May 7, 2024

White Paper on Clarifying Definitions in the Protecting Americans' Data from Foreign Adversaries Act of 2024

Peter Swire[1]

Executive Summary

This paper examines the text of the "Protecting Americans' Data from Foreign Adversaries Act of 2024." PADFAA contains a number of novel definitions for terms such as "data broker" and "controlled by a foreign adversary" ("CBFA"). This White Paper explores the definitions in PADFAA, seeking to provide an objective analysis of what the definitions mean and how they fit together.

The core prohibition of PADFAA is that it is illegal for (i) a data broker (ii) to sell or otherwise make available (iii) personally identifiable sensitive data of a U.S. individual (iv) to a CBFA individual or entity. This paper addresses each of these definitions, pointing out implications and highlighting some areas where the text is open to more than one interpretation.

For the definition of "data broker," the biggest uncertainty that I see concerns the effects of PADFAA on service providers – the companies that provide IT and all sorts of other services to other companies. The paper examines the legal status of a hypothetical WidgetCo and a company that provides services, called ServiceCo.

One key point is that ServiceCo gets paid by WidgetCo, and data brokers get paid to supply data. This similarity matters because PADFAA's definition of "data broker" applies when a company acts "for valuable consideration" (gets paid). A *central legal issue in this White Paper is how PADFAA draws the line between a "data broker" (subject to PADFAA's prohibitions) and the many sorts of service providers who are enabling ordinary business, but who do not fit the idea of a data broker.*

At least three issues arise in the definition of what counts as "controlled by a foreign entity":

1. The definition applies to both an "individual" and an "entity." It appears that an entity may be CBFA if one individual, such as an employee, is "domiciled" in a foreign country such as China, and someone in that company has access to sensitive data.

---

[1] Peter Swire is the J.Z. Liang Chair in the Georgia Tech School of Cybersecurity and Privacy, and a Professor of Law and Ethics in the Georgia Tech Scheller College of Business. Research Director of the Cross-Border Data Forum, and Senior Counsel to Alston & Bird LLP. Research for this White Paper was funded by the National Retail Federation. The views expressed are those only of Swire, and not the NRF, any member of the CBDF, or any client of Alston & Bird, LLP. I write as a privacy law professor who has taught legislative interpretation, and welcome comments and corrections. Email to swire@gatech.edu.

2. The definition may mean that the PADFAA prohibition applies to entities such as Chinese subsidiaries and affiliates of U.S. corporations. The prohibition would appear to require the U.S. corporation to cut off such companies from access to much or all of its corporate systems, to ensure that no sensitive data is accessed.
3. The prohibition appears to apply to occasional, incidental, and perhaps even accidental ability to access one U.S. individual's sensitive data by a CBFA individual or entity. WidgetCo and ServiceCo may thus risk violating PADFAA even where they don't know that one of the companies they do business with is actually CBFA.

Other implications of the definitions in PADFAA:

1) PADFAA goes beyond "**sale**" of data, and applies also where ServiceCo "**provides access**" to or "makes available" any sensitive data. Many service providers "provide access" to information.
2) The list of 17 categories of "**sensitive data**" are broader than U.S. state law definitions of "sensitive data," including types of data that may appear in a normal corporate IT system.
3) Unlike the recent Executive Order, which applies to "**bulk**" data sales, PADFAA applies to any one bit of sensitive data. ServiceCo may help "provide access" to that data.
4) With these broad definitions of "provides access" and "sensitive data" the PADFAA prohibition appears to apply if any bit of sensitive data is available to a CBFA entity.
5) Because **it gets paid** for its services, ServiceCo appears to qualify as a "**data broker**" unless it fits one of two exceptions.
6) The "**service provider**" exception stops working if ServiceCo makes any bit of sensitive data available to any one CBFA entity.
7) ServiceCo may **lose its "service provider" exception,** and become a prohibited "data broker," if only one of its clients is CBFA, even if its other clients are lawful and unrelated to China.
8) There is a second exception to "data broker," whose interpretation appears to apply to sale of physical goods more clearly than for services. That exception applies where ServiceCo makes sensitive data accessible to WidgetCo, but making data accessible to WidgetCo "**is not the product or service**."

In conclusion, PADFAA may have unintended effects on a large category of businesses, who provide services to companies but who do not fit the usual understanding of a data broker. The law as written creates uncertainty about the scope of its application.

May 7, 2024

White Paper on Clarifying Definitions in the Protecting Americans' Data From Foreign Adversaries Act of 2024

Peter Swire[1]

This paper examines the text of the "Protecting Americans' Data from Foreign Adversaries Act of 2024." PADFAA contains a number of novel definitions for terms such as "data broker" and "controlled by a foreign adversary" ("CBFA"). This White Paper explores the definitions in PADFAA, seeking to provide an objective analysis of what the definitions mean and how they fit together.

The core prohibition of PADFAA is that it is illegal for (i) a data broker (ii) to sell or otherwise make available (iii) personally identifiable sensitive data of a U.S. individual (iv) to a foreign adversary country, or to an individual or entity that is CBFA . This paper addresses each of these definitions, pointing out implications and highlighting some areas where the text is open to more than one interpretation.

For the definition of "data broker," the biggest uncertainty that I see concerns the effects of PADFAA on service providers – the companies that provide IT and all sorts of other services to other companies. The paper examines the legal status of a hypothetical WidgetCo and a company that provides services, called ServiceCo.

One key point is that ServiceCo gets paid by WidgetCo, and data brokers get paid to supply data. This similarity matters because PADFAA's definition of "data broker" applies when a company acts "for valuable consideration" (gets paid). A *central legal issue in this White Paper is how PADFAA draws the line between a "data broker" (subject to PADFAA's prohibitions) and the many sorts of service providers who are enabling ordinary business, but who do not fit the idea of a data broker.*

At least three issues arise in the definition of what counts as "controlled by a foreign entity":

1. The definition applies to both an "individual" and an "entity." It appears that an entity may be CBFA if one individual, such as an employee, is "domiciled" in a foreign country such as China, and someone in that company has access to sensitive data.
2. The definition may mean that the PADFAA prohibition applies to entities such as Chinese subsidiaries and affiliates of U.S. corporations. The prohibition would

[1] Peter Swire is the J.Z. Liang Chair in the Georgia Tech School of Cybersecurity and Privacy, and a Professor of Law and Ethics in the Georgia Tech Scheller College of Business. Research Director of the Cross-Border Data Forum, and Senior Counsel to Alston & Bird LLP. Research for this White Paper was funded by the National Retail Federation. The views expressed are those only of Swire, and not the NRF, any member of the CBDF, or any client of Alston & Bird, LLP. I write as a privacy law professor who has taught legislative interpretation, and welcome comments and corrections. Email to swire@gatech.edu.

appear to require the U.S. corporation to cut off such companies from access to much or all of its corporate systems, to ensure that no sensitive data is accessed.

3. The prohibition appears to apply to occasional, incidental, and perhaps even accidental ability to access one U.S. individual's sensitive data by a CBFA individual or entity. WidgetCo and ServiceCo may thus risk violating PADFAA even where they don't know that one of the companies they do business with is actually CBFA.

The paper now turns to more detailed consideration of the key definitions and their implications.

Passage of the Legislation. Rep. Pallone introduced PADFAA as H.R. 7520 on March 5, 2024. The bill passed unanimously in the House Energy & Commerce Committee on March 7. It then passed the House unanimously on March 20. It was referred to the Senate Commerce, Science, and Transportation Committee, but that Committee did not take any formal action on it. On April 20, the House approved H.R. 815, including PADFAA, as part of the package of legislation that included aid to Ukraine and Israel. The Senate passed the package 79-18 on April 23, and the President signed it the next day.

Prohibited actions under PADFAA. Section 2(a) of PADFAA has a general prohibition, which applies if each of the following exists:

1. A "data broker." The broad definition of "data broker" is addressed below.
2. Who "provides access" or "makes available" data. The full text of "provides access" is "to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available." Note that this definition is broader than merely selling data, and includes expansive terms such as "provides access to" or "otherwise makes available."
3. The data is "personally identifiable." The definition of "personally identifiable" is similar to or broader than other U.S. laws, and essentially means any data that is reasonably linkable to an individual or the individual's device.[2]
4. The data is "sensitive data." The broad definition of "sensitive data" is discussed below. It includes, for instance, "an individual's private communications," such as emails.
5. The data is about a "U.S. individual," referring to "a natural person residing in the United States."
6. The data is available to a foreign adversary country (such as China), or "any entity that is controlled by a foreign adversary." The broad definition of "controlled by a

[2] The definition of "personally identifiable" appears to be broader than the term is defined in other settings, by explicitly providing that data is identifiable if it is "reasonably linkable, alone or in combination with other data," to an individual or device. The text "in combination with other data" is not used in most other U.S. privacy laws.

foreign adversary" ("CBFA") is discussed below. Notably, data appears to be considered "available" if any sensitive data is available to any one of its customers.

Why the prohibited actions under PADFAA may be broader than many have realized. The common-sense version of the PADFAA prohibitions would be relatively narrow – data brokers should not be selling the sensitive data of U.S. individuals to foreign adversaries, including companies operating in a country such as China.

The discussion here, however, shows why the text of PADFAA may support a considerably broader prohibition, due to the broad definitions of "data broker," "provides access," "sensitive data," and "CBFA." *The broader prohibition would seem to apply, for instance, if someone in China, for a wide range of businesses, can access any bit of sensitive data of even a single U.S. employee.*

There is a low threshold for being considered "controlled by a foreign adversary" (CBFA). PADFAA creates multiple paths for an entity or individual to be considered CBFA. If any of the following are true, then the strict rules apply:

1. An *entity*, such as ChinaExampleCo, that "is domiciled in, is headquartered in, [or] has its principal place of business in" a foreign adversary country. Where this definition is met, then PADFAA prohibits sales to ChinaExampleCo by any data broker. To the extent ServiceCo provides services to ChinaExampleCo, then ServiceCo no longer qualifies as a "service provider."
2. An *individual* who "is domiciled" in the foreign adversary country.[3]
3. An entity, such as ChinaExampleCo, that is "organized under the laws of a foreign adversary company." For example, for a company headquartered in the U.S., this definition would apply to a subsidiary, affiliate, or other company that is incorporated in China.
4. An entity with 20% ownership, either by a foreign person or combination of foreign persons. PADFAA's penalties would thus appear to apply where there is an entity that is 20% owned by a combination of foreign persons, even if ServiceCo did not know who owned that entity.
5. "A person subject to the direction or control of" a foreign person or entity. This language may apply, for instance, to business situations where there is a Chinese-domiciled individual who is a member of a U.S. company's board of directors, or who is a senior manager who meets the "direction or control of" test.

The definition of CBFA is important under PADFAA because the law's prohibition applies where the CBFA entity can access the sensitive data of one U.S. individual. ServiceCo appears to lose its status as a "service provider" if it provides access to the sensitive data of

[3] The statutory text provides the broader definition, applying to "a foreign person that is domiciled in, is headquartered in, has its principal place of business in, or is organized under the laws of a foreign adversary country." As applied to an individual, the important provision is when the foreign person (not a U.S. citizen) is domiciled in that country.

one U.S. individual, to a CBFA entity, in the course of providing services. This access might occur, for instance, if a U.S. employee in China can access their own payroll information in their company's internal system, or if any employee in China can access payroll information for any American employee.

The use of the term "individual" in the PADFAA definition of CBFA is different than the definition of CBFA in the new law directed at TikTok, and this difference appears to have significant consequences. The PADFAA definition of CBFA begins: "The term "controlled by a foreign adversary" means, with respect to an **individual** or entity, that such **individual** or entity …". The rest of the definition then sets forth the list of ways to qualify as CBFA, such as being headquartered or organized under the laws of a foreign adversary country.

The definition of CBFA in the new law directed at TikTok is strikingly different: "The term "controlled by a foreign adversary means, with respect to **a covered company** or other entity, that such **company** or entity …". The TikTok portion of the law then defines "covered company" in some detail, including requiring the large scale of over 1,000,000 monthly users.

The use of the word "individual" appears to substantially increase the scope of the PADFAA definition of CBFA. The lead-in paragraph for the definition of CBFA applies to "an individual", and one of the ways to qualify as a CBFA is to be "domiciled" in a foreign adversary country. **This trigger of coverage is much lower than the 1,000,000 user threshold for the new law directed at TikTok. *The language of PADFAA thus applies the term "controlled by a foreign entity" even if there is only a single, low-level employee in China, and the other criteria in the PADFAA prohibition are met*.** Those other criteria, as stated throughout this paper, are that the entity makes available any sensitive data of a U.S. individual.

It appears possible that use of the term "individual" is a drafting error in PADFAA. The term "covered company" exists in the new law diredted at TikTok, but the term "covered company" does not appear in PADFAA, which applies to all data broker sales and not solely to certain social media companies such as TikTok.

The possibility of a drafting error increases due to the garbled text of this part of PADFAA. As written, the term CBFA "means that such an individual or entity is a foreign person that is domiciled in, is headquartered in, or is organized under the laws of a foreign adversary country." Obviously, an individual who is a person would not be "headquartered in" or "organized under the laws" of a foreign country. *This garbled text thus suggests that the provision was intended to apply only to corporations or other legal persons, and not to a human (a "natural" person).*

The specific apparent effect on IT companies and other "service providers." A main focus of this White Paper is on how PADFAA affects "service providers," using the

example of ServiceCo, which acts at the direction and control of another company, such as WidgetCo. The term "service provider" is also used in the Safeguards Rule for financial services under the Gramm-Leach-Bliley Act.[4] Although the definitions are not identical, a "service provider" under PADFAA is the same concept as "business associate" under HIPAA[5] and "processor" under the European Union General Data Protection Regulation ("GDPR").[6]

Service providers assist companies such as WidgetCo in numerous ways, including business services such as payroll and payments. For the discussion here, also consider companies that supply information technology (IT) to WidgetCo, including the cloud-based software, telecommunication services, and cybersecurity services that are used today by almost any international company. Employees of IT companies, to do their job, often have access to data about the actions of WidgetCo employees. That is, these *service providers often "provide access" or "make available" information about employees and other individuals in the U.S., and at least some of this information in the corporate network of ServiceCo or WidgetCo may be accessible in China or other countries*.

The effect of the "data broker" definition on "service providers." The PADFAA definition of "data broker" has two relevant exceptions for "service providers," but it appears that the exceptions often may not apply, as explained below. *Where an exception does not apply, companies will often be "data brokers" even though they don't fit the common-sense meaning of a data broker*.

The term "data broker" applies to the following:

1. The entity "provides access" or "makes available" data. As discussed above, "provides access" includes sale of data, but is much broader.
2. The entity provides access "for valuable consideration." For lawyers, "consideration" basically means any form of payment. For example, ServiceCo gets paid for the services that it provides to WidgetCo.
3. The data is of at least one "United States individual." Note that Executive Order 14117 applies only to "bulk" data sales, but PADFAA applies to data of any one U.S. individual.
4. The entity did not collect the data "directly from such individuals." In many instances, a service provider such as ServiceCo does not collect the data in its systems directly from the individuals.

Many service providers would appear to meet these four criteria: (i) They provide access to data in the course of their services; (ii) they are paid by WidgetCo; (iii) they provide access to the data of at least one U.S. individual; and (iv) they do not collect all the data they use directly from the individuals. *Unless there is an applicable exception to the definition of*

[4] 16 CFR §314.2(q).
[5] 45 CFR § 160.103
[6] GDPR, Art. 28.

"data broker," it appears that a wide range of companies that act as service providers will also be considered "data brokers."

Why the "service provider" exception for "data brokers" often does not apply to service providers. The PADFAA definition of "service provider" excludes many companies that would be considered "service providers" under GLBA or "business associates" under HIPAA.

The definition of "service provider" applies to an entity that:

1. Collects, processes, transfers, or receives data. These terms apply to many types of service providers.
2. "On behalf of, and at the direction of" an individual or entity. This language is the common definition for an entity that assists another company with data, such as a business associate under HIPAA or processor under GDPR.
3. "An individual or entity that is **not** controlled by a foreign adversary" ("CBFA") *This element of the definition narrows who can be considered a "service provider" eligible for the "service provider exception" to the definition of a "data broker."* As discussed below, PADFAA has a broad definition of CBFA.

In simple terms, many companies may be "data brokers" unless they fit the PADFAA definition of a "service provider." If ServiceCo provides services to a CBFA entity, such as by doing work for a Chinese affiliate, subsidiary, or contractor, then ServiceCo no longer is a "service provider" under PADFAA. *ServiceCo then falls into the general definition of "data broker." It appears to violate PADFAA, for instance, if its computer systems provide access to the sensitive information of a single U.S. individual.*

If ServiceCo fails to qualify for the "service provider" exception, then PADFAA may disqualify it from servicing any American company. This prohibition appears to apply even if ServiceCo qualifies as a "data broker" for only a small part of its business.

The analysis in the previous paragraphs reads the PADFAA text to mean that a minimal amount of business with one CBFA entity would affect a service provider's entire business. For example, assume that ServiceCo does work for WidgetCo and other companies that have no connection to a foreign adversary. Assume that ServiceCo also does work for ChinaExampleCo. In this example, ServiceCo appears to be a "data broker" but no longer qualifies as a "service provider" under PADFAA. ServiceCo would thus violate the law if it meets the other elements in the prohibition – providing access to the personally identifiable sensitive data of one U.S. individual.

Perhaps others can suggest a different interpretation of PADFAA. Absent such an interpretation, entities that provide services to many companies will lose their status as "service provider" if any one of their clients turns out to come within the broad definition of CBFA. This violation occurs due to the effect of two definitions:

1. The broad definition of "data broker" leads to a PADFAA violation when ServiceCo acts as a "data broker" by providing access to even one U.S. individual's sensitive data.
2. The narrow exception for "service provider" leads to a PADFAA violation if even one of ServiceCo's clients turns out to be CBFA.

A second exception to the "data broker" definition - the "not the product or service" exception - is open to more than one interpretation on whether it applies to many service providers. Even if ServiceCo doesn't qualify as a "service provider" under PADFAA, it can avoid being treated as a "data broker" if it meets a second exception, the "not the product or service" exception.

This "not the product or service" exception applies to an entity that:

1. "is providing, maintaining, or offering a product or service"
2. "with respect to which personally accessible sensitive data"
3. "**or access to such data**" (emphasis added)
4. "is not the product or service."

The "not the product or service" exception applies in an apparently simple way to entities that are "providing, maintaining, or offering" a **physical product**, even if that physical product is going to an individual or entity that is CBFA. For instance, WidgetCo can sell physical widgets, and not be covered as a "data broker."

The use of this exception, however, may be less clear as applied to a service. The common sense rationale for this exception is to prohibit actual data brokers – who sell data as a line of business – while permitting other service providers who perform other types of services. The text, however, is open to at least two interpretations:

1. Many service providers perhaps don't qualify for the exception. This interpretation focuses on the breadth of the term "access to such data." The word "access" is a broad term. Many types of service providers provide access to data, such as through software that helps WidgetCo give access to the corporate systems that each employee needs to do their job. Under this interpretation, ServiceCo doesn't qualify for the exception, if its service is providing access to any personally accessible sensitive data.
2. Many service providers perhaps qualify for the exception: Suppose that ServiceCo is hired to provide access to certain types of data, such as non-personal corporate records. As discussed below, the broad definition of "sensitive data" means that an employee or entity in China may have access to at least some "sensitive data." Nonetheless, under this interpretation, ServiceCo's business is to provide non-personal corporate records, not the "such" data (sensitive data) targeted by PADFAA. Even if ServiceCo enables access to some "sensitive data," its actions could be lawful under PADFAA – the product or service is not focused on providing "such data," i.e., "sensitive data." Under this interpretation, ServiceCo would qualify for the "not the product or service" exception, and would not be a "data broker."

As a law professor who has taught legislative interpretation, my view at this moment is that either interpretation may be correct. On the side that would ban more transactions, the broad goal of PADFAA is to stop transfers to foreign adversaries of any sensitive data about Americans. To achieve this goal, it makes sense to treat ServiceCo as a "data broker" if it actually enables access to any of that sensitive data. On the side that would ban fewer transactions, the "not the product or service" exception should be read broadly, and only prohibit "real" data brokers. *In short, many service providers currently face legal uncertainty about whether they qualify for the "not the product or service" exception, or instead would have their services banned by PADFAA*.

For the definition of "data broker," there is uncertainty about how sweeping the effect of the prohibition will be when part of a company's business fits an exception but another part does not.

There is an additional area of uncertainty in discussing the "data broker" exceptions for "service provider" and "not the product or service." As already discussed, the broad definition of CBFA means that the "service provider" exception often may not be available. The "not the product or service" exception may not apply when ServiceCo "provides access" to sensitive data.

The uncertainty arises from the interpretation of "to the extent." "The term 'data broker' does not include an entity *to the extent* that such entity" meets the exception. Suppose that ServiceCo has two lines of business, one as a "data broker" and the other as a service that does not enable any access to sensitive data. In this example, one plausible interpretation would be that ServiceCo can continue its non-data broker line of business under PADFAA, but not its data broker business. However, *"to the extent" is a vague term, and there appears to be uncertainty about whether in and in what ways PADFAA may enable ServiceCo to continue its non-data broker activities*.

PADFAA differs from the Biden Executive Order, which applies only to "bulk" transfers of data. Executive Order 14117 applies only to "bulk" transfers of data to a country of concern. By contrast, PADFAA's prohibition applies to any "sensitive data." The definition of "sensitive data" includes multiple references to the singular, rather than the plural, such as "a government-issued identifier," "any information" about health care, "a financial account number," or "an individual's race, color, ethnicity, or religion."

Because the PADFAA prohibition is triggered when data is "made available," such as through a computer system, the prohibition appears to apply to occasional, incidental, and perhaps even accidental ability to access one U.S. individual's sensitive data. ServiceCo may not have knowledge that any of this data is made available through its services, but the prohibition appears to apply nonetheless.

The definition of "sensitive data" is drafted broadly to address concerns about data broker sales to foreign adversaries, but the definition includes information that may be difficult to exclude from actual company systems. The principal and admirable purpose of PADFAA is to protect the sale of Americans' sensitive information to foreign adversaries, to protect both individual privacy (individuals consider this data sensitive) and national security (foreign adversaries should not be able to track U.S. military personnel via data brokers). To achieve these goals, it is understandable why the definition of "sensitive data" is inclusive, covering 17 categories of data, including some categories that go beyond the definitions of "sensitive data" in the comprehensive data privacy laws enacted in at least 14 states to date.[7] The law is intended to prevent data brokers from selling such data to foreign adversaries."

On the other hand, a service provider to an international company may provide access, in a corporate computer system, to many sorts of everyday information about an individual, such as:

1. The passport number of an employee, if the company assists with travel;
2. A credit card number, used for purposes such as reimbursements;
3. An individual's private communications, such as emails, or mention of a telephone number called;
4. Any information about an individual under the age of 17, apparently including mention of an employee's children's names; or
5. An individual's race, color, ethnicity, or religion.

Based on the analysis in this paper, the PADFAA prohibition appears to apply if there is even a single instance where these categories or any other sensitive data is available through a corporate computer system.

Conclusion: Why PADFAA may prohibit a U.S.-based service provider from processing data in the U.S. for a U.S.-based global company, even when that data is never accessed, and cannot be accessed, by a CBFA entity.

This detailed discussion of PADFAA and its definitions explains how the law appears to have broader prohibitions than its core goal, of prohibiting data broker sales of sensitive U.S. information to a foreign adversary or an entity controlled by a foreign adversary.

[7] For instance, I am not aware of a state law that specifies "information that reveals the status of an individual as a member of the Armed Forces," although a similar concern about selling such data to a foreign adversary helped motivate the recent Executive Order on bulk data sales. PADFAA also includes information "identifying an individual's online activities over time and across websites or online services." This definition may include "first party" information – information collected from individuals by the websites the individual chose to visit. By contrast, the major focus of state laws thus far has been on regulating "third party" information, where the data goes to someone other than the website that the individual navigated to.

As one important example, *consider how ServiceCo, based in the U.S., may lose the ability to process data in the U.S., for WidgetCo, based in the U.S.*.[8]

1. PADFAA goes beyond "sale" of data, and applies also where ServiceCo "provides access" or "makes available" any sensitive data.
2. WidgetCo pays ServiceCo, and all of the work done by ServiceCo meets the "for valuable consideration" requirement in the "data broker" definition.
3. ServiceCo becomes a "data broker," and loses its status as a "service provider," if it collects or receives data for any one entity that is CBFA.
4. The CBFA definition is broad, applying even to a single employee "domiciled" in China. Many companies that appear unrelated to a foreign adversary such as China may actually be CBFA, including Chinese subsidiaries or affiliates of U.S. companies."
5. ServiceCo would then be considered a "data broker." There is uncertainty about whether the PADFAA prohibition would apply only to services rendered to ChinaExampleCo, or to the services rendered to all of its clients.
6. Because there is no requirement of "bulk" data, PADFAA's prohibition applies if the sensitive data of even one U.S. individual is made available in the computer system.
7. In light of the broad definition of "sensitive" data, ordinary business practices often will "make available" in a company system at least one U.S. individual's sensitive data.

To summarize, the definitions appear to fit together in ways that would create, at a minimum, uncertainty for ServiceCo if its services for WidgetCo contain any data that would meet the broad definition of "sensitive" data. In addition, if ServiceCo happens to make such data available to one client, knowingly or unknowingly, it may lose its "service provider" status in general. Once that status is lost, ServiceCo may be a "data broker" when it does its ordinary business actions for its U.S. and other clients.

As stated above, this discussion is based on this professor's reading of the text of PADFAA. Comments and corrections are welcome to swire@gatech.edu.

[8] The example applies not just to companies and processing in the U.S., but also in allied and other countries not considered a foreign adversary.

May 7, 2024

Appendix to White Paper on Clarifying Definitions in Protecting Americans' Data from Foreign Adversaries Act

This Appendix compares the Protecting Americans' Data from Foreign Adversaries Act ("PADFAA") and Executive Order 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." ("EO 14117" or "EO") Where relevant, the Appendix refers to the Executive Order's Advance Notice of Proposed Rulemaking (ANPRM).

The Appendix presents a side-by-side comparison of important definitions in PADFAA and the EO/ANPRM, listed alphabetically and discussed in summary form here:

1. ***No definition of "bulk" in PADFAA.***

The EO applies to "bulk" sales of sensitive data. By contrast, there is no definition of "bulk" in PADFAA, and its scope is not limited to transactions involving data in bulk. As a result, as explained in the White Paper, PADFAA appears to apply where there is even one bit of sensitive data available to an entity subject to PADFAA's prohibition. PADFAA's scope is therefore significantly broader in this respect.

2. ***No finding of "unacceptable risk" to national security in PADFAA.***

The EO applies to "a class of transactions that has been determined by the Attorney General to pose an unacceptable risk to the national security of the United States." By contrast, there is no requirement in PADFAA of such a finding by the Attorney General of risk to national security.

3. ***Prohibitions on "providing access" to data***

Both PADFAA and the EO seek to prevent access to Americans' sensitive data by foreign adversaries. This includes restricting the sale of Americans' sensitive data to foreign adversary entities and persons, but they both go beyond the scope of "sales" to preventing "access," in different ways. PADFAA covers a broad scope of sensitive data transactions under its prohibition by including "to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available." The EO defines "access" with respect to "covered data transactions," including vendor, employment, and investment agreements. The ANPRM includes exemptions that keep certain types of transactions that may otherwise "provide access" to sensitive data outside its scope.

4. ***Controlled by a Foreign Adversary***

The PADFAA definition of "controlled by a foreign adversary" is similar to the ANPRM's definition of "covered person", with some differences. They both generally cover entities who are owned by, controlled by, or subject to the jurisdiction of a foreign adversary, along with such entities' respective employees and contractors. Companies headquartered in, or that have their principal place of business in, or are incorporated under the laws of, a foreign adversary are generally subject to their jurisdiction. They both also cover individuals who reside in foreign adversary countries. PADFAA is broader by covering companies where persons or entities of a foreign adversary country directly or indirectly own at least a 20% stake. PADFAA also covers any person subject to the direction or control of any CBFA person or entity.

5. Data Broker

Both definitions cover the selling, licensing, and providing access to data, but there are some differences in the language. PADFAA explicitly requires that the data broker receive valuable consideration in the transaction, language missing from the ANPRM definition. To be considered a data broker under PADFAA, the entity must not have collected directly from individuals, which is distinct from the ANPRM, where it is the *recipient* of the data that must not have collected or processed the data directly from the individuals. The PADFAA definition has a list of exceptions (see chart below) not present in the ANPRM, including two discussed in detail in the White Paper. First, to the extent that making sensitive data available is "not the product or service," the entity is not classified as a data broker. Second, to the extent an entity is acting as a service provider, it is also not a data broker under PADFAA. However, the definition of who qualifies as "service provider" is narrower than it may seem , as explained in the discussion of "service provider," below.

6. Sensitive Data & National Security Requirement

The PADFAA definition effectively covers all the data covered by the EO and adds a list of additional categories of sensitive data. Both definitions generally include personal identifiers (Social Security numbers, etc.), precise geolocation information, biometric and genetic data, and personal health and financial data. However, PADFAA adds private communications, calendar information, children's data, racial and religious information, online activity over time and across websites or online services, and several other categories (see chart below). The EO has two limits on its scope that are not present in PADFAA: (i) the sensitive data is able to be exploited by a country of concern to harm national security; and (ii) the definition applies only to the extent that is consistent with the International Emergency Economics Powers Act, which applies only within the scope of a declared national emergency. Furthermore, because the EO limits its prohibitions to sensitive data in bulk quantities and PADFAA does not, the universe of data and data transactions covered by PADFAA appears broader in practice in that respect.

7. *Service Provider*

PADFAA generally defines service providers similarly to a business associate under HIPAA or processor under GDPR, with one notable narrowing limitation. To be a service provider, the entity must process data on behalf of an individual or entity that is not CBFA – when a service provider enables access to sensitive data to anyone defined as CBFA, then it no longer meets the PADFAA definition of "service provider." "Service provider" is not defined in the EO or ANPRM, but it is mentioned five times in the ANPRM and asks for comment on how to address service providers.

PADFAA Term	PADFAA Definition	EO/ANPRM Term	EO/ANPRM Definition
	"Bulk" is not a term defined or used in PADFAA.	Bulk	EO §7(b) The term "bulk" means an amount of sensitive personal data that meets or exceeds a threshold over a set period of time, as specified in regulations issued by the Attorney General. The ANPRM sets varying volume-based "bulk thresholds" for each category of sensitive personal data based on a risk assessment of each category. See ANPRM §III(B).
Provides access	§2(a) It shall be unlawful for a data broker to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available personally identifiable sensitive data of a United States individual to – (1) Any foreign adversary country; or (2) Any entity that is controlled by a foreign adversary.	Access	EO §7(a) The term "access" means logical or physical access, including the ability to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, or otherwise view or receive, in any form, including through information technology systems, cloud computing platforms, networks, security systems, equipment, or software. The EO/ANDPRM prohibitions/restrictions are not directly based on providing access but are instead based on whether the transaction is a "covered data transaction" under ANPRM §III(D).
Controlled by a foreign adversary	§2(c)(2): The term ''controlled by a foreign adversary'' means, with respect to an individual or entity, that such individual or entity is— (A) a foreign person that is domiciled in, is headquartered in, has its principal place of business in, or is organized under the laws of a foreign adversary country;	Covered Person	EO §7(d): The term "covered person" means an entity owned by, controlled by, or subject to the jurisdiction or direction of a country of concern; a foreign person who is an employee or contractor of such an entity; a foreign person who is an employee or contractor of a country of concern; a foreign person who is primarily resident in the territorial jurisdiction of a country of concern; or any person designated by the

	(B) an entity with respect to which a foreign person or combination of foreign persons described in subparagraph (A) directly or indirectly own at least a 20 percent stake; or (C) a person subject to the direction or control of a foreign person or entity described in subparagraph (A) or (B).		Attorney General as being owned or controlled by or subject to the jurisdiction or direction of a country of concern, as acting on behalf of or purporting to act on behalf of a country of concern or other covered person, or as knowingly causing or directing, directly or indirectly, a violation of this order or any regulations implementing this order.
Data broker	§2(c)(3): (A) IN GENERAL.—The term ‘‘data broker’’ means an entity that, for valuable consideration, sells, licenses, rents, trades, transfers, releases, discloses, provides access to, or otherwise makes available data of United States individuals that the entity did not collect directly from such individuals to another entity that is not acting as a service provider. (B) EXCLUSION.—The term ‘‘data broker’’ does not include an entity to the extent such entity— (i) is transmitting data of a United States individual, including communications of such an individual, at the request or direction of such individual; (ii) is providing, maintaining, or offering a product or service with respect to which personally identifiable sensitive data, or access to such data, is not the product or service; (iii) is reporting or publishing news or information that concerns local, national, or international events or other matters of public interest; (iv) is reporting, publishing, or otherwise making available news or information that is available to the general public— (I) including information from—	Data brokerage	ANPRM §III(D): The program would define data brokerage as the sale of, licensing of access to, or similar commercial transactions involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data.

	(aa) a book, magazine, tele24 phone book, or online directory; (bb) a motion picture; (cc) a television, internet, or radio program; (dd) the news media; or (ee) an internet site that is available to the general public on an unrestricted basis; and (II) not including an obscene visual depiction (as such term is used in section 1460 of title 18, United States Code); or (v) is acting as a service provider.		
Sensitive Data	Note: There is no requirement in PADFAA of the finding of a national security emergency as required by IEEPA. §2(c)(5): The term ‘‘personally identifiable sensitive data’’ means any sensitive data that identifies or is linked or reasonably linkable, alone or in combination with other data, to an individual or a device that identifies or is linked or reasonably linkable to an individual. §2(c)(7): The term ‘‘sensitive data’’ includes the following: (A) A government-issued identifier, such as a Social Security number, passport number, or driver’s license number. (B) Any information that describes or reveals the past, present, or future physical health, mental	Sensitive Personal Data	EO §7(l) The term “sensitive personal data” means, to the extent consistent with applicable law including sections 203(b)(1) and (b)(3) of IEEPA, covered personal identifiers, geolocation and related sensor data, biometric identifiers, human ‘omic data, personal health data, personal financial data, or any combination thereof, as further defined in regulations issued by the Attorney General pursuant to section 2 of this order, and that could be exploited by a country of concern to harm United States national security if that data is linked or linkable to any identifiable United States individual or to a discrete and identifiable group of United States individuals. The term “sensitive personal data” does not include: (i) data that is a matter of public record, such as court records or other government records, that is lawfully and generally available to the public; (ii) personal communications that are within the scope of section 203(b)(1) of IEEPA; or

	health, disability, diagnosis, or healthcare condition or treatment of an individual. (C) A financial account number, debit card number, credit card number, or information that describes or reveals the income level or bank account balances of an individual. (D) Biometric information. (E) Genetic information. (F) Precise geolocation information. (G) An individual's private communications such as voicemails, emails, texts, direct messages, mail, voice communications, and video communications, or information identifying the parties to such communications or pertaining to the transmission of such communications, including telephone numbers called, telephone numbers from which calls were placed, the time calls were made, call duration, and location information of the parties to the call. (H) Account or device log-in credentials, or security or access codes for an account or device. (I) Information identifying the sexual behavior of an individual. (J) Calendar information, address book information, phone or text logs, photos, audio recordings, or videos, maintained for private use by an individual, regardless of whether such information is stored on the individual's device or is accessible from that device and is backed up in a separate location. (K) A photograph, film, video recording, or other similar medium that shows the naked or undergarment-clad private area of an individual.		(iii) information or informational materials within the scope of section 203(b)(3) of IEEPA.

	(L) Information revealing the video content requested or selected by an individual. (M) Information about an individual under the age of 17. (N) An individual's race, color, ethnicity, or religion. (O) Information identifying an individual's online activities over time and across websites or online services. (P) Information that reveals the status of an individual as a member of the Armed Forces. (Q) Any other data that a data broker sells, licenses, rents, trades, transfers, releases, discloses, provides access to, or otherwise makes available to a foreign adversary country, or entity that is controlled by a foreign adversary, for the purpose of identifying the types of data listed in subparagraphs (A) through (P).		
Service provider	§2(c)(8): The term ''service provider'' means an entity that— (A) collects, processes, or transfers data on behalf of, and at the direction of— (i) an individual or entity that is not a foreign adversary country or controlled by a foreign adversary; or (ii) a Federal, State, Tribal, territorial, or local government entity; and (B) receives data from or on behalf of an individual or entity described in subparagraph (A)(i) or a Federal, State, Tribal, territorial, or local government entity.		"Service provider" is not defined in the EO or the APRM.