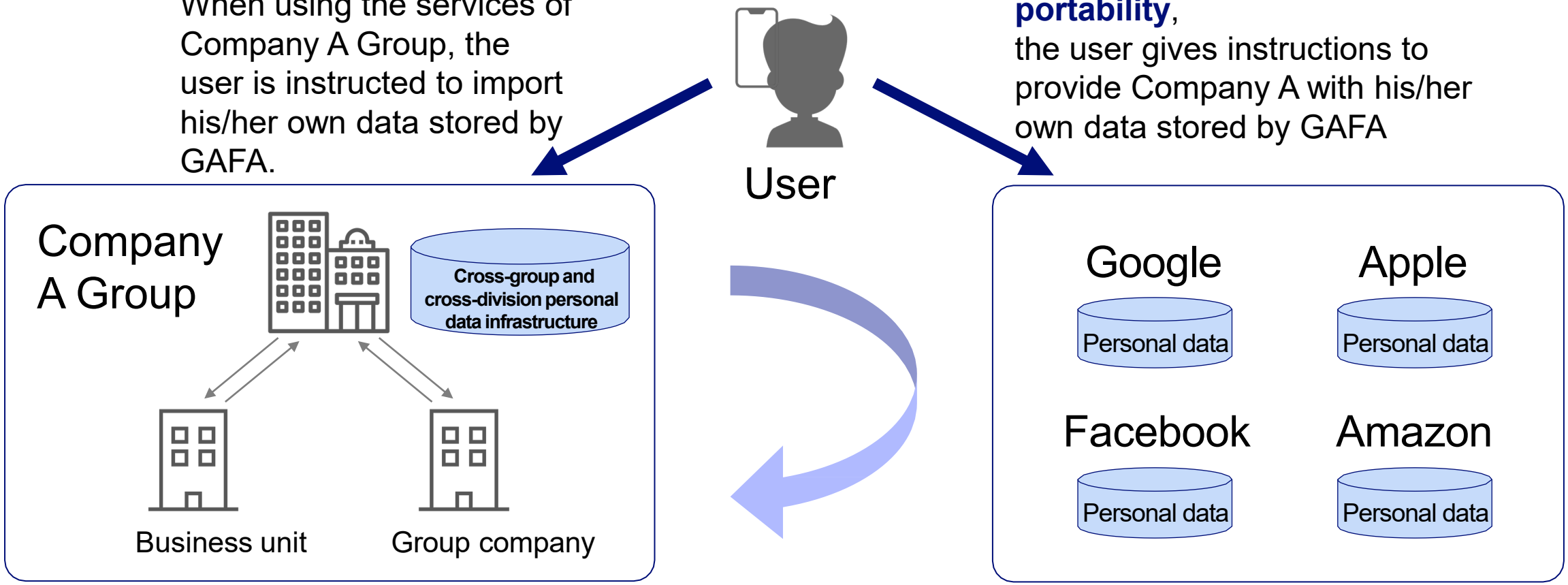
3. Proposals for necessary “privacy investments” | Utilizing data across group companies and divisions

Offensive Privacy Investments

In order to support data portability and incorporate GAFA data, it is necessary to establish a centralized personal data management system and structure.

When using the services of Company A Group, the user is instructed to import his/her own data stored by GAFA.

Exercising **the right to data portability**, the user gives instructions to provide Company A with his/her own data stored by GAFA



Offensive Privacy Investments

Make your own rules and develop areas where you can utilize data

To create rules to fill in the areas where the applicable scope of legal regulations is unclear (gray zones), companies will create their own rules to fill in the gray zones, and develop white zones where data can be used safely and securely.

Key Points of Rulemaking

- **Meet consumer expectations (use opt-out correctly so as not to surprise them)**
- **Utilize a multi-stakeholder process**

Precedents for rulemaking

NTT DoCoMo, Inc. Mobile Spatial Statistics	**JR East** Sale of Suica data (second attempt)	**Television broadcasters, etc.** Viewing data

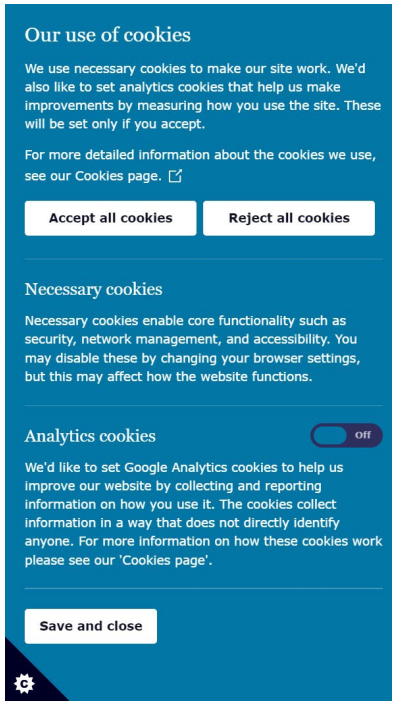
3. Proposals for necessary “privacy investments” | Developing white zones through rulemaking

Since opt-in* significantly reduces the amount of data available, opt-out rules must be created in light of the risk of flaming incidents

*Obtaining prior consent from the individual for the handling of data

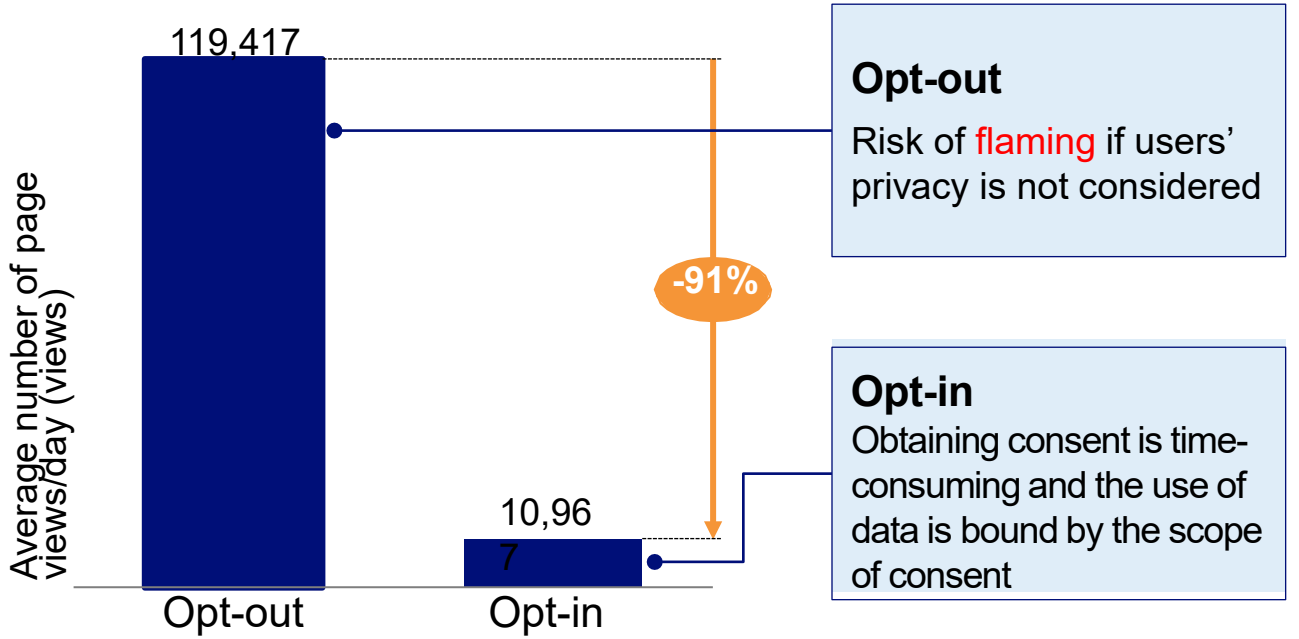
- The UK’s privacy authority (ICO) tested its own website and found that 91% of users did not consent to the use of cookies when they changed their consent from opt-out to opt-in.

ICO Website Cookie Consent Screen



Source: ICO Website

Change in Number of Page Views Due to Change in Method of Obtaining Consent



Note: The number of page views per day is calculated as the average of the three months before and after the change in the method of obtaining consent

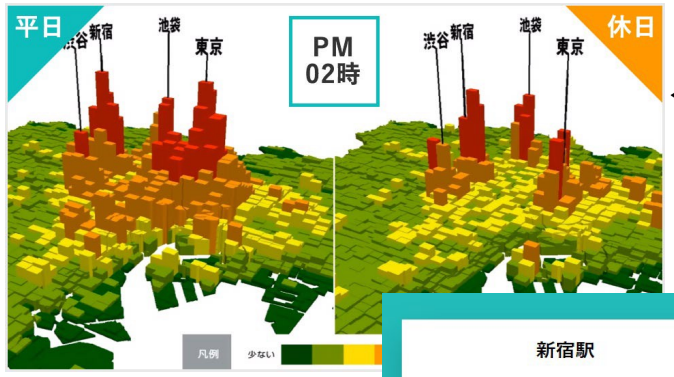
Source: Prepared by NRI based on publicly available materials of the UK privacy authority (Information Commissioner’s Office)

3. Proposals for necessary “privacy investments” | Developing white zones through rulemaking

NTT DOCOMO: Mobile Spatial Statistics
Mobile phone location information is utilized in an opt-out manner

- NTT DOCOMO’s “Mobile Spatial Statistics” uses location information related to base stations to estimate geographic distribution by aggregating the number of cell phones in each base station area by user attributes.

Examples of Data Applications for Mobile Spatial Statistics



← Distribution of people in a given area
https://mobaku.jp/service/jpn_distribution/

Coronavirus measures → Population change rate in major areas
https://mobaku.jp/covid-19/

Opt-Out screen (Personal Data Dashboard)

https://datadashboard.front.smt.docomo.ne.jp/

Provides consumers with a means to opt out of data use without obtaining explicit consent.

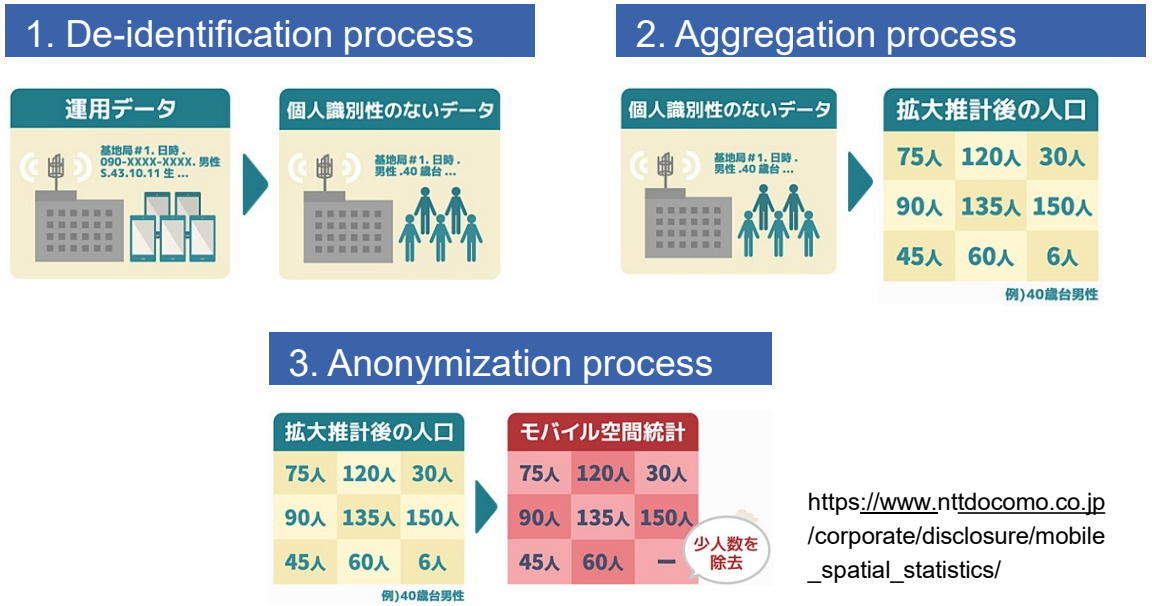
Offensive Privacy Investments

3. Proposals for necessary “privacy investments” | Developing white zones through rulemaking

NTT DOCOMO: Established voluntary rules (guidelines) based on prior discussions with experts in order to use mobile phone location data without obtaining consent.

- Started empirical research in the field of disaster prevention around 2010, and started service in October 2013.
- Organized the ”Study Group on Social and Industrial Development through Mobile Spatial Statistics,” an expert panel, to develop guidelines.

Procedures for Creating Mobile Spatial Statistics



https://www.nttdocomo.co.jp/corporate/disclosure/mobile_spatial_statistics/

Source: NTT DOCOMO Mobile Spatial Statistics Website

Members of Expert Panel

- **Jurist (Chair)**
  Masao Horibe, Professor Emeritus, Hitotsubashi University
- **Information Economy Expert**
  Akihiko Shinozaki, Professor, Graduate School of Kyushu University
- **Statistics Expert**
  Takeshi Hiromatsu, Professor, Institute of Information Security
- **Consumer Perspective Advocate**
  Sawako Nohara, President, IPSe Marketing Inc.
- **Attorney**
  Tsunemichi Yokoyama, Attorney at Law, Mori Hamada & Matsumoto

3. Proposals for necessary “privacy investments” | Developing white zones through rulemaking

NTT DOCOMO: Mobile Spatial Statistics are worth using

Comparison with Similar Services

Target		Data acquisition	Sample size	Area	Resolution	Attributes	Route analysis
Mobile Spatial Statistics (base station data)	Japan residents	24/365 (only when powered on)	80M	Nationwide	125m mesh (approx)	Gender, age, area of residence, industry, family structure, hobbies and interests, etc.	○
	Foreign visitors		12M		1Km mesh (approx)	Country and region, length of stay, airports of entry and exit, etc.	
Wi-Fi data	Japan residents	24/365 (In addition to being powered on, an application/Wi-Fi connection is required.)	-	Wi-Fi hot-spot areas	100m mesh (approx)	Gender, age, etc. (based on consent)	△
	Foreign visitors		~1.7M			Country, region, etc. (based on consent)	
GPS data	Japan residents	24/365 (In addition to being powered on, GPS needs to be on)	~.5M	Nationwide	100m mesh (approx)	Gender, age, etc. (based on consent)	○
	Foreign visitors		~.1M		125m mesh (approx)	Country, region, purpose of visit, etc. (based on consent)	
National census	Permanent residents	Once every five years	All households	Nationwide	town/block level (500m mesh)	Gender, age, occupation, family/resident status, educational history, etc.	-
Traffic volume survey	-	Survey period	Passers-by in the survey area	Specific areas		Gender, age (estimate)	-

Features of Mobile Spatial Statistics

- Highly accurate population information estimated from a large sample size
- Know hourly population 24 hours a day 365 days a year
- Possible to analyze not only domestic residents but also foreign visitors
- Also provides past population data

Source: NTT DOCOMO Mobile Spatial Statistics Website

Offensive Privacy Investments

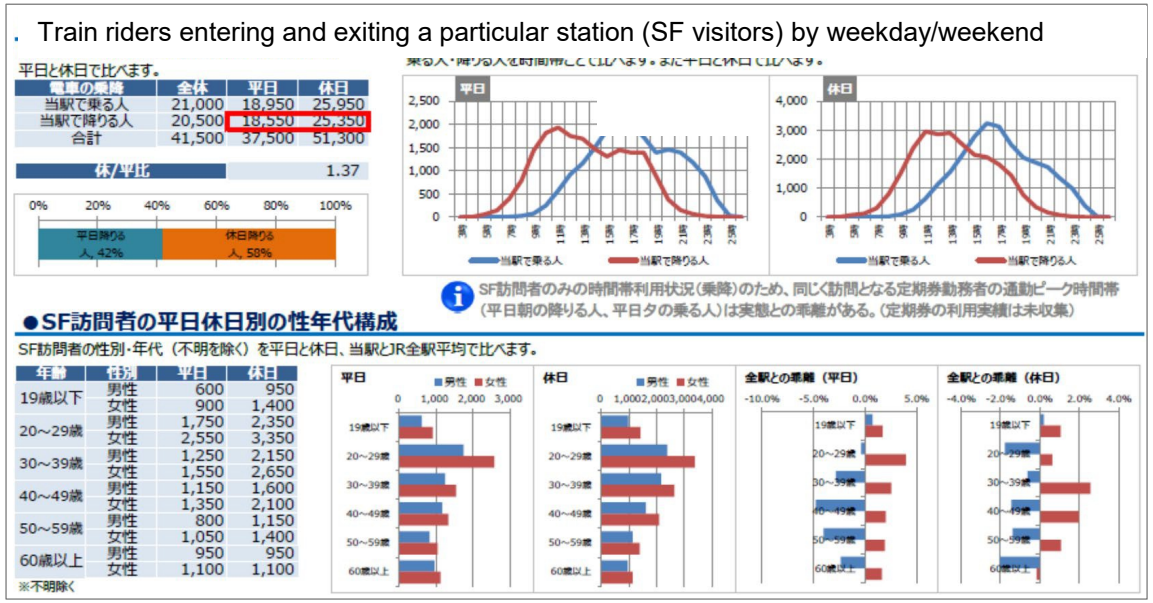
3. Proposals for necessary “privacy investments” | Developing white zones through rulemaking

JR East: Sale of Suica Data (Second Attempt) Thoroughly considering privacy and creating statistical information “Station Charts”

- JR East has been promoting privacy protection efforts since the Suica incident in 2013
- In January 2022, it announced plans to sell statistical information “Station Charts” to municipalities and outside the company.

Number of Suica users per station by time of day, gender, and age

Train riders entering and exiting a particular station (SF visitors) by weekday/weekend



https://www.jreast.co.jp/press/2021/20220120_ho01.pdf

Source: JR East News Release (January 20, 2022)

Overview of “Station Charts”

- Monthly Suica usage data is aggregated to provide a standardized report showing usage at each of the approximately 600 stations in the JR East metropolitan area
- Average values per month (by weekday and non-workday), calculated by the hour and 10-year age groups
- Aggregated in units of 50 (less than 30 not shown)
- Reports in PDF format (with security features)

3. Proposals for necessary “privacy investments” | Developing white zones through rulemaking

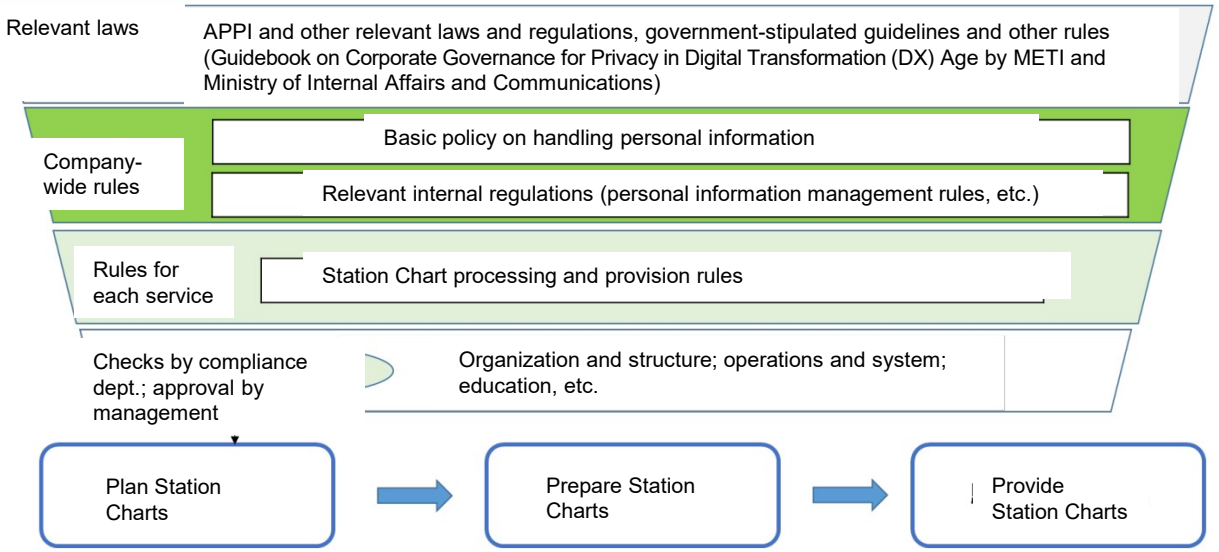
JR East: Working to build trust with users and society

- JR East is emphasizing efforts to meet the expectations of users by communicating its achievements in highly public projects and publicly announcing the status of its establishment of rules and regulations.
- Consent for data utilization is not obtained and opt-out means are provided

Efforts to build trust with users and society

Efforts	Overview
Communicating information to users	● Continuing provision of opt-out window ● Continuing provision of easy-to-understand information on company website etc.
Communicating achievements in highly public projects	● Covid-19 impact case studies ● Examples of service improvement ● Examples of provision to local governments
Establishment of rules and regulations	● Strict data management in accordance with laws, regulations, and rules ● Preparation of rules on processing and provision of “Station Charts”

Establishment of rules and regulations for the provision of “Station Charts”



https://www.jreast.co.jp/press/2021/20220120_ho01.pdf

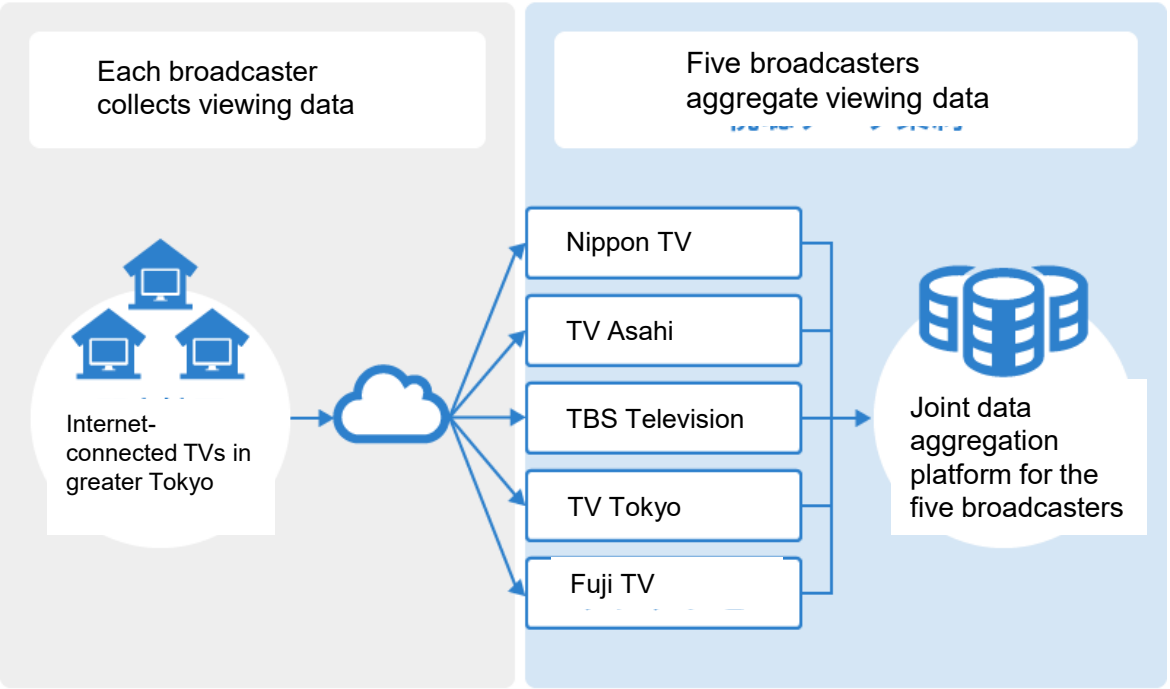
Source: JR East News Release (January 20, 2022)

3. Proposals for necessary “privacy investments” | Developing white zones through rulemaking

Viewing data: through demonstration projects and multi-stakeholder consultations, data utilization rules are being carefully considered (2018-present)

Notice of demonstration project jointly conducted by five commercial broadcasters (excerpt)

Viewing data collection and aggregation: flow chart



https://www.tv-viewing-log.info/2019/

Source: “Five Commercial Broadcasters’ Joint Technical Verification and Operational Demonstration Experiment on TV Viewing Data” (December 13, 2019).

Members of Council on Handling of Viewing-Related Information etc.

- **Experts/consumer representatives**

Takashi Uchiyama, Professor, School of Cultural and Creative Policy, Aoyama Gakuin University
Jouji Shishido, Professor, Graduate Schools of Law and Politics, University of Tokyo
Ryoji Mori, Attorney at Law, Eichi Law Offices
Junichiro Makita, Attorney at Law, Harago & Partners Law Offices
Keisuke Uehara, Associate Professor, Faculty of Environment and Information Studies, Keio University
Miki Osada, Information and Communication Consumer Network

- **Commercial broadcasters (Tokyo key stations, Osaka, Nagoya, BS representative stations)**
- **Pay-TV operators (JCOM, SKY PerfecTV, WOWOW)**
- **TV manufacturer (Toshiba, Sony, Panasonic)**
- **Broadcasting-related organizations (NHK, Japan Commercial Broadcasters Association, Japan Cable and Telecommunications Association, Japan Satellite Broadcasting Association)**
- **Observers (Dentsu, Hakuhodo, Yomiuri Shimbun, JEITA, Ministry of Internal Affairs and Communications)**
- **Secretariat (SARC, Nomura Research Institute, Ltd.)**

Source: Council on Handling of Viewing-Related Information, "Practices for Handling Non-Specific Viewing History Obtained by the Opt-Out Method (ver. 2.1)" (March 2021)

3. Proposals for necessary “privacy investments” | Developing white zones through rulemaking

Viewing data: The Council wrapped up discussions on the need for consent, and compiled a set of norms on the scope of opt-out-based data utilization.

Consent not required?

- Web browsing services send browsing history to the server side without obtaining consent.
- Viewing data alone cannot be used to identify a specific individual, so it does not fall under personal information.
- The consent process could discourage the use of services.

Consent required?

- Television was for many years a one-way service, so the transmission of viewing data is incomprehensible to the average viewer.
- Viewing data can be used to infer personal tastes and preferences. Many viewers feel a sense of privacy even if they cannot be identified.
- Including a consent process and gaining viewer trust will lead to a wider range of service possibilities.

Practices for handling non-identifying viewing history obtained by the opt-out method

Through discussions in a multi-stakeholder council with experts and consumer representatives, practices that allow data use on an opt-out basis for “analysis and reporting” and “program promotion (in-house use)” in combination with external data were announced.

Offensive Privacy Investments

Investments are required for both protection and utilization of personal data, in terms of both system development and rulemaking

- In order to support data portability and incorporate GAFA data, it is necessary to establish a centralized personal data management system and structure

- Through the development of white zones (elimination of gray zones) through rulemaking, consumer safety and security can be secured, and companies can focus on their data utilization businesses

(Key points for achieving both protection and utilization of personal data)

1. It is assumed that users will be made aware of the fact that their data is being utilized and that an easy way to opt out will be provided for those users who do not want their data to be utilized.
2. Data utilization should be in line with the characteristics and context of the product/service and remain within the scope of user expectations (so that users will not be surprised).
3. When using anonymized information or statistical information, it is essential to ensure anonymity so that specific individuals cannot be identified from processed data.
4. It is important to ensure compliance and social acceptance of data utilization through a multi-stakeholder review process that includes experts, consumer representatives, and industry participants, and through the compilation and publication of a code of conduct.


Share the Next Values!