EUJUS FLOW

A strategic approach to tracking international cross-border data flows across the EU-JAPAN and the US.
CONTENT

Introduction and landscape 3
  Evidentiary landscape 5
  Legal implications for digital evidence collection 8
  Possible conflicts 9

Collecting digital evidence 9
  Developing a basic foundational understanding of data 9
  Data definition 10

Developing a methodological framework 11
  Phase 1: Recognize 11
  Phase 2: Collect 11
  Phase 3: Extract 12
  Phase 4: Protect 12
  Phase 5: Analysis and Reporting 13

Case Study—the synergies between the Japanese gaming industry and EU-JAPAN-US Transfers 14
The strategic plan presents an analysis of potential data flow channels across the EU, US and Japan, based on file data from a similar investigation. The case study deconstructs the collection and transfer of data across the three jurisdictions into 6 main areas of planning (building data capacity, data goals, data collection methodologies and techniques, tracking and monitoring, evaluation and analysis). The analysis identifies underlying activities and processes which intersect at each jurisdiction in transferring data across the three jurisdictions. Furthermore, it analyses the required resources, equipment and relations of the transfers and examines the actors involved and the legal processes that might both facilitate and hinder data collection.

Introduction and landscape

Article 48 of GDPR blocks personal data transfers to third countries pursuant to a judgment by a court or administrative body of that third country unless the transfer is authorized by an international agreement or one of the other grounds in Articles 45–47 or 49. The EU’s executive branch or the European Commission can determine whether a third country has an adequate level of data protection and may issue an adequacy decision to the third country. An adequacy decision permits a cross-border data transfer outside the EU, or onward transfer from or to a party outside the EU without further authorization from a national supervisory authority (Article 45(1), GDPR). In 2019, the EU, based on compliance with the requirements, determined that Japan had met the standards to warrant an adequacy decision.
The existence of Japan's Personal Information Protection Commission (PPC), additional protections, mechanisms for investigations, and venues for complaint resolutions reinforced the reciprocal adequacy decision with the EU. Japan's PPC may be called on by the European Data Protection Board (EDPB) as the point of contact for extra-territorial jurisdiction in the event of a breach in Japan affecting the personal data of EU citizens, and vice versa. On the EU side, the adequacy finding was decided based on a series of additional safeguards that Japan will apply to the data of Europeans when transferred to their country. These safeguards are intended to bridge certain differences between the two data protection systems: for instance, the Japanese definition of sensitive data will be expanded, the exercise of individual rights will be facilitated, and the further transfer of European data from Japan to another third country will be subject to a higher level of protection. Japan also agreed to establish a system of handling and resolution of complaints, under the supervision of the Japanese data protection authority (the Personal Information Protection Commission), to ensure that potential complaints from Europeans regarding access to their data by Japanese law enforcement and national security authorities will be effectively investigated and resolved.

In 2022, the European Commission and the U.S. government announced an important agreement governing the transfer of data between the EU and the U.S. This new Trans-Atlantic Data Privacy Framework is designed to rebuild and strengthen the data protection bridge between the EU and the U.S. by addressing the concerns of the Court of Justice of the European Union when it invalidated the original Privacy Shield framework in 2020. For example, the new framework ensures that:

- The collection of signals intelligence may be undertaken only when necessary to advance legitimate national security objectives, and must not have a disproportionally impact on the protection of individual privacy and civil liberties;

- EU individuals may seek redress from a new multi-layer redress mechanism that includes an independent Data Protection Review Court that would consist of individuals chosen from outside the U.S. Government who would have full authority to adjudicate claims and direct remedial measures as needed; and

- U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards.

This Framework will provide vital benefits to citizens on both sides of the Atlantic. For EU individuals, the deal includes new high-standard commitments regarding the protection of personal data. For citizens and companies of the EU and the U.S, the deal will enable
the continued flow of data that underpins more than $1 trillion in cross-border commerce every year, and will enable businesses of all sizes to compete in each other's markets. It is the culmination of more than a year of detailed negotiations between the EU and the U.S. following the 2020 decision by the Court of Justice of the European Union ruling that the prior EU-U.S. framework, known as Privacy Shield, did not satisfy EU legal requirements. The existing personal data protection legislation in the United States, Europe, and Japan is currently three representative forms. The US model is an industry self-discipline model, which focuses on industry self-discipline, supplemented by national legislation. The US model is also based on the right to privacy and relies on relevant supplements in different laws, essentially adopting a decentralized legislative approach. After the adoption of the General Data Protection Regulation, all existing personal data use links have been opened up. Because of the unified standards, this can promote the flow of information and resource sharing among all EU countries. The Japanese model combines the characteristics of the United States and Europe and adopts the mature part of the two an adequacy approach (in combination with the APEC CBPR) that allows data flows with countries in several regions. The goal laid out in this strategy is to determine whether there is a potential violation of EU law due to the use of Japan as a 'data haven' and to point out the incongruence in both the legal frameworks as well as the practical data protection standards.

Evidentiary landscape

The Budapest Convention on Cybercrime of the Council of Europe is the most relevant international instrument on Cybercrime and Digital Evidence. Opened for signature in 2001, with currently 66 Parties spread around the world, its scope of application is not restricted to the borders of Europe. It aims to create a global framework on cybercrime and digital evidence among practitioners from a very diverse array of jurisdictions, facilitating international cooperation in criminal cases, with substantive and procedural provisions. This legal framework includes provisions for collecting digital evidence in emergencies, directly from service providers, with extra-territorial powers and on international cooperation.

More than 20 years have passed since the drafting of the Budapest Convention, but its criminal substantive aspects, technology neutral in their provisions, remain fully updated. However, in relation to the provisions that support the operational work of Law Enforcement and Judicial Authorities, in view of new introduced technologies such as Cloud Computing and its impact in territoriality and jurisdiction, specific solutions were needed and brought forth by a second Additional Protocol to the Budapest Convention,
approved in November 2021. In response to the identified challenges related to cross border gathering and sharing of digital evidence, the recently approved second Additional Protocol presents new provisions on disclosure of domain name registration information, direct cooperation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate cooperation in emergencies, and a specific provision on Joint Investigations Teams (JITs).

The text was opened for signature in Strasbourg on the 12th May 2022. Other very relevant EU legal instruments for lawful collection of electronic information in cross-border investigations are the Mutual Legal Assistance Treaties (MLATs), and the European Investigation Order (EIO), which replaced MLATs in the context of a subset of participating EU members (EU members except for Denmark and Ireland). These cooperation instruments rely on the independent judicial scrutiny of the competent authorities in the different countries to guarantee that the corresponding investigation requests and retrieved information are lawfully obtained during investigation processes. The EIO aims to speed up cooperation by extending the principle of mutual recognition in evidence gathering. Thus, EU participating member states and their corresponding judicial authorities are entrusted with the task of checking the legitimate grounds to either refuse or execute an EIO. An interesting feature of the EIO Directive is that, in conformity with the EU Charter on Human Rights art 47, allows the defense, as well as the victim’s lawyer, to request a Court to issue an EIO to obtain digital evidence.

This possibility enables lawyers, in equal arms with Prosecution Services, to seek access to the electronic data before it is deleted by requesting the issue of an EIO within the framework of applicable rights of suspects and victims, in conformity with the national criminal procedure or directly in the competent court of the issuing state. The MLAT process is the most widely used international cooperation protocol (i.e., MLAT also covers cases in which some of the EU members that want to co-operate are not bound by the EIO Directive). Thus, an MLAT is used to request data residing in countries such as Denmark, Ireland, as well as non-EU countries such as the US or Japan. The main issue with the MLAT requests is that such a procedure was designed before the consolidation of the Cloud as the primary storage platform of most decentralized services on the Internet. Hence, due to this paradigm shift, the increase of cyberthreats that required cross-border co-operation hindered the efficacy of MLATs. As a consequence, the MLAT is currently regarded as an insufficient method to cope with actual needs due to its slowness and the resources that it requires. To reduce the burden and speed up the acquisition of electronic data that law enforcement and judicial authorities need for investigating and successfully prosecuting criminals and serious crimes, such as
terrorism, the EU Commission created the E-evidence initiative, which consists of two main tools, the European Production Order (EPROD) and the European Preservation order (EPRES). The EPROD allows a judicial authority in one Member State to obtain electronic evidence directly from a service provider or its legal representative (thus, entails the creation of such a figure in each corresponding service provider) in another Member State. The EPROD imposes a very strict response time (within 6 hours in case of emergencies and to a maximum of 10 days, compared to 120 days in the case of EIO and an average of 10 months for MLAT).

The EPRES allows a judicial authority in one Member State to request that a service provider or its legal representative in another Member State preserve specific data given a subsequent request to produce this data by using either an EPROD or an EIO. A parallel instrument with a similar aim was created in the US. JITs are a tool for international cooperation in criminal matters, created by a legal agreement between competent authorities of two or more States for the purpose of carrying out criminal investigations, established for a fixed period, usually 12 to 24 months, as needed to conclude the investigation.

One of the most relevant aspects of the Clarifying Lawful Overseas Use of Data (CLOUD) Act and the E-evidence initiatives is their impact on the actual landscape since most technology corporations are based in the US and EU. Therefore, since both initiatives deviate from the principle by which the physical location in which data is stored determines jurisdiction, and both determine that in specific cases, law enforcement officers should be able to directly access a provider's data under their corresponding jurisdiction without needing an MLAT, their application could change the cross-border investigation paradigm. As noted in the literature, a series of questions are raised as to the E-evidence, and the CLOUD Act's compatibility with current legal frameworks in relation to privacy, human rights, and the necessity and proportionality principles of the requests made in the context of cross-border investigations. A clear example of the complexity of the challenges in relation to the E-evidence initiative is the still ongoing triad between the EU Commission, Council of the European Union, and European Parliament for the approval of the E-evidence Package. In the case of US-EU cooperation, the E-evidence initiative could require US-based online service providers to grant access to data in their possession.

At the same time, the Stored Communications Act forbids the provision of such access, unless there is an executive agreement with the US. On the other side, when US authorities request data stored in the EU, companies may risk breaching the EU General
Data Protection Regulation (GDPR) under Article 48, since any judgment or decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable if it is based on an international agreement, such as an MLAT. Moreover, Article 46 of the GDPR also hinders the execution of data exchange procedures on the European side if there is no mechanism allowing European individuals to have the safeguards and legal remedies comparable to those resulting from the GDPR.

Legal implications for digital evidence collection

Setting aside issues such as identity management and access rights, which are more technical, an important aspect that has to be considered is the admissibility of digital evidence in court. The questions that emerge are primarily related to the collection of digital evidence. For instance, the collection of digital evidence by involving specific methods might be admissible in one country but not in another. Thus, the exchange of digital evidence would be legal, but the evidence would not be admissible. This is rather important, especially in the eyes of authoritarian regimes, lawful interception, deception during interrogations, and in the use of AI and machine learning against use of, e.g. decentralized platforms and end-to-end encryption. All the above, individually, may punch holes in the admissibility of evidence in court while raising ethical issues.

The case of using the notorious Pegasus spyware, while exceptional, clearly illustrates how different countries consider lawful interception and surveillance. Moreover, the legality of using specific tools, methods, and the overall practice of the judicial system is questionable in many authoritarian regimes and may result in further violations of human rights. Of particular interest is the recurring discussion on encryption and access to the underlying data from the LEAs. Clearly, the abuse of encryption by criminals, not only cyber criminals, introduces many additional burdens for LEAs and digital forensics experts. This is something that troubles law and policy makers, regardless of the laws that have been adopted or plan to be adopted by some countries, especially targeting end-to-end encryption. The red line between excessive surveillance capabilities and providing LEAs with the necessary access can be very thin. Even more, measures to prevent unintended negative side effects might not be enforceable as the integration of a backdoor in an encryption algorithm practically renders encryption useless and jeopardizes the protection of fundamental rights and citizens data.
Possible conflicts

The location of a crime in a country's territory is generally accepted as, and remains the primary criterion determining its right to investigate, as are national rules, procedures and criteria to determine that the location of physical crimes are well established. However, regarding crimes involving the use of digital means, determining the location of crime is often more complex, having to take into account other factors such as the location of the suspect(s) at the time the crime is committed, and/or the location of the victim(s). In establishing the right to investigate, national rules and procedures may also take into account the location of the harm, while being mindful of the risk of creating de facto universal jurisdiction over crimes with widely distributed harm.

Collecting digital evidence

Developing a basic foundational understanding of data

This includes a consistent lexicon of legal and data related techniques that will be maintained for the duration of the data collection and streamlining data collection processes. Tradition would have us divide the types of data we are dealing with into either two categories (metadata and content data), or three categories (subscriber data, transactional data (including traffic data and, as a further subgroup, access data) and content data).

This also includes maintaining standards regarding scopes (types of crime and data covered), particular standards applicable to different types of actors (authorities, providers and users) and transparency/accountability mechanisms. There should be care taken to ensure that the procedures for requesting data are consistent and in full accordance with the provisions of the relevant national laws and of the regime under which it is submitted. Communication, coordination and cooperation between several countries may be necessary to guarantee respect of rights, ensure optimal efficiency, distribute responsibilities and avoid jeopardizing existing procedures.
Data definition

Main characteristics of the data collection processes.

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data privacy</strong></td>
<td>Level of data which the application will have access to personal data such as age, gender or genre, among others. Anonymous use of these data and indication of the management to third parties.</td>
</tr>
<tr>
<td><strong>Data security</strong></td>
<td>Level and quality of implementation of application security against possible attacks that may steal data collected by the application. There are security level protocols to evaluate the management of user data.</td>
</tr>
<tr>
<td><strong>Data destruction</strong></td>
<td>Time span during which the data will be stored on servers of private companies or public institutions that collect the data. The deletion of the data must be certified anonymously, and users should be informed who would have access to their data before they are deleted.</td>
</tr>
<tr>
<td><strong>Voluntary access</strong></td>
<td>There must be protocols that indicate whether the collection of their data through an application is voluntary or mandatory for its use. The data that the application collects must be specified so that users voluntarily accept the said collection.</td>
</tr>
<tr>
<td><strong>Time span</strong></td>
<td>The frequency with which the data are collected. Ranges from weekly or monthly to real-time data. The latter allows the automatic management of data with the use of AI applications.</td>
</tr>
<tr>
<td><strong>Storage</strong></td>
<td>The type of data storage. The data can be stored on a server or be part of the software that users use to access services on the Internet, such as cookies or the cache of browsers and applications. The user must be informed if these data should be deleted by him/herself or by companies within the indicated time frame.</td>
</tr>
<tr>
<td><strong>Technology</strong></td>
<td>Technology used to access and collect user data. Depending on the sophistication of the given technology, the speed of data collection and the amount may be truncated.</td>
</tr>
</tbody>
</table>
Privacy levels according to type of data collection and user privacy.

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PII</td>
<td>Personally identifiable information, or PII, is the data set that can be used to identify, contact, or locate a user. It is also the data set that allows one to differentiate one individual from another.</td>
</tr>
<tr>
<td>PIFI</td>
<td>Personally identifiable financial information, or PIFI, is related to the collection of information in financial and accounting terms, such as credit cards, bank accounts, and their details and other data that affect the economic health of the individual.</td>
</tr>
<tr>
<td>Non-sensitive PII</td>
<td>It is a set of information that is already in the public domain and, therefore, is not sensitive to the user. However, if it is combined with PII, it can offer information about the user or individual.</td>
</tr>
<tr>
<td>Non-PII</td>
<td>Non-personally identifiable information (Non-PII) is data that cannot be used in any way to identify a person. The most common examples are the ID of the connected devices, cookies, or the like. However, both types of information may offer clues as to who the user or individual is.</td>
</tr>
</tbody>
</table>

Developing a methodological framework

Phase 1: Recognize
Tangible and intangible digital evidence can be found in the incident of interest. It may also be hidden or visible. The priority of obtaining evidence is established based on its volatility and criticality. In this step identify, recognize, and document the storage media and/or processing containing data associated with the event. In identifying the methodology to be deployed, it is beneficial to promote an iterative framework that allows for mixed methods to capture the quantitative and qualitative aspects of proving the jurisdictional transfers. This affects several aspects of data (including training, access to sources and governance), processes (which would require flexibility and agility in an iterative methodology) and the objectives (including the business case and a scope that is defined for all members of the team regardless of their role in the data collection process).
Phase 2: Collect

Once the verifiable elements have been identified, according to the circumstances, cost and time, a decision is made whether to collect or extract. The process of collecting digital evidence is extracting the evidence from its place of origin to a controlled environment for its subsequent extraction and analysis. In this phase all actions or omissions taken are documented. It is important to remember that selecting or using a tool inappropriately to collect or extract the digital evidence, can produce the partial or total loss of the evidence. For this reason, it is relevant to systematically assess the risks and their impact.

Several data collection tools can be utilized to capture digital data traffic over networks as well as capture webpage data and information on data transfer protocols for instance Forensic Acquisition of Websites (FAW) which is a web browser explicitly created to capture web pages for forensics purposes. It can acquire a web page or part of it, also including streaming videos, frames and tool-tips. FAW uses the capabilities of Wireshark (a packet sniffer) to capture all of the traffic on all interfaces active network during the acquisition of the web pages. In addition, FAW calculates MD5 and SHA1 hashes of all acquired files, producing a detailed log of operations carried out with related time references. The function of acquisition’s integrity check allows to verify if all the captured files have not been forged. Finally, the acquisition output can be automatically sent at a certificated mailbox with the purpose to temporally attest the acquired data.

Phase 3: Extract

Extraction consists of generating, without introducing changes, a bit-by-bit copy of the relevant digital evidence, documenting the methods, tools and activities used. Both the copy and its original must be checked with an acceptable hash function where the hash result of the original and the copy must be the same. Digital proofs must comply with four characteristics: Justifiability, Auditability, Repeatability and Reproducibility. The extraction of digital evidence is contingent upon environmental factors such as: financial resources, time and particularities of the critical systems. When it is not feasible and/or permissible, it is extracted in a logical manner, i.e. justifying and specifically selecting specific selection of certain types of data, files or locations.

Phase 4: Protect

The integrity of digital evidence can be altered, disclosed and/or destroyed, leading to inconsistent results. If there are several stakeholders involved in the issue, the intervention should be coordinated with the other evidence collectors.
The chain of custody is to document completely and chronologically all the actions established by the technician from the moment the digital evidence is identified, collected, extracted and how it is protected, to the current status and location of the evidence.

This means that the chain of custody is a set of interrelated documents that provide traceability, integrity, and authenticity of the processes related to the treatment of digital evidence. This process preserves the integrity and authenticity of the evidentiary elements found and instruments used from recognition to the end of the chain of custody, to protect the elements involved from unauthorized or malicious entities or parties. This entails developing a two pronged method of managing data access - the physical evidence and the digital evidence. Physical access can be controlled by monitoring and keeping logs on persons who access the data, and digital evidence can be controlled using the application of the hash key. This means that if a person uses a file, to ensure that the two files are the same, they can identify it from the same hash key values between the two files.

In other words, it is to protect the relevant digital evidence from conscious or unconscious damages, as well as to take care of the from wear and tear, alterations, loss of data, and thermal affectations. dust, grease, rust-generating chemical pollutants, condensation that generate rust, moisture condensation, electromagnetic and static emissions.

**Phase 5: Analysis and Reporting**

Consists in consolidating through a written and verbal report, arguing the decisions taken, the results found in the collection of relevant and sufficient digital evidence. Data analysis is a systematic and essentially taxonomic process of sorting and classifying the data that have been collected. Four key steps are usually present in the analysis process: immersion in the data, coding, creating categories, and the identification of themes. Data analysis starts and occurs alongside the interviews that generate the data. Data analysis is time-consuming, and requires constant movement between immersion, coding, categorizing, and creation of themes. In systematically making sense of a whole dataset, the researcher moves back and forth through the processes we describe below. The analytical process must engage in a constant process of ‘testing the fit’ as new data are integrated into the analysis. This includes assessing the relevance of the theoretical concepts that are being used in the study as data analysis proceeds. Having a thorough knowledge of the data enables researchers to capitalize on opportunities to broaden and diversify the sample. It allows follow-up on emerging ideas and enables building in new
questions that arise during the course of research, rather than mulling over missed opportunities after the interviews have been conducted. This is entirely appropriate, indeed central, to a research method that is, by its very nature, interpretive and where analysis is anchored in the ideas that are located in the data themselves.

CaseStudy—the synergies between the Japanese gaming industry and EU-JAPAN-US Transfers

Video games are technically complex interactive, multimedia and multimodal products designed to entertain, unlike utility software applications that are designed to assist in specific tasks. Games are considered cultural artifacts due to their cinema quality graphics and their universal narrative themes, which brings them closer in nature to other audiovisual products, such as movies. Video games are also designed to demand a high level of user interactivity. When playing games, players interact as agents with the game, adopting a participatory role that goes beyond that of mere spectator of a movie, which is a passive experience in terms of the user's tangible input. Game designers seek to foster the development of an effective link between the player and the game, in order to make game play more engaging and to facilitate the player's immersion in the game world.

Video games are made up of different assets, namely:

a) in-game or onscreen text, such as the user interface (UI);

b) audio assets;

c) cinematic assets;

d) art assets, and

e) the manual and packaging. Therefore they contain different text types, such as menus, help and system messages, narrative and descriptive passages, a script for dubbing and/or subtitling, and printed instruction manuals. Some games, such as flight simulators, also contain specialized terminology as well as technical instructions and tutorials. The video game industry has outgrown film and music industries combined, making it the
major industry in the entertainment sector. The transition to the digital era had a major influence on the gaming industry. Due to digitalization, it has become possible for developers to directly distribute their game projects to its consumers via a digital store. Digital distribution completely eliminates the deficit of video game copies and reduces unnecessary hard-copy production costs. The most popular video game distribution markets of today are “Steam”, “GoG”, “Origin”, “Uplay”, and “Epic Games”. To demonstrate the phenomenon caused by this digital transition, in 2009 digital sales accounted for just 20% of total video game sales in the United States. In 2019, it made up over 80% of the total game revenues in the US. Starting from the Nintendo eShop to the PlayStation Store, all major console manufacturers have invested in their digital distribution stores, allowing them to grab a portion of the revenue chain from game purchases made directly on their website. Digital marketing of games not only helped developers to gain further sales but also allowed them to monetize gamers past the original game purchase through various means of microtransactions such as downloadable content (DLC), in-game items, season passes, and subscriptions. Additional content, such as DLCs, allowed game developers to monetize their audience after a game’s initial release by distributing it through the internet shops.

With a global COVID-19 pandemic influence, the video game market is now at its prime state, in 2020 it generated $179.7 billion revenue completely outstanding the forecasts of the previous year. The rapid growth continued in 2021 with the popularization of the recently introduced next-generation consoles Xbox series X and PlayStation 5.

**Japanese Game Developers - The Big Five**

The Big Five Japanese game developers are Nintendo Co. Ltd., Square Enix, Sega Sammy Holdings, Bandai Namco Holdings, and Konami. All the big 5 developers have subsidiaries and affiliated companies in the United States and in their privacy policies/terms of service agree to data sharing with the United States.

**Nintendo**

Nintendo, based in Kyoto, is the biggest but also the oldest company in the game industry. It was originally founded in 1889 to produce handmade hanafuda cards, used in a Japanese playing card game. Over the years, it became a video game company, one of the most powerful in the industry.
**Square Enix**

Square Enix was formed in 2003 as the result of a merger between rivals Square Co. and the Enix Corporation. Square’s Final Fantasy, first released in 1987, is the most widely distributed game series of all time, including both standard console games and portable games, a massively multiplayer online role-playing game, games for mobile phones, three anime series, and two full length CGI films.

**Sega**

Sega provided many of the hits for arcade games, such as Frogger and Zaxxon, and enjoyed huge success in the home console market with its Mega Drive, Saturn and Dreamcast. But after losing to Nintendo and Sony in the fierce competition of the 1990s, they pulled out and began concentrating on software development for multiple platforms. Sega has its origins in a company called Standard Games set up by three Americans in Hawaii in 1940, which in 1951 moved to its present base in Tokyo. The current name comes from the phrase "SEnvice GaMes of Japan," and was adopted after a merger in 1965.

**Konami**

Konami is a leading developer and publisher of numerous popular and strong-selling computer and video games. As of 2005, it is the 4th largest game developer in Japan. The company was founded in 1969 as a jukebox rental and repair business in Osaka by Kagemasa Kozuki, the still-current chairman and CEO. The name "Konami" is a conjunction of the names Kagemasa Kozuki, Yoshinobu Nakama, Hiro Matsuda, and Shokichi Ishihara, who were partners acquired by Kozuki and the original founders of Konami Industry Co., Ltd in 1973. Konami also means "Small waves." Konami is currently headquartered in Tokyo and additionally operates health and fitness clubs in Japan.

A typical data model that could capture both the qualitative and quantitative aspects of data transfers in the gaming industry relies on a multi-tiered data collection system that relies on several mixed methodologies.

1. Establishing the legal background for data sharing

   This information is publicly offered and publicly acquired by the aforementioned companies. A digital evidence tool to capture the policy can be used for instance Page Saver, which allows to capture and backup web pages (or visible portions of
web pages) as images. The capturing process can be tuned by means of a variety of settings, which include image format and scale.

This also includes the aforementioned trade agreement between Japan and the US as well as the provisions of the adequacy agreement which would indicate, particularly in the absence of updates to the privacy policies or terms of service following the Schrems decision, that there was no indicated change in the data sharing terms (in as far as any changes were communicated on the public fora) and that additional protective measures or halting the data transfers pending a more accurate data sharing strategy were not made by any of the companies.

2. Data collection based on interviews with industry stakeholders

This includes establishing a data sharing relationship between the USA from Japan. Websites such as SEAIR make note of video game import data between the US and Japan. One possible route of transfer capability in the international context is technology transfer between parent firms and their foreign affiliates. For instance, parent companies may deploy their professional managers and technicians to their foreign affiliate plants or export their R&D outcomes such as patents and copyrights to their foreign affiliates.

**Video game users**

The data transfer mechanisms can be assessed by subject access requests made by video game users to request information on the data held about them with a data protection authority lodged in the European union. Included in the data would be information on transfers made to third parties, from which refusal to disclose the data transfer can be escalated to a data protection authority and disclosure of the information provides evidence of linkages and onward transfers of data between Japan and the US.

3. Evidence Documentation

Recording all interactions with the evidence is easy to do for the handling of physical evidence, but not for the digital evidence. The simplicity of remote access, copy, file transfer, and user mobility trends in performing daily activities allow a digital to conduct exploration activities and data analysis anywhere and anytime. It will certainly complicate the documentation process of digital evidence. There must be an accurate and complete log of digital evidence, the legal process and the law enforcement agencies that will require much more complete information. Signature of the object, the identity of all
parties who interact with the evidence, the location where the evidence is handled, the time of access to the evidence and all the descriptions that contain any transactions and access to evidence is some information that is needed in the process of recording digital evidence. Handling digital evidence is conducted in particular environment tools. For example, the EnCase Guidance Software tools can start the imaging, extraction, exploration, and reporting phase of digital evidence analysis either in the individual mode or networking mode. Nevertheless, if the same file is then analyzed by using other tools, the recording and documentation process of the file cannot be done in an integrated manner.

Establishing the chain of custody for physical and digital evidence

The storage model involves the complex interactions between the parties related to the digital evidence. On the physical evidence, access to the evidence can be easily controlled. The person who uses, borrows and moves the evidence will be easily recorded and detected. Nonetheless, in the digital evidence, the person who does those actions cannot be easily traced. Being easy to copy activities, duplication, transmission, and access to digital evidence make it difficult to monitor a person’s interaction with the digital evidence. On the physical evidence, changes to the evidence can be easily controlled and monitored. However, it is not easy to do that on digital evidence. The application of the hash key (MD5, SHA1) is the standard method as a solution to control the integrity and credibility of digital evidence.

4. Analysis and Reporting

Primarily, collecting both quantitative and qualitative data comes down to a matter of coding and categorizing. The data interpreted can be from a variety of sources, whether the technical data from collecting traffic logs or trade data among the jurisdictions, to subject access requests. Ideally, each level of data is placed in relation to its strength in proving the claim by establishing the relationship, pre and post the Schrems decision. Determining the data continuity despite the inadequacy of the privacy shield and the differentiated privacy protection frameworks, lastly, adding onto the harm that data subjects face and the subsequent irreparable retrieval of their data that cannot be returned and will be used for both overarching gaming entity decisions but also in making up big data that can be used in onward transfers and a multitude of data uses.