4.4 National Privacy Considerations

Return to Common Elements | **Provide Feedback**

Overview

Return to Top

Although there is no general federal legislation for data and metadata protection and privacy, there are a number of federal data protection laws that are sector-specific or focus on particular types of data. In addition to the Federal regulations, there are some state laws that are also applicable.

Table 1 summarizes the number of U.S. Laws and Regulations covering Privacy Considerations. The total number (i.e., **16**) indicates the complexity of the Privacy that confronts the CBDC just within the U.S. The more Laws and Regulations, the more effort there is to coordinate the CBDC efforts and to work with the Legislative and Executive Branches to keep the Laws and Regulations current with CBDC efforts.

Table 1: Summary of the number of laws and regulations covering National Security Considerations.

U.S. Privacy Consideration	No. of Laws and Regulations
U.S. Federal Laws and Regulations	10
U.S. State Laws and Regulations	6
Total	**16**

U.S. Federal Laws and Regulations

Return to Top

There is no single U.S. law or regulation covering **Privacy**, but a whole set of laws. Table 2 outlines most of the laws as determined by the OMG DIDO-RA .

There are roughly 10 Laws and Regulations in the U.S. covering Privacy.

Table 2: List of Applicable U.S. Federal Laws.

U.S. Federal Laws		
Kind	**Law / Regulation**	**Description**
Privacy	**Driver's Privacy Protection Act of 1994 (DPPA)**	DPPA governs the privacy and disclosure of personal information gathered by state Departments of Motor Vehicles, including photographs, Social Security Number (SSN), Driver Identification Number (DID), name, address (but not the five-digit ZIP code), telephone number, medical information and disability information.
Privacy	**Video Privacy Protection Act (VPPA)**	VPPA restricts the disclosure of rental or sale records of videos or similar audio-visual materials, including online streaming.
Privacy	**Cable Subscriber Protection**	Cable Subscriber Protection provides access to all Personal Identifiable Information (PII) regarding the subscriber which is collected and maintained by a cable operator.

U.S. Federal Laws		
Kind	**Law / Regulation**	**Description**
Privacy	**Right to Financial Privacy Act of 1978 (RFPA)**	The RFPA was put in place to limit the government's ability to freely access nonpublic financial records. The RFPA defines financial institutions as any institution that engages in activities regarding banking, credit cards, and consumer finance. It also defines financial records as any documentation of a consumer's relationship with a financial institution.
Privacy	**Gramm-Leach-Bliley Act (GLBA)**	The GLBA promotes consumer privacy, the Gramm-Leach-Bliley Act included regulations to limit the ways in which companies handled and shared financial data.
Privacy	**Fair Credit Reporting Act (FCRA)**	The FCRA regulates credit agencies and promotes fair and secure handling of consumer information. The FCRA attempts to limit the dissemination of information through five main rules: 1. Credit reports and investigative reports must be differentiated so that any irrelevant data are not mixed 2. Reports can only be made available to those with “legitimate business needs” 3. The subject of a report must be notified of any request for their information 4. Agencies must give consumers access to their own files if they should ever request them 5. A time limit is set for the retention of information on reports. Information that is seven years or older must be deleted, while information regarding bankruptcies can be removed only after fourteen years
Privacy	**Fair and Accurate Credit Transactions Act (FACTA)**	FCRA amended the FCRA with stricter regulations that need to be enforced first. State laws regarding credit scores, credit reports, and insurance were to remain in effect as a result of the amendments. FCRA gave consumers more rights to explanations of their credit scores and the right to a free credit report each year. It also includes two rules: 1. Disposal Rule - how to dispose of consumer records 2. Red Flag Rule - how financial institutions identify and prevent identity thefts
Privacy	**Credit and Debit Card Receipt Clarification Act**	Credit and Debit Card Receipt Clarification Act requires account numbers printed on receipts have to be shortened to five digits in order to protect consumer privacy
Privacy	**Fair Debt Collection Practices Act (FDCPA)**	Under the FDCPA, collectors are not allowed to publish a consumer's name and address on a bad debt list or reveal any information regarding the debt to unaffiliated third parties except the consumer's partner or attorney.
Privacy	**Electronic Funds Transfer Act**	The act implemented requirements so that banks have to notify their customers of any policies regarding the electronic transfer of funds. Banks are also held liable in the event that information is disclosed through telephone without consent. Also, banks would be held responsible for any damages that came as a result of unauthorized access to a consumer's information.

U.S. State Laws and Regulations

Return to Top

The U.S. States each can have their own laws or regulations covering **Privacy**, as well as, a whole set of laws. Table 3 outlines most of the U.S. State laws as determined by OMG DIDO-RA .

There are roughly 6 major U.S. State Laws and Regulations covering Privacy.

> **Note:** FACTA ensured that any state laws with stricter regulations than those outlined in the FCRA would be enforced first. State laws regarding credit scores, credit reports, and insurance that were to remain in effect as a result of the amendments were outlined within the act.

Table 3: List of Applicable U.S. State Laws and Regulations.

State Laws		
Kind	**Law / Regulation**	**Description**
Privacy	**California Privacy Act**	California Privacy Act is a state-level privacy act that provides protection of consumer information. The act is described as a stricter version of the Gramm-Leach-Bliley Act.
Privacy	**California Consumer Privacy Act (CCPA)**	CCPA gives consumers more control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law.
Privacy	**California Consumer Credit Reporting Agencies Act (CCCRA)**	The CCCRA regulates consumer credit reporting agencies as well as any users of credit reports. The act also provides a narrower definition of “consumer credit report” as any information that falls within credit reports is protected by the act.
Privacy	**California Right to Financial Privacy Act**	California's Right to Financial Privacy Act regulates the state's government agencies' abilities to access nonpublic consumer information. As a result of the act, California's government agencies are not authorized to access financial records unless the consumer gives consent or if a subpoena or a search warrant is issued for the information.
Privacy	**California Song-Beverly Credit Card Act**	Under the California Song-Beverly Credit Card Act, companies may not collect personally identifiable information from consumers who purchase goods or services using credit cards. Companies cannot set conditions in which consumers must consent to share their information in order to use their credit cards for a transaction. However, consumer information can be requested in order to complete a credit card transaction as long as the information is never recorded. The act also set a redundant state-level requirement that companies must shorten a consumer's credit and debit card information on receipts.
Privacy	**Vermont Privacy of Consumer Financial and Health Information**	The law defines the purpose, scope, application, compliance, and exceptions to the law. The purpose of the Vermont Privacy of Consumer Financial and Health Information is to govern the treatment of nonpublic personal information about consumers by financial institutions.

Exemplar for Metadata

Return to Top

The following user scenario is meant as an exemplar of the importance of Data Strategy and Data Governance for a U.S.-based CBDC.

Theoretical Problem

Return to Top

The following is a theoretical problem used to highlight some major issues with privacy.

Two U.S. citizens go into a U.S. clinic: John Doe and Jame White.

- John Doe works in an assembly line
- Jane White is a Chief Executive Officer (CEO) and President of one of the largest, most valued innovative companies in the world

Both show up at a medical facility that treats mental health and substance abuse. The diagnosis and treatment for John and Jane are identical, with the same prognosis, and the outcomes are expected to be the same. On a personal level, this is a tragedy for both John and Jane, their families, and their friends.

Both John and Jane would like to keep their visit to the medical facility quiet. John has a better chance of keeping his visit secret, especially since there is no real economic incentive to divulge the secret. However, if it is known that Jane has visited this clinic, the collateral impact on her company, its employees, the investors, and even those investing in competing companies can be wide-reaching and significant.

Regardless, if the data and metadata are about John or Jane, there is a reasonable expectation by both of them that data and metadata about their transaction with the medical facility are secure and remain private.

Theoretical Solution

Return to Top

A theoretical solution is for the CBDC to develop a rigorous and comprehensive Data Strategy that guarantees the security and privacy of the transactional data associated with the CBDC. The CBDC and the Federal Reserve do not need to develop their own Security and Privacy framework but can rely on the existing framework laid out by the U.S. Federal Government.

The OMG DIDO Reference Architecture (DIDO-RA) provides a discussion on what a **U.S. Federal Data Strategy** is.

U.S. Federal Government on Data Strategy

Return to Top

The following is from the U.S. Federal Government on Data Strategy:

> *The U.S. **Federal Data Strategy (FDS)** provides a common set of data principles and best practices. The 2020 Action Plan identifies milestones that are essential for establishing processes, building capacity, and aligning existing efforts. This initial plan builds a solid foundation that will support the implementation of the strategy over the next decade.*
> https://strategy.data.gov/progress/

- Privacy refers to the control over a person's Personal Identifiable Information(PII) and how the information is used. PII is any information that can be used to determine a person's identity.
- Security refers to how protected a person's PII is from unauthorized or unintended use.

The DIDO-RA summarizes the areas required for a U.S. Federal Data Strategy covering the following areas:

1. Principles

- Ethical Governance
- Conscious Design
- Learning Culture

2. Practices

- Building a Culture that Values Data and Promotes Public Use
- Governing, Managing, and Protecting Data
- Promoting Efficient and Appropriate Data

3. Actions

- Agency Actions
- Community of Practice Actions
- Shared Solution Actions

Examples

Return to Top

The “desirements” specified in White Paper and identified by the OMG's White Paper Analysis as **Privacy Issues** are listed in Table 4.

Table 4: Examples of **Privacy Desirements** identified during the White Paper Analysis conducted by the

OMG

Category	Desirements
Benefits	B0004, B0022
Policies and Considerations	P0004
Risks	R0014
Design	D0012

Note: B = Benefit, **P** = Policy, **R** = Requirement, **D** = Design.

Discussion of Examples

Return to Top

Table 5 provides discussion points for each of the “desirements” identified by the OMG's White Paper Analysis.

Table 5: Privacy references of desirements in the **White Paper**

Desirement No.	Desirement Text	Comment
B0004	**Protect consumer privacy**	Consumer privacy is information privacy as it relates to the consumers of products and services. A variety of social, legal and political issues arise from the interaction of the public's potential expectation of privacy and the collection and dissemination of data by businesses or merchants
B0022	**Provide a CBDC that is:** **1. YES Privacy-Protected** **2. NO Intermediated** **3. NO Widely Transferable** **4. NO Identity-Verified**	Privacy-Protected means that the Central Bank Digital Currency (CBDC) protecting consumer privacy is critical. Any CBDC would need to strike an appropriate balance, however, between safeguarding the privacy rights of consumers and affording the transparency necessary to deter criminal activity.
P0004	**Protect consumer privacy**	See **B0004**.
R0014	**Risk of not achieving an appropriate balance between safeguarding the privacy rights of consumers and affording the transparency necessary to deter criminal activity**	1. See **B0004** for Consumer privacy. 2. Transparency is the ability to easily access and work with data no matter where they are located or what application created them, or the assurance that data being reported are accurate and are coming from the official source.
D0012	**Design should address privacy concerns by leveraging existing tools already in use by intermediaries**	Intermediaries means commercial banks and regulated **nonbank** financial service providers that would operate in an open market for CBDC services
B = Benefit Considerations		

Desirement No.	Desirement Text	Comment
P = Policy Considerations		
R = Risk Considerations		
D = Design Considerations		

Note: FACTA ensured that any state laws with stricter regulations than those outlined in the FCRA would be enforced first. State laws regarding credit scores, credit reports, and insurance that were to remain in effect as a result of the amendments were outlined within the act.

Table 6: List of Applicable U.S. State Laws and Regulations.

State Laws		
Kind	**Law / Regulation**	**Description**
Privacy	**California Privacy Act**	California Privacy Act is a state-level privacy act that provides protection of consumer information. The act is described as a stricter version of the Gramm-Leach-Bliley Act.
Privacy	**California Consumer Credit Reporting Agencies Act (CCCRA)**	The CCCRA regulates consumer credit reporting agencies as well as any users of credit reports. The act also provides a narrower definition of “consumer credit report” as any information that falls within credit reports is protected by the act.
Privacy	**California Right to Financial Privacy Act**	California's Right to Financial Privacy Act regulates the state's government agencies' abilities to access nonpublic consumer information. As a result of the act, California's government agencies are not authorized to access financial records unless the consumer gives consent or if a subpoena or a search warrant is issued for the information.
Privacy	**California Song-Beverly Credit Card Act**	Under the California Song-Beverly Credit Card Act, companies may not collect personally identifiable information from consumers who purchase goods or services using credit cards. Companies cannot set conditions in which consumers must consent to share their information in order to use their credit cards for a transaction. However, consumer information can be requested in order to complete a credit card transaction as long as the information is never recorded. The act also set a redundant state-level requirement that companies must shorten a consumer's credit and debit card information on receipts.
Privacy	**Vermont Privacy of Consumer Financial and Health Information**	The law defines the purpose, scope, application, compliance, and exceptions to the law. The purpose of the Vermont Privacy of Consumer Financial and Health Information is to govern the treatment of nonpublic personal information about consumers by financial institutions.