DATA AS AN IP ASSET

Part I

INTA Data Protection Committee, Data Assets Subcommittee and Education & Awareness Subcommittee

Chair: Philip V. Marano (Greenberg Traurig LLP)

Vice Chair: Nicola Benz (MLL Legal)

Subcommittee Chairs: Otavio Padilha (Soerensen Garcia Advogados Associados) and Stephanie O. Sparks (Hoge Fenton Jones & Appel)

INTA Liaisons, Lori Schulman, Erica Vaccarello

November 2023

Section 1 – Introduction & Summary

Businesses are investing significant resources in products and services that rely on the collection and processing of data. Data management has become essential to innovation and to improve the customer experience. The net result is that data has *de facto* become an intangible business asset. The evolution of data privacy laws has raised questions as to the legal bases through which data should be protected as a business asset and/or intellectual property and as to whether the systems in place sufficiently balance individual rights and business interests.

This report analyzes a selection of important jurisdictions worldwide to find common trends regarding the legal treatment and protection of data under existing laws, and to provide a basis for further discussion on whether new approaches to the protection of data as an intellectual property (IP) asset would be desirable. In particular, the report explores the legal basis through which data is currently protected as an asset in Brazil, China, the European Union, India, and the United States and compares this with the protection in these jurisdictions of data related to identifiable individuals through privacy laws.

From the analysis of existing laws conducted in the selected jurisdictions, it emerges that, while raw personal data is not and cannot be protected as an intellectual property asset, aggregated data (*e.g.* databases, data compilations, customer lists, anonymized statistical information etc.) can be protected as trade secrets and/or through sui generis rights, copyright, unfair competition rules and contractual provisions.

This finding supports INTA's view that the intellectual property community has an important role to play in the ongoing evolution of legal frameworks for data protection. This includes focusing on the protection of investments in data collection and processing and, most importantly, the safeguarding of consumer trust.

Section 2 – Key Definitions

Below is a list of key definitions developed for the purposes of this report. They represent terms as generally understood by practitioners and are INTA's interpretation for the purposes of our analysis.

Personal data is defined differently in various jurisdictions, but, generally, is data that relates to an identified or identifiable natural person such as, name, address, government-issued identification number, account name and passwords (or means to access an account), taxpayer numbers, and family members.

Sensitive information means special categories of data that involve high risks to the rights and freedoms of individuals, such as health data, financial data, data on religion, sexual orientation, trade union or political association, criminal records, data belonging to minors etc.

Intellectual property is an umbrella term for a set of rights in intangible assets (assets that are not physical in nature), including copyright, patent, trademark, know-how, and trade secrets. This report does not further consider whether or how patent or trademark rights may arise in or from data.

Trade secrets are ancillary intellectual property rights in confidential information that is subject to reasonable efforts to maintain its secrecy and derives commercial value from that secrecy. To be considered a trade secret, the data in question must: 1) have commercial value; 2) remain secret; and 3) be subject to reasonable precautionary measures ensuring the data's secrecy.

Know-how may or may not be legally protected knowledge. It covers intangible assets, business information, and knowledge of a business' employees that contributes to the value and success of a business.

Proprietary information is information that belongs exclusively to its owner and may include trade secrets, ideas, techniques, know-how, unpatented inventions, documents, recorded data, and many sorts of treated information.

Section 3 – Emerging Questions Around Data and Intellectual Property

Data has been described by some as “the new oil”, with a value so high that many business models frequently provide free services in exchange for the ability to collect and process consumer data seeking to provide personalized customer experiences.

Simplified shopping experiences, travel planning, and the emergence of myriad social affinity groups have made life easier and more enjoyable for those who choose to engage. That the model works, is unquestionable. That the model produces serious consequences, is also unquestionable.

Privacy and consumer fundamental rights must be respected, and additional precautionary measures must be adopted to avoid breaking the bond of trust with customers. Voluntary measures are becoming legal obligations and legal obligations are becoming more complex.

New questions have arisen about the appropriate classification and protection of data in all realms of society. We have seen data protection laws emerge in every region of the globe. While these new regimes focus on data related to the individual, what about the treatment of data as a business asset or intellectual property (IP) asset?

Entrepreneurs have invested billions in products and services that rely on the collection and processing of data to innovate and improve the customer experience. How should this data be treated? How far should the law go in protecting it? Are the systems in place sufficient to protect both individual rights and the businesses interests that serve individuals?

Privacy rights are protected as fundamental human rights in many constitutions worldwide. Once companies adopt precautionary measures to safeguard privacy rights of customers, should the result of the treated information gathered belong to the company? If so, then on what legal basis? And if not, then why not?

This report examines these questions in the context of Brazil, China, the European Union, India, and the United States with the aim of providing recommendations for moving forward.

Section 4 – Analysis of the Trends in 5 Key Jurisdictions

We examined 4 categories of data through the lens of Brazilian, Chinese, European Union, Indian and US law. The following trends emerged through the study of these 5 jurisdictions.

A. **Raw Personal Data**. Raw personal data is not an intellectual property asset because data privacy laws generally identify the individual data subject as the owner or holder of rights of control over their data and require explicit consent or a lawful justification for use of the data by anyone other than the data subject. As an example, in some jurisdictions, including in certain U.S. states, there are statutory and common law rights protecting individuals' privacy and publicity rights (*e.g.*, absent obtaining a written publicity waiver and release, a person may be sued for appropriation of another person's name, likeness or other personal characteristics, if used for the appropriator's benefit, among other claims). Nevertheless, such laws do not prevent businesses from protecting the control over personal data (including assets like customer lists) as trade secrets or through contracts with data subjects or third parties.

B. **Data That Is Aggregated and Anonymized**. Anonymized and aggregated data that cannot be reverse engineered using reasonable efforts and that cannot be linked to an identified or identifiable natural person, are no longer subject to privacy statutes and can be considered proprietary business information and/or a trade secret. Businesses in certain jurisdictions similarly assert exclusive ownership over aggregated and anonymized data (often referred to as "statistics") as either trade secrets, via copyright protection, and/or through contracts with data subjects or third parties.

C. **Databases of Personal Data Compiled Through Sweat of the Brow**. In European jurisdictions, a thin layer of *sui generis* protection applies to personal information that has been collected with substantial investment (financial, materials, and/or human) in either obtaining the verification or presentation of the database content. This form of *sui generis* protection applies to those databases which are not "original" in the sense of an author's own intellectual creation ("non-original" databases), but which involved a substantial investment in their making. This property right for databases may be protected through unfair competition legislation; for example, the Swiss Unfair Competition Act (Art. 5 c.) makes it unlawful to take the market-ready work result of another [*note: this supposes a substantial investment has been made*]

without reasonable own effort [*note: this supposes that no investment is made*] by means of technical reproduction processes and to utilize it as such.

Under the Italian Copyright Act, "Repeated and systematic extraction or re-use of even insubstantial parts of the content of the database are not permitted if they involve operations contrary to the normal management of the database or cause unjustified prejudice to the creator of the database".

D. **Data Compilations or Presentations that Embody an Original Intellectual Creation.** Where the collection, arrangement or presentation of the data involves an original intellectual creation, copyright protection may also apply to such databases. The standard of the original intellectual creation required for copyright protection varies among jurisdictions. Even jurisdictions that set a high bar of creativity for copyright protection, for example, some European countries, recognize that there may be copyright in certain aspects of a database. On the other hand, there is uncertainty around the copyright protection of data generated by a machine or automated process, with a tendency towards denying copyright protection (for example *Stephen Thaler v. Shira Perlmutter and the US Copyright Office,* No. 1:22-cv-01564 (D.D.C. August 18, 2023) (upholding Copyright Office decision that human authorship requirement in copyright law foreclosed protection for AI-generated work) and legislative moves to make machine generated data more widely accessible in order to encourage innovation (for example the draft EU Data Act).

Section 5 – Existing Laws

Over the past few years, we have been studying multiple jurisdictions to find common trends regarding the legal treatment and protection of data. We chose Brazil, China, the European Union, India, and the United States as examples in this study because of the size of their economies and their influence in their regions and globally. They are provided in table format below. A table of relevant case-law will be provided as an Annex to Part 2 of this report.

Country/ Jurisdiction	Grounds for Legal Protection as an Asset	Privacy Laws
Brazil	Protection of **trade secrets** in Brazil has been traditionally provided under the criminal provisions relating to unfair competition, such as in article 195, items XI and XII of the Brazilian IP Statute. The 1996 Industrial Property Law, while not giving a more specific definition, provides that it is an act of unfair competition to use, without authorization (or obtain through illicit methods) confidential information, which constitutes a trade secret, proprietary information etc., as long as the information is indeed treated as confidential. Article 7, XIII of the Brazilian Copyright Statute also provides that compilations of information such as databases, depending on the originality of the selection of information that is chosen to be within the database or of the organization of the information in the database etc., may be subject to **copyright protection**. Data may be protected as a trade secret or confidential information by **contract**. Parties to the contract should in good faith fulfil their obligations under the contract, including obligations of confidentiality and restrictions on the use of the data.	The General Data Protection Act (*Lei Geral de Proteção de Dados* or LGPD), Federal Law no. 13, 709/2018, entered into force on September 18, 2020. The LGPD defines personal data as any information related to an identified or identifiable natural person. Anonymized data is not considered personal data, except when the process of anonymization has been reversed or if it can be reversed applying reasonable efforts. Individuals' rights under the LGPD are similar to those under the EU-GDPR, e.g., access, correction, deletion, blocking, and portability. Anonymized data that cannot be reverse engineered using reasonable efforts and that cannot be linked to an identified or identifiable natural person can be compared to proprietary information or trade/industrial secrets. This data can be monetized, traded, or used for marketing. The LGPD provides an explicit right to anonymization, where data is unnecessary, excessive, or processed in violation of the law.

Country/ Jurisdiction	Grounds for Legal Protection as an Asset	Privacy Laws
China	Data as an asset can be protected under different laws in China depending on the nature of the data concerned. The general principle is data can be freely crawled, scraped, traded, stored, transferred, or used in any manner, unless it falls within any of the following categories: **Trade Secret**: Article 9 of the Anti-Unfair Competition Law provides a legal remedy against unauthorized disclosure and use of others' trade secrets. Data that is not in the public domain may be protected as a trade secret, such as lab statistics, client list, technical know-how, business plan, computer software and algorithms (also eligible for copyright protection), etc. Trade secret thievery may also trigger criminal liability. Nevertheless, the burden of proof from the plaintiff is hard to meet. **Copyright**: The source code, object code and the relevant documentations of computer software and algorithms (covering programs running on PC and smartphones) are eligible for copyright protection. If the program is used in conjunction with memory devices, computer hardware, and together with operational process, it might fall into the patentable subject matter, and the much stronger protection under the Patent Law is available. Copyright law can be invoked to protect user generated data /contents: Typically, the authorship	Privacy laws in China consist of comprehensive data protection laws, sectoral laws and regulations, and industry standards. The **Civil Code** stipulates that individuals enjoy the right of privacy. There is a whole section in the Civil Code (**Section 6, Chapter 4**) to specify some high-level principles for the protection of privacy and personal information. Then, there are three laws governing data protection, including **Personal Information Protection Law (PIPL), Network Security Law, Data Security Law** and its implementing rules, such as Measures for the Security Assessment of Outbound Data Transfers from PRC. PIPL is the most relevant and comprehensive law governing the protection of personal information akin to GDPR in the EU, which sets forth the principles in collecting, processing, transferring, disclosing and deleting personal information, including transparency, accuracy, security, and consent-based collection mechanism. According to Article 4 of PIPL, anonymized data is not treated as "personal information" and therefore can be freely monetized, traded, or used for business purposes, as long as it is not sensitive information (biometrics, DNA, etc.). Anonymization occurs when any personal information,

Country/ Jurisdiction	Grounds for Legal Protection as an Asset	Privacy Laws
	thereof shall belong to the network user, and therefore the platform cannot claim independent copyright to those types of works without due authorization from the author. However, platforms can rely on Article 2 of *Anti-unfair Competition Law* for the protection of user generated data. In the leading case-law, the defendant reproduced many user comments, posts, complaints, and account information to its website, which was found to be a violation of Article 2. The courts recognized that the platform acquired a "competitive advantage" by collecting and processing the user generated data. Therefore, unauthorized scraping and using of such data, even if the data is publicly accessible, makes use of the other's "competitive advantage" by improper means and is unlawful. **Contract Law** also can play a role in the protection of data. This usually happens for data that would otherwise not be protectable. Examples might be agreements between the data controller and processer, as well as the agreements to exploit the secondary use of platform generated data and user derivative data.	after being processed, cannot be linked to an individual or cannot be re-identified.
European Union	Directive (EU) 2016/943 of June 8, 2016, on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. Member States were required to comply with the Directive by June 9, 2018. The	Under the General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR"), brand owners and platforms may use (and monetize) personal data anonymously. The anonymization of data aims at preventing the identification of the data subject.

Country/ Jurisdiction	Grounds for Legal Protection as an Asset	Privacy Laws
	Directive's aim was to harmonize and provide a more uniform approach to the protection of trade secrets across the EU. Some Member States introduced specific new trade secrets laws to implement the Directive. According to the Directive, information can be a protected **trade secret** if: *(a)* it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or ready accessible to persons within the circles that normally deal with the kind of information in question; *(b)* it has commercial value because it is a secret; and (c) it has been the subject of reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. Data use, whether or not the data is a trade secret, may be permitted and/or restricted by **contract law**. In addition, Directive (EU) of 11 March 1996 on the legal protection of databases requires the EU Member States to create a ***sui generis* right of protection for computer databases** that allows action to be taken against unlawful copies. This protection is available to makers of databases who are EU nationals or residents. The right arises automatically and there is no requirement for registration. The creation of the database must have involved a substantial investment	This can be achieved by applying different techniques grouped into two families: randomization and generalization. Randomization modifies the degree of truth of data to eliminate the correlation between data and person. Generalization dilutes the attributes of the subject by modifying the scale or order of magnitude (age range instead of the precise age of the subject). Personal data may also be used (and monetized) without anonymization, provided the use is permitted by one of the legal bases set out in the GDPR (compliance with a legal obligation, contractual performance, vital interests, public interest, legitimate interests, or data subject consent) (Art. 6(1)(a)-(f) GDPR).

Country/ Jurisdiction	Grounds for Legal Protection as an Asset	Privacy Laws
	(financial, material and/or human) in obtaining, verifying, or presenting the database content. There is no requirement for an original intellectual creation, unlike under copyright law. Protection is for 15 years from the date of creation or first making available the database. A new EU Data Act is currently under discussion. Under the original proposal (Art 35 of the draft Act), it could be understood that computer generated databases will in future no longer be protected by the sui generis database right arising from Directive 96/9/EC. However, the intent and effect of Art. 35, if it remains in the final Act, is not clear and the aims of improving access to data and of encouraging investment in databases can both be argued. The draft EU Data Act does however remove any right to a database right for public authorities. Regardless of the above, and in parallel to any other rights that exist in data, any aspect of a database that is an original intellectual creation, for example the structure or the layout of the database, may also be protected under national **copyright laws**, provided the conditions for protection as a copyright work are met.	
India	India is a signatory of the TRIPs Agreement and is obligated to protect undisclosed information. India does not have specific codified legislation to protect trade secrets, but it has taken steps toward recognizing the protection to be	India has for several years worked towards a specific data protection legislation. In August 2023, the Digital Personal Data Protection Act, 2023 ("DPDP") received the Presidential assent. The DPDP will be notified in phases. The rules

Country/ Jurisdiction	Grounds for Legal Protection as an Asset	Privacy Laws
	given to trade secrets, including drafting and approving the National Intellectual Property Rights Policy ("National IPR Policy"), approved May 2016. Even in the absence of unified legislation formally recognizing or defining "**trade secrets**," the protection of such information is extensive in India under several statutory provisions that recognize and protect different types of confidential information, e.g., Section 27 of Indian Contract Act; Indian Penal Code, 1860, Sec. 72 of the Information technology Act, etc. Data can be protected as trade secrets particularly if the data is provided in relation to a contract or under trust. With regard to protection of data under **copyright law**, the Copyright Act, 1957, recognizes protection in compilations and in databases. To be protected under the Copyright Act, a work must be original. While data by itself being factual in nature may lack the test of originality and therefore not itself be protectable under copyright law, the expression of the fact, *i.e.,* of the idea or presentation of data within a compilation or database, may be protected as a compilation or database. For several years, this protection arose from an application of the sweat of the brow doctrine. In more recent years, there has been a shift to require a modicum of creativity. While the copyright	under it are being framed and will detail important aspects for the implementation of the legislation's provisions. India's regulatory mechanism for data protection and privacy prior to the DPDP was primarily under the Information Technology Act, 2000 (the "IT Act") and its corresponding Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "IT Rules"). Additional sectoral regulations also applied (e.g., in the banking, telecommunications, health sectors). This legislation continues to apply and the interplay between the DPDP and IT Act and IT Rules as well as other legislations and regulations will become clearer over time. If customers are aware and agree that information will be collected, treated, and used (informed consent), anonymized data may be monetized. However, this is subject to the implications of developing data protection laws in India, which are still subject to interpretation. Some notable Rules are: A body corporate shall obtain consent in writing from the provider of sensitive personal data or information regarding purpose of usage before collection of such information. A body corporate can disclose sensitive personal data to

Country/ Jurisdiction	Grounds for Legal Protection as an Asset	Privacy Laws
	legislation itself does not stipulate the degree of creativity or how originality is to be determined, the Supreme Court of India has held that to establish copyright, the creativity standard applied is not that something must be novel or non-obvious, but some amount of creativity in the work is required. Data in India qualifies for protection under **contractual confidentiality and use restrictions**. The restrictions, however, may not apply to data that is already publicly available, made available through no fault of the recipient, data which may need to be revealed as per law and such.	a third party as long they have sought prior permission from the provider of such information. A body corporate can transfer sensitive personal data to any other body corporate located in India or outside India that ensures the same level of data protection. Such a transfer may be allowed for fulfilment of a contract between the body corporate and the provider of information or where such person has consented to the data transfer. Again, the implications of the DPDP will need to be examined in this regard.
United States	In the United States, data may qualify for protection under (not only contractual confidentiality and use restrictions, but also) one or more categories of intellectual property, specifically: trade secrets, and copyrights. **Trade Secret Protection** U.S. Federal Defend Trade Secrets Act ("DTSA"), 18 U.S.C. §§1832, et seq. The DTSA defines "trade secret" as "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, whether tangible or intangible, and whether or how stored, compiled or memorialized, physically, electronically, graphically, photographically, or in writing if: a)	The United States does not have a comprehensive federal law regulating the collection, use and other processing of personal information in the interest of individual privacy rights. There are, however, several subject matter and sector-specific federal laws that regulate privacy, e.g., the Gramm-Leach-Bliley Act ("GLBA") that applies to financial institutions, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") that applies to health care providers, etc., and the Electronic Communications Privacy Act ("ECPA") that applies to electronic communications and remote computing service providers, to name a few. And as of the first publication of this paper, 5 states have enacted comprehensive consumer privacy

Country/ Jurisdiction	Grounds for Legal Protection as an Asset	Privacy Laws
	the owner thereof has taken reasonable measures to keep such information secret: and b) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by , another person who can obtain economic value from the disclosure or use of the information". In addition to the DTSA, most U.S. states have well-established trade secrets laws protecting a business' right to own exclusively as an IP asset certain customer lists, a compilation that necessarily or inevitably includes personal information. In the U.S., parties also have the freedom to contract for the identification of certain data to be deemed a trade secret, and for the exclusive ownership of data—at least as between the parties to a contract. For example, California law provides that the "facts recited in a written instrument are conclusively presumed to be true as between the parties thereto, or their successors in interest ...." (Calif. Evid. Code § 622.). Under this statute, in the recitals of their contract, parties may declare certain data to be an IP asset and declare the exclusive ownership of data as an IP asset. **Copyright Protection** The US Copyright Act recognizes rights in compilations, defined as "a work formed by the collection and	legislation (California, Utah, Colorado, Virginia and Connecticut), and all 50 States and 3 U.S. Territories have data breach notification laws. With respect to data being treated as an asset, including as an IP asset, it should be noted that aggregate or deidentified consumer information is not personal information subject to regulation by, e.g., the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights and Enforcement Act ("CCPA"). *See,* Cal. Civ. Code 1798.140(v)(3). Cal. Civ. Code 1798.140(v)(3). The CCPA defines "aggregate consumer information" as relating to a group or category of consumers, from which individual consumer identities have been removed, and that is not linked or linkable to any consumer or household. The CCPA also defines "deidentified" as information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, provided that any recipient of the information is contractually obligated to take reasonable measures to ensure the information cannot be associated with a consumer or household, and publicly commit to maintain and use the information in deidentified form and not to attempt to reidentify the information. CCPA also defines "deidentified" as

Country/ Jurisdiction	Grounds for Legal Protection as an Asset	Privacy Laws
	assembling of preexisting materials or of data that are selected, coordinated or arranged in such a way that the resulting work as a whole constitutes an original work of authorship." 17 USC S 101. To be clear, the underlying facts and data that comprise a compilation may not be protected under copyright, however an original selection and arrangement of those facts and data can be protected. In other words, a company that makes numerous creative choices with respect to the categories of consumer data it collects, and how it selects, coordinates, or arranges that data, may be able to successfully argue that its database should enjoy copyright protection, at least in a very narrow sense against verbatim copying. *Compare Feist Publications, Inc. v. Rural Telephone Service Co*., 499 U.S. 340 (1991) (denying protection for names and numbers arranged alphabetically in a generic telephone white pages could not be protected); *with Key Publications v. Chinatown Today Pub. Ent.,* 945 F.2d 509 (2d Cir. 1991) (upholding protection for names and numbers of Chinese-American businesses which organized businesses into over 260 unique categories and excluded certain categories unlikely to remain open).	information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, provided that any recipient of the information is contractually obligated to take reasonable measures to ensure the information cannot be associated with a consumer or household, and publicly commit to maintain and use the information in deidentified form and not to attempt to reidentify the information. Whether or not personal information is aggregated or deidentified, at this time in the U.S., there is no statutory prohibition of a business owning personal data elements that it has lawfully collected. Indeed, several state statutes, such as Massachusetts Data Security Regulation (201 Mass. Code Regs. §§ 17.01 *et seq*.), apply to all persons, including businesses, "that own or license personal information about a resident" of that State. (*See also,* Calif. Civ. Code § 1798.81.5, stating that the purpose of California's data breach notification law "is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information.")

Section 6 – Conclusions & Recommendations for Best Practices

A. Conclusions

Data management for improving products, services, experiences, technologies, and solutions seeking to satisfy the customer´s needs and expectations is here to stay. There is no turning back the clock as customers have come to rely on personalized experiences in their engagement with the brand. Excellent, reliable data management is essential to maintaining goodwill and customer trust.

Transparency is key. Customers must know that their data is collected and treated/processed.

Anonymization as a security measure. Where collected data is anonymized, it falls outside the scope of data protection law in the jurisdictions considered in this report. In order to remain outside the scope of data protection law, jurisdictions typically require companies to make the anonymization irreversible so that it cannot be connected again to the individual. Failure to do so could result in serious data breaches with legal and customer relationship consequences. Aggregate/anonymized data has the potential to generate important business information, with commercial value, allowing companies to make strategic decisions.

Purpose limitations. According to many data protection laws and regulations, every processing of personal data must be compatible with the purposes made transparent to the data subject, while the processing must be limited to the minimum required for achievement of those purposes, encompassing pertinent, proportional, and non-excessive data in relation to the purposes of the data processing.

Raw data cannot be considered an intellectual property asset.

Databases, data compilations (customer lists), statistical information etc. can be protected as trade secrets and/or through sui generis database rights, unfair competition rules, copyright, and contractual provisions.

Data privacy laws expressly exempt aggregated and anonymized data. Aggregate/anonymized data can be regarded in most jurisdictions as a trade secret/business information (intangible assets) and thus the IP community should create awareness and be more involved in this field, with the resultant attention to protection and enforcement.

Rights in the assets will depend on the form of data, for example whether it is still linkable to identifiable or identified customers, whether there has been investment in its collection, structure and presentation, whether the data or database is machine generated, whether the database is created by or for a public body or private purposes etc.

INTA Resources for Practitioners can assist practitioners with counseling clients on best practices including establishing checklists and procedures. They are written with the brand professionals in mind. See recent committee reports:

Privacy Law Issues for Trademark Owners: https://www.inta.org/wp-content/uploads/public-files/advocacy/committee-reports/20231013_Privacy-Law-Issues-for-Trademark-Lawyers.pdf

The Digital Services Act, Countdown to Compliance: What Do Brands Need to Know and Do?: https://www.inta.org/wp-content/uploads/public-files/advocacy/committee-reports/DSA-Committee-Report-July-2023.pdf

Data Protection Checklist for Brand Owners: https://www.inta.org/wp-content/uploads/public-files/advocacy/committee-reports/20230223-Data-Protection-Checklist-for-Brand-Owners-2.pdf

B. Recommendations

Our general recommendation is for INTA to hold its course and not to advocate for a specific new legislation since the current legal framework already provides for protection of data as an asset through trade secret law, database rights or similar *sui generis* rights, unfair competition laws, copyright and contractual protection, at least in the jurisdictions examined in the course of preparation of this report. We will continue to study additional jurisdictions and identify trends that may affect this recommendation in the future.

Our conclusion supports the view that the intellectual property community should continue to be involved in and consulted on decision-making around the protection of investments in data collection and processing and the safeguarding of consumer trust as legal frameworks continue to evolve.