DRAFT
Report of the
Identity Management Legal Task Force
American Bar Association

Solving the Legal Challenges of
Online Identity Management

PART 2
Legal Regulation of, and Barriers to
Identity Management

The views expressed herein have not been approved by the Council of the Section of Business Law, the House of Delegates or the Board of Governors of the American Bar Association and, accordingly, should not be construed as representing the policy of the American Bar Association.

Please submit comments to Task Force Chair:
Thomas J. Smedinghoff: tsmedinghoff@edwardswildman.com

2183159_2.DOC
# TABLE OF CONTENTS

Executive Summary .......................................................................................................................... 1

Scope and Structure of Report ........................................................................................................ 1

LEGAL REGULATION OF, AND BARRIERS TO, IDENTITY MANAGEMENT .......... 2

1. General Law Potentially Applicable to Identity Management .............................................. 3
   1.1. Law Governing the Conduct of Identity System Participants Generally ................... 4
      1.1.1. Tort Law - Negligence ................................................................................. 4
      1.1.2. Unfair Business Practices Law ................................................................. 5
   1.2. Law Governing the Accuracy of Identity Information ............................................ 6
      1.2.1. Negligent Misrepresentation ........................................................................ 6
      1.2.2. Negligent Endorsement ................................................................................ 7
      1.2.3. Defamation ................................................................................................... 8
      1.2.4. False Statement Acts ..................................................................................... 8
      1.2.5. Warranty Law .............................................................................................. 8
      1.2.6. Identity Theft Laws .................................................................................... 10
   1.3. Law Governing the Privacy of Identity Information ............................................. 10
   1.4. Law Governing the Security of Identity Information and Processes ..................... 11
   1.5. Law Governing Use of Public Sector Information ................................................ 15
   1.6. Law Governing Intellectual Property Rights ......................................................... 16
      1.6.1. Ownership Issues ....................................................................................... 16
      1.6.2. Patent Law ................................................................................................. 16
      1.6.3. Copyright Law ........................................................................................... 16
      1.6.4. Trademark and Trustmark Law ................................................................. 17
   1.7. [Other Law??] ........................................................................................................ 17

2. Law that Specifically Regulates Identity Management Activities ............................... 17
   2.1. Laws Focused on a Duty to Identify ...................................................................... 17
   2.2. Laws Focused on a Duty to Authenticate .............................................................. 18
   2.3. Laws Regulating Identity Systems or Participants ................................................ 21

3. Legal Barriers Created by Existing Laws and Regulations ........................................ 22
   3.1. Law Does Not Address All Relevant Issues ......................................................... 22
   3.2. Legal Uncertainty / Ambiguity ............................................................................. 23
   3.3. Inappropriate Results .......................................................................................... 23
   3.4. Jurisdictional Variations and Conflicts .................................................................. 23
   3.5. Inability to Modify Law by Contract ..................................................................... 24
   3.6. Other Legal Factors ........................................................................................... 24
      3.6.1. Nature of the Participant ............................................................................ 24
      3.6.2. Nature of the Information .......................................................................... 25
      3.6.3. Nature of the Use ....................................................................................... 25
      3.6.4. Nature of the Harm .................................................................................... 25

Executive Summary
[to be completed after rest of doc]

Scope and Structure of Report

This Report examines the legal issues associated with the development, implementation, operation, and maintenance of online identity systems. Its primary objectives are to:

- Provide a general understanding of the concept of identity management sufficient to identify and analyze the legal issues;
- Identify the legal issues raised by the development, implementation operation, and maintenance of online identity systems, both in the U.S. and internationally;
- Analyze those legal issues so as to better understand their impact and to evaluate possible approaches for addressing them where required;
- Identify existing law applicable to online identity management, and any barriers created by such law;
- Evaluate possible approaches to developing the Legal Rules for an identity system;
- Clarify the interaction between the technical controls and legal obligations of the stakeholders in an identity management ecosystem; and
- [Other??]

This Report is set forth in three parts, as follows:

- Part 1: Identity Management Fundamentals and Terminology
- Part 2: Legal Regulation of, and Barriers to, Identity Management
- Part 3: Structuring the Legal Framework for an Identity System
LEGAL REGULATION OF, AND BARRIERS TO, IDENTITY MANAGEMENT

This Part 2 has two objectives. The first is to identify and describe (by way of example) some of the primary types of existing laws and regulations that comprise the Legal Framework, and which will impact the development of System Rules, for an identity system. The second is to identify the legal barriers to the operation of an identity system resulting from such existing laws and regulations, which must be addressed in the System Rules of an identity system.

In most jurisdictions there are numerous existing laws and regulations that will have a significant regulatory impact (and which may impose barriers, compliance requirements, and/or liability risk) on participation in an identity system. Some of these laws and regulations focus specifically on identity-related activities. Most, however, were developed in a context completely unrelated to identity management (e.g., tort laws, contract law, warranty law, etc.), but may nonetheless have a significant impact, and often in ways that were unanticipated at the time of their original adoption.¹

Such laws and regulations will directly regulate, inform or influence the development of the System Rules for an Identity system. In some circumstances these laws and regulations can be altered by contractual agreement; in other cases they cannot. But in all cases, existing law will comprise at least part of the overall Legal Framework in which an Identity system operates. In fact, unless the System Rules for an identity system include contractually-defined Legal Rules, existing laws and regulations will define the entirety of the Legal Rules of an Identity system.

As a result, it is critical to understand which of such laws and regulations apply to identity systems, and what impact they have.

The presence of background law supports all commercial, governmental and social structures. For example, the presence of a court system (and its many rules of procedure, evidence and jurisdiction) provides private parties with a forum for the resolution of commercial and social disputes. Even the most hardened anti-regulation advocate does not advocate for an abolition of the court system. There are myriad zoning laws, traffic laws, criminal laws, commercial laws, corporate laws, trade laws and many, many other public law constructs that offer support to the many commercial transactions and social and governmental interactions that all individuals and commercial, governmental and other entities depend on.

In fact, not only is the legal landscape largely dependent on public law, many of the players owe their very existence to public law sources. All legal entities (such as corporations, LLCs, LLPs, partnerships, co-ops, REITs, non-profit organizations and many others owe their entire existence and legal capacity to government legislation and regulation.

All of this is a way of saying that role for government legislation and regulation in supporting reliable, predictable, normalized identity and attribute management systems. In some jurisdictions that role will be more limited, while in others it will be more expansive. The

¹ See, e.g., Smedinghoff, CA Liability Analysis.
question is, for a system of the jurisdictional and sectoral scope of the internet on which most identity systems will function, how much of the rulemaking should appropriately be attempted by a single or even multiple sovereigns, and how much of the rulemaking effort can be more appropriately and nimbly accomplished from various rule making collaborations among the system participants.

The latter model, a self-regulatory structure, is at the heart of many commercial markets, but in each instance is supported in some way by government laws and regulations. Notwithstanding such support, SROs derive most of their authority from the sheer force of their benefits to participants. These benefits together form a sort of “economic compulsion” that arises from the cost savings, risk reduction, stakeholder efficacy, revenue generation and market expansion opportunities that derive from consensus-based, common rules and standard Operating Agreements that will help to make identity systems perform more reliably and in accordance with known, predictable rules.

A similar form of “economic compulsion” is the essence of the value proposition associated with the rule sets that form the core of all commercial markets, social communities and political governance structures. The documented rules, rights and duties, which are derived from public or private law sources, form the core of the legal “users guide” to engaging with such structures. For example, if you want to trade on the crude oil commodities exchange, you better know the rules for that market.

Those core rule sets are in the process of being constructed in the nascent federated identity systems that are being developed on top of the internet and other networked information systems. They are being built on an existing legal landscape that provides the starting point of the design, development and deployment exercise for future legal structures for these systems. It is to that landscape that this report will now turn.

1. General Law Potentially Applicable to Identity Management

There are numerous laws and regulations that, while not specifically focused on identity management, may have a significant impact on identity systems or various identity management activities. Obvious examples include the various laws regulating the privacy and security of the personal information that is collected and shared as part of any identity management process. Warranty law and the common law of negligent misrepresentation (both of which may govern the liability of the Identity Provider for incorrect identity credentials and identity assertions) may also have a significant effect. There are myriad other existing laws and regulations that will have an effect on the organization and operation of identity systems such as employment laws, intellectual property laws, banking laws, telecommunication laws, public records laws, and a host of others. A comprehensive treatment of all such laws, even within the U.S., is beyond the scope of this report. The following will identify the major categories of existing laws and regulations likely to affect identity management.

2 Note that the Open Identity Exchange hosts a “knowledge center” that is intended to provide a collaborative tool for the accumulation and analysis of these laws, and the further development of the ideas discussed in this Report.
1.1. Law Governing the Conduct of Identity System Participants Generally

1.1.1. Tort Law - Negligence

In the absence of contractual commitments, the performance of duties under many identity system relationships may be evaluated pursuant to the concepts and analytical structures of tort law. This includes the law of negligence, including negligent misrepresentation and negligent endorsement, intentional torts such as fraud, and the privacy-related torts of misappropriation of name or image for commercial purposes without compensation, invasion of privacy, publication of private facts, and defamation. In the U.S., much of this is common law. In civil law countries some of these rules are formalized by statute.

Negligence is perhaps the broadest category of tort liability imposed for harm caused to others. Negligence occurs when one fails to meet a recognized minimum standard of accountability to others for actions or activities that result in some damage to persons or property.\(^3\) The elements of a cause of action in negligence are: (1) a legally-recognized duty to another person or class of persons; (2) breach of that duty by failing to meet the legally-recognized level of conduct (i.e., the “standard of care”) in performing that duty; (3) the breach must actually cause, or be legally linked to, the cause of harm to a person or property; and (4) the complaining person must suffer compensable damages as a result of the activity.\(^4\)

In identity transactions, negligence can take many forms. Basically the breach of any duty by any participant in an identity transaction that causes harm to another participant (or third party) could form the basis for a claim of negligence. It might include, for example, the failure of an Identity Provider to properly identify a Subject or to revoke the Subject’s credential when requested, the failure of a Subject to protect his or her private key or to request revocation of his credential in the event his key is compromised, or the failure of a Relying Party to validate/authenticate a credential before reliance. Essentially any acts or omissions that cause harm to other participants in the identity system, or that cause harm to third parties, may form the basis for a negligence claim if it represents the breach of a duty assumed by the participant by virtue of its participation in an identity transaction.

The duty of care and the standard by which it is measured can arise under common law, can be founded on a statute, or it can be created and defined by the System Rules governing the identity system. [add cites re system rules]

Some courts have applied the law of negligence to conduct relating to identity transactions. For example, in *Wolfe v. MBNA America Bank*\(^5\) the court held that, under Tennessee negligence law, where “the injury resulting from the negligent issuance of a credit card is foreseeable and preventable, . . . Defendant has a duty to verify the authenticity and


accuracy of a credit account application before issuing a credit card.”

“[T]his duty to verify” the court held, “requires Defendant to implement reasonable and cost-effective verification methods that can prevent criminals, in some instances, from obtaining a credit card with a stolen identity.”

[Discuss other cases?? Discuss economic loss doctrine?? Perhaps include a discussion of Citizens Financial Bank and Experi-Metal here??]

1.1.2. Unfair Business Practices Law

In the U.S., statutes at both the federal and state level prohibit unfair and deceptive business practices. [Do other countries have such laws??]

While unfair and deceptive business practice statutes are aimed at a wide variety of inappropriate business practices, they have been used recently to punish failure to properly identify persons with whom one is doing business. Cases to date have primarily been aimed at relying parties who failed to properly identified the parties they thought they were dealing with, resulting in damages to other third parties.

For example, in the wake of a well-publicized security breach, the U.S. Federal Trade Commission (FTC) filed a complaint in 20__ against ChoicePoint under Section 5 of the Federal Trade Commission Act (which governs unfair and deceptive business practices generally). That complaint alleged that ChoicePoint “has not employed . . . reasonable policies and procedures to . . . verify or authenticate the identities and qualifications of prospective subjects.” Specifically, the FTC alleged that “ChoicePoint failed to detect [false credentials and other misrepresentations] because it had not implemented reasonable procedures to verify or authenticate the identities and qualifications of prospective subjects.”

Similarly, in the March 2009 the FTC alleged that a consumer reporting agency failed to employ reasonable and appropriate security policies and procedures to “verify or authenticate the identities and qualifications of prospective subjects,” and that as a result, it sold at least

§ 485 F.Supp.2d at 882.

¹ Id.


³ Id., Complaint at Para. 13.

¹⁰ U.S. v. Rental Research Services, Inc., FTC File No. 072 3228, D. Minn. (Stipulated Final Judgment, March 5, 2009), (Settlement of allegations that its lack of reasonable client identification procedures and adequate data security safeguards resulted in the sale of credit reports to identity thieves); available at http://www.ftc.gov/os/caselist/0723228.

318 credit reports to identity thieves. This practice, the FTC asserted, was “an unfair act or practice” in violation of Section 5 of the FTC Act, as well as the FCRA.\textsuperscript{12}

In addition, the FTC is on record recommending “that Congress consider establishing national consumer authentication standards covering all private sector entities that maintain consumer accounts.” These standards, the FTC indicated, “should require private sector entities to create a written program that establishes reasonable procedures to authenticate new or existing customers.”\textsuperscript{13}

\textbf{[Cite other FTC authentication cases as well. Discuss similar laws in other countries]}

\textbf{1.2. Law Governing the Accuracy of Identity Information}

Identity management activities focus on the collection, verification, and/or communication by Identity Providers and/or Attribute Providers of information about Subjects to Relying Parties. At its essence, this involves the communication of information in situations where the accuracy and/or reliability of that information are important. It is therefore possible that a variety of existing laws regarding providing false or incorrect information, whether intentionally or negligently, will be relevant in the evaluation of the rights, obligations, and liabilities of the participants in identity systems. Key among those are the following:

\textbf{[Consider research on the tort of negligent credentialing – e.g., in the medical field.]}\textsuperscript{21}

\textbf{1.2.1. Negligent Misrepresentation}

The tort of negligent misrepresentation creates liability for intentionally communicating false information in a situation where the information provider did not exercise reasonable care in determining the accuracy of the information prior to the communication. In the right circumstances, an incorrect assertion of one or more identity attributes, for example, might qualify as a negligent misrepresentation.

The definition of negligent misrepresentation used by a majority of courts in the U.S., states:

\begin{quote}
§ 552 Information Negligently Supplied for the Guidance of Others

(1) One who, in the course of his business, profession or employment, or in any other transaction in which he has a pecuniary interest, supplies false information for the guidance of others in their business transactions, is subject to liability for pecuniary loss caused to them by their justifiable reliance upon the
\end{quote}

\textsuperscript{\textcopyright}

\textsuperscript{12} Id., at para. 29.

information, if he fails to exercise reasonable care or competence in obtaining or communicating the information.\textsuperscript{14}

In essence, the tort of negligent misrepresentation is grounded in the duty of suppliers of information (such as an Identity Provider or Attribute Provider) to use “reasonable care or competence” in making representations to others (e.g., credentials and the identity assertions they contain), so as to prevent harm caused by justifiable reliance on that information. Most states in the U.S. recognize negligent misrepresentation in their common law.\textsuperscript{15}

This tort creates a duty to exercise reasonable care or competence to verify facts and creates liability for incorrect representations made without exercising reasonable care about the accuracy of the facts asserted.\textsuperscript{16} It does not, however, make the information provider a guarantor of the accuracy of an identity assertion. Generally, the information provider does not have liability for inaccurate or “false” information unless the provider failed to exercise reasonable care in obtaining or communicating the information. Thus, the tort of negligent misrepresentation does not create absolute liability, but rather a standard of care based on reasonableness to which the information provider is held. And as with the tort of negligence generally, the standard for the duty of care can arise under common law, can be founded on a statute, or it can be created and defined by the System Rules governing the identity system. [add authority for latter point]

1.2.2. Negligent Endorsement

In addition to liability for negligent misrepresentation based upon statements made in credentials issued by the Identity Provider, there exists the possibility that the use of Identity Provider branded credentials by Subjects (such as to validate the identity of their Web site or to validate the identity of their own business) may be construed as an endorsement of the Subject by the Identity Provider in a manner that would constitute negligent misrepresentation.

A line of cases holds that endorsers of products may be liable for negligent misrepresentation if the product fails to live up to the justifiable expectations of quality created by the endorsement and a consumer is harmed by relying on that endorsement. Independent testing laboratories such as Underwriters Laboratory,\textsuperscript{17} magazines which endorse products such as Good Housekeeping,\textsuperscript{18} and trade associations which lend their mark to products\textsuperscript{19} have all been held liable for negligent misrepresentation when the products that enjoyed their

\textsuperscript{14} \textit{RESTATEMENT (SECOND) OF TORTS} § 552(1) (1977).
\textsuperscript{17} \textit{Hempstead v. General Fire Extinguisher Corp.}, 269 F. Supp 109 (D.C. Del. 1967). Information about the Underwriters Laboratory “UL” marks is available at \href{www.ul.com}{www.ul.com}.
\textsuperscript{19} \textit{King v. Nat’l Spa and Pool Inst., Inc.}, 570 So.2d 612 (Ala. 1990).
endorsement failed to meet expectations. It is possible that, in the proper circumstances, a credential itself might be considered an endorsement by the Identity Provider of the identity (e.g., the Web site) that it is used to verify. That is, the Identity Provider may be perceived as lending its reputation and mark to the transaction for the purpose of building trust -- conduct that could be considered to make the Identity Provider analogous to an endorser.

1.2.3. Defamation

The elements of a claim for the tort of defamation include a false statement of fact about a person that is considered defamatory and that is published to a third party.\(^{20}\) Question sto consider include whether the issuance of an identity credential to an identity thief can constitute defamation of the person whose identity was stolen, or whether an inaccurate credential issued to (or inaccurate identity assertion issued about) the correct person can also be considered defamation. [Asserting an attribute – e.g., poor credit, age, employment, etc. might be defamatory?? Need Research]

1.2.4. False Statement Acts

The making of false or deceptive statements to government identity proofers by Subjects seeking a credential could be subject to false statement laws at the federal or state level. For example, when dealing with the U.S. federal government, the U.S. law make it a crime to knowingly and willfully: (1) falsify, conceal, or cover up a material fact; (2) make any materially false, fictitious, or fraudulent statement or representation; or (3) make or use any false writing or document knowing it to contain any materially false, fictitious, or fraudulent statement or entry.\(^{21}\) The purpose of the statute is to "punish those who render positive false statements designed to pervert or undermine functions of governmental departments and agencies."\(^{22}\) [Do similar laws exist in other countries??]

1.2.5. Warranty Law

Does someone who makes an identity assertion – e.g., the Subject making an assertion of his own identity to the Identity Provider, or the Identity Provider making an assertion about a Subject’s identity to a Relying Party – make a warranty as to the accuracy of the information? It would appear, for example, that the conduct of the Identity Provider – e.g., in issuing credentials and making identity assertions – could, in appropriate circumstances, be argued to create a warranty under existing law. Warranty concepts arise in a variety of circumstances, and several existing laws address warranties, and may potentially be applicable.

In the U.S., the Uniform Commercial Code affirms the existence of express warranties based on statements or affirmations of the seller and also creates various implied warranties that

---

\(^{20}\) See, generally, Rodney A. Smolla, LAW OF DEFAMATION, 2Ed. (Thomson Reuters/West, 2008), at Section 1:34.

\(^{21}\) 18 U.S.C. § 1001

become part of the contract between the parties. The Magnuson-Moss Warranty Act regulates warranties to consumers (but only for products, not services). [The concept of a warranty also arises under common law.]

In analyzing any law regarding warranties, two key questions must always be considered: (1) What warranties apply? and (2) Who receives the benefit of the warranties? In the U.S. for example, Uniform Commercial Code (UCC) Article 2 (which applies to goods, not information), addresses three types of warranties: (1) express warranties, (2) implied warranties of merchantability, and (3) implied warranties of fitness for a particular purpose. In addition, the UCC extends such warranties to certain persons other than the purchaser on the theory that such persons are third-party beneficiaries of the warranties.

Other common law warranty obligations often apply to transactions in services and to contracts pertaining specifically to the provision of information. And as noted in Section ___ below, some identity-specific statutes (e.g., ________) mandate the creation of warranties. Thus, it is certainly possible that identifying Subjects and issuing and validating credentials and identity assertions could be construed to involve the making of a warranty.

UCC law governing contracts and associated warranties for goods is very results-oriented -- certain default warranties and other obligations arise under a UCC-governed contract to ensure that the product conforms to ordinary standards of performance. Conversely, the common law governing contracts and associated warranties for services (which presumably includes identity management services) is more process-oriented. Courts ask whether the provider of the service performed in a reasonably careful and workmanlike manner, especially in light of the particular trade or profession from which the service provider is drawn and of the abilities, skill, and knowledge claimed by that service provider. Because those who provide services often must deal with factors beyond their control, courts tend not to read into contracts express and implied warranties that amount to “insuring” or “guaranteeing” favorable results, unless the parties have expressly agreed to that higher standard (which often entails the payment of a higher price). Alarm/security companies, title searchers, inspectors, and others are not expected to produce infallible results; instead, they are expected to adhere to certain procedures depending on the circumstances. Likewise, information providers have typically not been required to ensure 100% accuracy. This is especially true for those who publish for a mass-market, as a newspaper does. As the relationship between the parties gets closer, and the information provider has more reason to know of the relying party’s particular needs and is compensated accordingly, the obligations regarding the provision of information increase.

A fourth type of warranty, a warranty of title and against infringement (UCC § 2-312), could theoretically apply to the extent that the goods that the Identity Provider is providing have intellectual property attributes; because the possibility of this seems remote, we do not address it in this memorandum. In any case, such warranties can be disclaimed under UCC § 2-312(2), which requires either specific language or certain circumstances that put the buyer on notice.

See, UCC Section 2-318.
1.2.6. **Identity Theft Laws**

[making false statements to get a credential may also violate identity theft laws and/or fraud laws – Need research on impact of identity theft laws]

1.3. **Law Governing the Privacy of Identity Information**

General privacy and data security laws, among others, are a key component of the identity system Legal Framework, and also have a big impact on all identity system transactions.

By its nature, identity management typically involves the collection (by an Identity Provider or its agents) and disclosure (to a Relying Party) of personal information about a Subject.\(^\text{25}\) Thus, privacy and other laws and regulations governing the collection, use, processing, transfer and storage of the personal data will have a major impact on identity management activities. While such privacy laws were presumably not written for the purpose of regulating identity systems, they quite obviously have a direct impact on such activities.

In the U.S., privacy laws are limited in their scope and applicability, and may not affect all identity management activities. U.S. privacy laws generally apply only to certain sectors (e.g., financial sector, healthcare sector, video rental sector, federal government sector, etc.), certain types of data (e.g., Social Security numbers, credit card numbers, driver’s license numbers, etc.), or certain types of activities or events (e.g., breach of data security, rental of videos, communications of SSN over the Internet, etc.). Thus, federal and state privacy laws in the U.S. may be broken into the following categories:

- **Data-Specific Laws:** Laws regulating conduct with respect to specific types of personal data, regardless of the entity that possesses the data (e.g., laws governing social security numbers, credit card data, drivers license data);
- **Entity-Specific Laws:** Laws regulating the entity that possesses the personal data (e.g., healthcare entities, financial entities); and
- **Activity-Specific Laws:** Laws that govern certain types of activities (e.g., video rental, security breach of personal data, transmission of personal data over the Internet, or via wireless transmission).

By contrast, many countries have enacted omnibus privacy legislation that regulates the collection, processing, use, transfer, storage, and destruction of all personal data in all cases. The best example of this is the European Union member country privacy laws that, guided by the EU Data Protection Directive, regulate almost all processing of personal data, regardless of purpose, sector, data element, or activity. The Data Protection Directive (95/46/EC) formulates the basic principles and rights of data subjects with respect to the processing of personal data about them, and thus will be a key compliance requirement for identity system. In addition, the EU Electronic Signatures Directive (1999/93/EC) mandates that member states regulate the

\(^{25}\) Except where the Subject is not a human being – e.g., where the Subject is a corporation, device, software application, etc.
collection of personal data about Subjects by certain Identity Providers (called certification service providers). 26 And transfer of that data across country borders, whether for identification or identity assertion purposes, will also raise issues under the EU Data Protection Directive and implementing country laws. 27

The use of personal data in an identity system governed by such laws will be subject to such regulation. Fundamental structural differences between jurisdictions such as these make it more difficult to design, develop and deploy identity systems at internet scale. The System Rules of those identity systems that can best accommodate the data privacy rules of the greatest number of the most populous jurisdictions will enjoy the broadest and most rapid adoption across internet based systems.

1.4. Law Governing the Security of Identity Information and Processes

Many laws and regulations impose on companies an obligation to protect the security of personal information and other data in their possession. Although not written specifically with identity management in mind, such laws will undoubtedly apply to identity systems as well.

In most countries, privacy laws include an obligation to provide security for personal data. In the U.S., there is typically no single law, statute, or regulation that governs all of a company’s obligations to provide security for its information. Corporate legal obligations to implement security measures are set forth in an ever-expanding patchwork of state, federal, and international laws, regulations, and enforcement actions, as well as common law duties, contractual commitments, and other express and implied obligations to provide “reasonable” or “appropriate” security for corporate data. 28

The nature of the obligation to provide security for personal data is often simply stated in the law as an obligation to provide “reasonable” or “appropriate” security designed to achieve certain objectives. In some cases, statutes and regulations define those objectives in terms of positive results to be achieved, such as ensuring the availability of systems and information, controlling access to systems and information, and ensuring the confidentiality, integrity, authenticity of information 29 In other cases, they define those objectives in terms of the harms to


27 For a general analysis of the application of EU privacy law to identity management activities, see GINI, Legal Provisions for Deploying INDI Services” (October 5, 2011); available at http://www.gini-sa.eu/images/stories/2011.11.06_GINI_D3.1_Legal%20Provisions%20for%20Deploying%20INDI%20Services_FINAL.pdf.

28 See Appendix for a compilation of some of the key laws and regulations governing information security.

29 See, e.g., in the U.S., FISMA, 44 U.S.C. Section 3542(b)(1); GLB Security Regulations (OCC), 12 C.F.R. Part 30 Appendix B, Part II.B; HIPAA Security Regulations, 45 C.F.R. Section 164.306(a)(1); Microsoft Consent Decree at II, p. 4; in other countries, Argentina Act, Section 9(2); Estonia Act, Section 19(1); Italy Act, Annex B, Section 19.4; Liechtenstein Ordinance, Article 9.
be avoided – e.g., to protect systems and information against unauthorized access, use, disclosure or transfer, modification or alteration, processing, and accidental loss or destruction.\textsuperscript{30}

Unfortunately, laws and regulations rarely specify what specific security measures a business should implement to satisfy its legal obligations.\textsuperscript{31} This is because they typically view security as a relative concept. That view is evident from the fact that most laws and regulations simply require that the security be “reasonable,” “appropriate,” “suitable,” “necessary,” or “adequate.”

In Europe, for example, the Data Protection Directive requires the controllers of personal data to:

\[
\text{implement } \textit{appropriate} \text{ technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.}\textsuperscript{32}
\]

Thus, country implementations of the EU Data Protection Directive generally require the use of security measures that are \textit{appropriate} to protect the personal data\textsuperscript{33} or that are \textit{necessary} to protect the personal data\textsuperscript{34}.

Most other countries also use the \textit{appropriate} standard in their security laws,\textsuperscript{35} although some use other variations, such as requiring security measures \textit{reasonable under the}
circumstances, \textsuperscript{36} requiring \textit{useful precautions}, \textsuperscript{37} requiring \textit{all practical steps}, \textsuperscript{38} and requiring \textit{necessary and proper measures}. \textsuperscript{39}

In the U.S., the Privacy Protection Act of 1974 \textsuperscript{40} requires government agencies that maintain a system of records about an individual to:

- establish \textit{appropriate} administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; \textsuperscript{41}

Other laws applicable to the private sector take a similar approach. HIPAA requires \textit{“reasonable and appropriate”} security. \textsuperscript{42} The GLB Security Regulations require financial institutions to \textit{“implement a comprehensive written information security program that includes administrative, technical, and physical safeguards \textit{appropriate} to the size and complexity of the bank and the nature and scope of its activities.”} \textsuperscript{43} And many of the state personal information security laws in the U.S. generally require \textit{“reasonable security procedures and practices.”} \textsuperscript{44}

By adopting this approach, the laws recognize that the choice of security measures and technology can (and should) vary depending on the situation. Thus, most laws do not require companies to implement any specific security controls (such as a firewall), nor do they specify any safe harbours (e.g., if you implement a firewall you will be compliant). But security laws often do require companies to address certain \textit{categories} of security controls \textsuperscript{45} (such as access control), while leaving to the company the decision as to whether using a specific control (e.g., a firewall) will provide adequate security to address that control category.

\textsuperscript{35} See, e.g., Albania Act, Article 9; Bahamas Act, Article 6.1(d); Canada Act, Schedule 1, Section 4.7 Principle 7; Isle of Man Act, Schedule 1 Articles 17 and 21; Malta Act, Article 26; Mauritius Act, Article 27(1); Philippines Act, Article 8.1; Singapore Model Guidelines, Article 4.7 Principle 7; United Arab Emirates Act, Article 15(1).

\textsuperscript{36} Australia Act, Schedule 3, Section 4.1; Russia Act, Section 19(1).

\textsuperscript{37} France Act, Article 34.

\textsuperscript{38} Hong Kong Act, Principle 4.

\textsuperscript{39} Japan Act, Article 20.

\textsuperscript{40} 5 U.S.C. Sec. 552a. This statute applies only to government agencies.

\textsuperscript{41} 5 U.S.C. § 552a (d)(10) (emphasis added).

\textsuperscript{42} 42 U.S.C. 1320d-2(d)(2).


\textsuperscript{44} See, e.g., Cal. Civil Code § 1798.81.5(b).

\textsuperscript{45} See Chapter 6.
Although the law views security as a relative concept, and provides businesses with little or no specific guidance as to what is required for legal compliance, developments over the past few years suggest that a definition of the legal standard for “reasonable” security is clearly emerging. That standard rejects requirements for specific one-size-fits-all security measures (such as firewalls, passwords, encryption, or the like), and instead adopts a fact-specific approach to corporate security obligations that requires a “process” applied to the unique facts of each case. As noted in one opinion:

The reasonableness standard . . . is . . . not technically or operationally prescriptive. It does not specify particular technologies or procedures that must be used to protect personal information. The reasonableness standard recognizes that, because situations vary, the measures needed to protect personal information vary. It also accommodates technological changes and the challenges and solutions that they bring to bear on, and offer for, personal information security.  

Thus, rather than requiring companies to implement specific security measures, the legal standard requires companies to engage in an ongoing and repetitive process. Sometimes referred to a comprehensive written information security program, the process involves assessing the specific risks a company faces, identifying and implementing appropriate security controls responsive to those risks, verifying that they are effectively implemented, and ensuring that they are continually updated in response to new developments. The results of that process, rather than the text of any specific law or regulation, will determine the specific security controls a company must implement to be legally compliant.

As a consequence, the presence or absence of specific security measures says little about the status of a company’s legal compliance with its information security obligations. Because armed guards at the front of a building do not protect against hackers accessing information through the Internet, and because firewalls designed to stop hackers do not protect against dishonest employees with authorized access, the law puts its focus on implementing those security measures that respond to the specific threats a business faces. It recognizes that there are a variety of different appropriate security measures responsive to specific threats, and recognizes that threats (and appropriate responsive security measures) vary from business to business, and are constantly changing.

Based on a review of available security laws, regulations, court decisions, and consent decrees, the essence of the legally-required process-oriented approach to security compliance

---


becomes clear. In fact, while some laws contain much more detail than others, what emerges is an amazing consistency among most security statutes and regulations.

At its essence, the global legal standard for information security requires companies to implement a comprehensive (and written) information security program whereby the company:

- Identifies its information and system assets;
- Conducts periodic risk assessments to identify the specific threats to those assets the company faces, its vulnerabilities to those threats, and the harm that would result if the threats materialize;
- Selects and implements appropriate security controls to manage and control the risks identified;
- Monitors and tests the program to ensure that it is effective;
- Continually reviews and adjusts the program in light of ongoing changes, including obtaining regular independent audits and reporting where appropriate; and
- Oversees third party service provider arrangements.

A key aspect of this process is recognition that it is never completed. It is ongoing, and must be continually reviewed, revised, and updated.

1.5. **Law Governing Use of Public Sector Information**

In many cases, governments provide an authoritative source of identity attribute information about individuals and legal entities. This includes, for example, information relating to birth certificates, driver’s licenses, passports, criminal records, incorporation, payment of real estate taxes, franchise fees, and the like.

Such data is often considered to be highly trustworthy, as evidenced by common identity proofing requirements for one or more government-issued identity documents. Leveraging such data could therefore enhance the credibility and trustworthiness of the identity credentials used within an identity system.

Access to, and/or use of this information, however, is often regulated. In the U.S., for example, many state laws restrict the use of *[driver’s license records? Other? Describe]*.

In the EU, the Directive on the re-use of public sector information (2003/98/EC) targets the information industry creating information products and services based on bulk data from the public sector. And it creates a number of legal barriers and gaps towards the large-scale use of data maintained by public sector bodies in the context of identity services.48

1.6. Law Governing Intellectual Property Rights

[Discuss re whether to delete this section or keep it. If retained, consider scope – e.g.,
the different ideas around IP in credentials and the information they embody;
apropriate rules and roles regarding use of software licenses; etc.]

Intellectual property is a set of legally-recognized rights in intangible subject matter such as inventions, works of authorship, and trademarks. These rights include patents, copyrights, trade secrets, and trademarks and related rights arising under unfair competition law and privacy. Activities of an IdM participant that violate intellectual property rights of another party are said to infringe the other party’s rights. Depending on the right infringed, remedies for infringement may include damages, profits, punitive damages, attorneys’ fees and injunctions against further infringement.

Activities of a federated identity system participant that violate intellectual property rights of another party are said to infringe upon, or misappropriate, the other party’s rights. Depending on the right infringed or misappropriated, remedies may include damages, profits, punitive damages, attorneys’ fees and injunctions against further infringement.

Intellectual property law is, of course, important to the technology and processes used in various identity system implementations. The software, technical processes, and other technology used, for example, may be subject to patent or copyright protection. But that is beyond the scope of this Report. The focus here is on the impact of intellectual property laws on the direct activities of the participants.

1.6.1. Ownership Issues

[Should we consider who OWNS the credential and/or authenticator? The credential,
the authenticator and the data that comprise them are not the subject of traditional IP law. Is it
owned by the IDP? Is it owned by the subject? Can the subject transfer it from one IDP to
another? The IDP can presumably revoke the credential, does the subject have rights in this
case? Is there a difference if the credential was revoked because the subject failed to meet its
obligations vs. the credential being revoked in spite of the subject meeting its obligations?]

1.6.2. Patent Law

Patents may cover technology or business processes used by the Identity Provider and/or
the Relying Party, including software, encryption, and security procedures.

1.6.3. Copyright Law

Copyright protects original works of authorship fixed in a tangible medium of expression. Copyrightable subject matter includes text, photographs, drawings and computer code. Identity Providers and the Relying Parties deal with many copyrightable works, including software and documentation, and potentially the format and content of a credential.
1.6.4. **Trademark and Trustmark Law**

Trademarks are words, symbols or other devices used to distinguish the goods or services of one person from those of another. Everyday examples include “Ford” for automobiles and “IBM” for computers. The owner of a trademark has the exclusive right to use the mark in a particular market on particular kinds of goods or services. A federal statute known as the Lanham Act provides remedies to trademark owners for infringement of their rights. These remedies include damages, disgorgement of the infringer’s profits, and injunctive relief.

One potential concern that has been raised in discussions to date is the question of IdP liability under the Lanham Act to third parties whose marks have been misappropriated in IdP credentials issued at the request of impostors. Such trademark liability, if applicable, does not require the IdP to have acted negligently or with bad intent. Once the credential is issued containing the trademark, liability may arise. However, the Lanham Act provides an “innocent infringer” defense. It is not clear whether this defense would be available to an Identity Provider, however. Even if available, the defense requires the Identity Provider to have acted objectively reasonable in determining that the subject of the credential was authorized to use the mark at issue. [verify]

1.7. *[Other Law??]*

*[What is missing?]*

*[Perhaps add section on UETA & E-SIGN, or the Computer Fraud and Abuse Act?]*

2. **Law that Specifically Regulates Identity Management Activities**

Some existing laws expressly regulate one or more elements of an identity system and/or the identity management process.

2.1. **Laws Focused on a Duty to Identify**

Many laws and regulations, both in the U.S. and internationally, require identification as a component element, particularly in an electronic environment.

For example, the UN Convention on the Use of Electronic Communications in International Contracts expressly requires identity as a component of a legally binding electronic signature. Specifically, where a law requires that a communication or a contract should be signed by a party, the UN Convention provides that the signature requirement is satisfied if a method is used to identify the party and to indicate that party’s intention in respect of the information contained in the electronic communication.49 Because the UN Convention deals with remote electronic communications, the requirement to “identify the party” is, in reality, both an identification and an authentication problem. That is, it requires evidence of “who” the party

---

49 UN Convention at Article 9(3)
is (e.g., a name, affiliation), as well as evidence that such party is actually associated with the transaction.

The general law of evidence also imposes legal requirements to identify and authenticate. [Is this true in all countries??] A good example is a U.S. federal court decision in a case involving the enforceability of an electronic signature. While the court agreed that (under U.S. law) an electronic signature itself did not need to identify the person signing, it held that the signature would be considered valid “only if [the proponent] could reasonably identify the person who made them.” In another case also involving the enforceability of an electronic signature, the court refused to attribute an electronic signature to the plaintiff because the authentication process could be easily circumvented, raising legitimate doubts as to who actually signed the electronic record.

Some laws expressly impose a duty to identify. For example, the [Financial industry KYC requirements].

Other laws regulate the identity proofing process. For example, the [Arizona and Texas laws restrict the collection of biometric information] [state notary laws regulate what ID a notary may rely upon].

Other laws regulate the improper use of identifying information. See, for example, the [Identity theft laws].

Other laws regulate misuse of credentials – e.g., password theft.

[Other laws ??]

2.2. Laws Focused on a Duty to Authenticate

Similarly, other existing laws in the U.S. and internationally regulate one or more elements of authentication. Some impose on businesses a duty to authenticate the persons with whom they deal remotely, and others regulate aspects of the authentication process.

One prominent sector-specific example is the requirements of the U.S. banking regulators for authentication in online banking activities. Those requirements are set forth in a guidance document stating that “Financial institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using

51 Id. At *25 (emphasis added).
those products and services.”

Expanding on the rationale for this requirement, the regulators point out that:

An effective authentication system is necessary for compliance with requirements to safeguard customer information, to prevent money laundering and terrorist financing, to reduce fraud, to inhibit identity theft, and to promote the legal enforceability of their electronic agreements and transactions. The risks of doing business with unauthorized or incorrectly identified persons in an Internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements.

Other countries, such as Singapore, have also adopted similar requirements.

In addition, many laws and regulations that impose on a company a duty to provide reasonable security for its data typically include (expressly or implied) an obligation to properly authenticate persons seeking to access its data, networks or services. Examples of the express duty to authenticate under U.S. laws include:

- The Gramm-Leach-Bliley security regulations, which require covered financial institutions to ______________________;
- the HIPAA security regulations, which require covered entities to “implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed;”
- state information security laws, such as Massachusetts, which require the use of “secure user authentication protocols” and “secure access control measures,” and
- __________________________________

---

53 FFIEC Guidance, at p. 1. Other countries, such as Singapore, have also adopted similar requirements. Monetary Authority of Singapore, Circular No. SRD TR 02/2005, 25 November 2005.

54 “The Interagency Guidelines Establishing Information Security Standards that implement section 501(b) of the Gramm–Leach–Bliley Act, 15 USC 6801, require banks and savings associations to safeguard the information of persons who obtain or have obtained a financial product or service to be used primarily for personal, family or household purposes, with whom the institution has a continuing relationship. Credit unions are Subject to a similar rule.” FFIEC Guidance, at fn. 3.

55 “The regulations implementing section 326 of the USA PATRIOT Act, 31 USC § 5318(l), require banks, savings associations and credit unions to verify the identity of customers opening new accounts. See 31 CFR 103.121; 12 CFR 21.21 (OCC); 12 CFR 563.177 (OTS); 12 CFR 326.8 (FDIC); 12 CFR 208.63 (state member banks), 12 CFR 211.5(m) (Edge or agreement corporation or any branch or subsidiary thereof), 12 CFR 211.24(j) (uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States (FRB); and 12 CFR Part 748.2 (NCUA).” FFIEC Guidance, at fn. 4.

56 FFIEC Guidance, at p. 2.


59 HIPAA Security Regulations, 45 C.F.R. § 164.312(d).
California, which requires “reasonable security procedures and practices . . . to protect the personal information from unauthorized access . . . “; 60

- the FTC Identity Theft Red Flags Rules, which require most financial institutions and creditors in all sectors to develop and implement a written Identity Theft Prevention Program that includes reasonable policies and procedures for detecting, preventing, and mitigating identity theft in connection with existing accounts or the opening of new accounts; 61
- the FCC Order addressing the problem of pretexting, which imposes specific authentication requirements on telephone and wireless carriers to protect personal telephone records from unauthorized disclosure; 62
- the Homeland Security Act, which requires “utilizing digital credentials to assure the identity of users and validate their access,” and “protecting information and information systems from unauthorized access;” 63
- Homeland Security Presidential Directive 12, which mandates the development of a Federal standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees), and requires the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems; 64

Numerous data protection laws in other countries that also impose similar requirements. 65

Related to the general obligation to authenticate is the express obligation in some laws and regulations to utilize access controls to prevent unauthorized persons from gaining access to systems and data, and appropriately limit and control the scope of access granted to any authorized person. 66 This includes requirements to control access to information systems and

---

60 See, e.g., Cal. Civil Code § 1798.81.5(b); Mass., Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17.04.


63 Homeland Security Act of 2002 § 1001(b), amending 44 U.S.C. § 3532(b)(1)(D), and § 301(b)(1) amending 44 U.S.C. § 3542(b)(1) (“‘information security’ means protecting information and information systems from unauthorized access, . . . .”)


65 See, e.g., Italy, Personal Data Protection Code, Section 34(a) and (b) and Annex B, Sections 1 - 13; Poland, Regulation of April 29, 2004, Section § 5.2 and Attachment A (Basic Security Measures) § II.2; Spain, Royal Decree 1720/2007, Articles 93 and 98 (Basic-level and medium-level security measures);

66 See e.g., ISO 27002, Section 11 (“Access Control”) at pp. 60-76; NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems (February 2005) at pp. 40-47 (“Access Control”)
data, or that measures be taken to prevent unauthorized persons from gaining access to the information systems where personal data are processed or used.

In addition, laws and regulations often require companies to implement security measures and procedures to establish an appropriate level of authorization for persons entitled to access the personal data. This includes measures and procedures to ensure that personnel will only have access to the data and resources they need to know to perform their duties, and that they are only able to access the data within the scope and to the extent covered by their respective access permission. Procedures to prevent information systems from being used without (or in excess of) authorization are also required in some cases.

2.3. Laws Regulating Identity Systems or Participants

Several jurisdictions have statutes or regulations that expressly regulate at least some aspects of identity management activities. In some cases these laws address identity management in the general sense, whereas in other cases they are focused on specific technical implementations (typically PKI systems).

Examples of such laws include the digital signature laws enacted in Utah, Washington, Missouri, and Minnesota in the U.S., and similar laws enacted in Germany, Italy, Malaysia, Colombia, and other countries. These laws generally regulate PKI-based systems for the issuance, use, and revocation of digital certificates, including licensing of certification authorities.

Other laws take a more technology-neutral approach to the regulation of identity management, although they are typically interpreted as applying to PKI systems. These include the EU Electronic Signatures Directive, which mandates that member states regulate the collection of personal data about Subjects by certain Identity Providers (called certification authorities).

---

67 See e.g., Estonia Act, Section 19(2)(2); Poland – Ordinance, Attachment A (Basic Security Measures) § II.1
68 See e.g., German Federal Data Protection Act, Annex (to the first sentence of Section 9 of this Act), Section 1; Italy Act, Section 34(c) and Annex B, Sections 1 – 13; Portugal Act, Article 15(1)(d)
69 Belgium Act, Art. 16(2)(2); Estonia Act, Sections 19(2)(2) and 19(2)(4); German Federal Data Protection Act, Annex (to the first sentence of Section 9 of this Act), Section 1; Italy Act, Section 34(c) and Annex B, Sections 12 and 13; Poland – Ordinance, Section § 5.1; Slovakia Act, Section 16(6)(b) and (c); Spain Royal Decree 1720/2007, Article 91 (Basic-level security measures)
70 German Federal Data Protection Act, Annex (to the first sentence of Section 9 of this Act), Section 2; Italy Act, Section 34 and Annex B, Sections 1 – 13; Portugal Act, Article 15(1)(e); Spain Royal Decree 1720/2007, Article 91 (Basic-level security measures).
72 See, generally, Stephen Mason, ELECTRONIC SIGNATURES IN LAW, 2d Ed. (Tottel Publishing, 2007)
73 See, e.g., EU Electronic Signatures Directive, Articles 6 – 8 and Annexes I and II.
service providers), and regulates the issuance of credentials. Similarly, the UNCITRAL Model Law on Electronic Signatures (which has now been adopted in approximately 100 countries) sets forth rules for the issuance and use of the identity credentials required for the creation of certain electronic signatures.

[Other laws? What is missing??]

3. **Legal Barriers Created by Existing Laws and Regulations**

Existing laws and regulations pose several basic problems for the operation of an identity system –

- There are some key identity management issues that existing laws and regulations simply do not directly address, leaving legal resolution of such issues uncertain;
- There are some issues that existing laws and regulations may address, but the fact of their application to such issues, or the manner of their application, is unclear, uncertain, or ambiguous, leaving identity system participants with a great deal of legal uncertainty;
- There are some key issues that existing laws and regulations may address in a manner that is contrary to the intentions of the participants or in a manner that constitutes a barrier to the operation of the identity system;
- There are some key issues on which the application of existing laws and regulations varies considerably across jurisdictions, often in an inconsistent manner; and
- Some existing laws and regulations cannot be modified by contract.

As a consequence, existing laws and regulations may create barriers to the adoption of efficient, interoperable, and acceptable identity systems. These challenges from existing laws and regulations can be summarized as follows:

3.1. **Law Does Not Address All Relevant Issues**

Because most existing law of relevance to an identity eco-system was not written from the perspective of an identity system, it is likely inadequate in the manner in which it addresses or regulates identity activities. Many novel issues raised by identity management processes are simply not addressed by existing law.

---


For example, existing law is silent with regard to the liability of a subject for failing to protect his or her password or private key, the duty of care an identity proofer must meet when evaluating the authenticity of identity proofing documents, or the scope of any disclosure duty owed by an identity provider to a data subject. Judicial decisions may be able to fill some of these gaps over time, but only if cases squarely raising these issues are litigated. Contractual governance systems may reduce uncertainty for stakeholders that have formally agreed to be bound by them, but contractual system rules generally cannot be used to decide the rights and obligations of parties that have not explicitly agreed to be bound by them.

As a result of uncertain application of relevant existing laws and regulations, and gaps in existing laws and regulations with regard to fundamental issues, existing laws and regulations constitute a potentially major barrier to the widespread adoption of identity systems.

3.2. Legal Uncertainty / Ambiguity

As noted above, many of the existing laws and regulations of relevance to an identity system were not written with the concept of an identity system in mind. As a result, their application to identity management processes may be uncertain or ambiguous, giving rise to more than one plausible interpretation. Thus, the manner or extent to which such laws and regulations will apply to an identity system is often unclear. This will, of course, make the process much more difficult, as it will often not be clear how existing laws and regulations will impact a specific issue or proposed approach in an identity system.

As a result of uncertainty surrounding the application of existing law, and gaps in existing law, parties entering into identity transactions may be unable to assess and manage the risks they assume by so doing. Parties may decide not to join identity systems whenever they find that they cannot assess accurately and manage effectively the risks associated with participation in those systems.

3.3. Inappropriate Results

Even where the application of existing laws and regulations may be reasonably clear, it may produce a counterproductive allocation of rights and responsibilities among the parties in an identity system.

In many cases, existing law may actually hinder or restrict the operation of an identity system, or alternatively cause what the participants would regard as inappropriate results.

[Need examples. Consider adding discussion of seal of approval liability. For a federation operator, this could be a concern.]

3.4. Jurisdictional Variations and Conflicts

The foregoing legal challenges to participating in an Identity System are magnified significantly when such systems cross jurisdictional borders. In such cases, the foregoing challenges are compounded by the fact that existing laws, as well as rules regarding contractual structures, vary (often significantly) between jurisdictions. The problem of identifying and
complying with existing laws and regulations is greatly magnified as the number of relevant jurisdictions increases.

Concepts of regulatory and judicial jurisdiction rooted in territorial sovereignty do not work well when applied to online activities and identity management is no exception. Existing laws applicable to identity systems vary significantly across jurisdictions. For example, the U.S. has sectoral information privacy laws that are very strict in some economic sectors, but non-existent in others, while many other countries have broad information privacy laws that apply to virtually all economic activity. Conflicting substantive laws and claims of jurisdiction may even result in a party being mandated to act in one jurisdiction and forbidden to act in another with regard to a specific activity within an identity system. For example, broad civil discovery rules in the U.S. may require an identity provider to turn personal information over to another party in a lawsuit, while EU data protection laws may prohibit the same information from being turned over. [Insert Examples]

While identity systems must comply with applicable existing law, achieving this goal is made problematic where applicable law comes from different jurisdictions, and such laws differ, are inconsistent, and/or are in conflict.

3.5. Inability to Modify Law by Contract

Many contract and commercial law doctrines merely establish “default rules” that apply in the absence of express choice by the parties. In such cases, parties are free to modify default rules, and fill-in the blanks by contract. In other cases, however, parties to an identity system may not be permitted to “opt out” of statutory default rules. In many cases, mandatory rules of law cannot be discarded by mere agreement of the parties, because they serve other useful purposes, such as the protection of third parties.

Where portions of existing law in one or more jurisdictions cannot be modified by contract (e.g., certain consumer protection laws), compliance may be the only option. Thus, identifying such laws will be critical for the development of the Legal Rules.

In such cases, the Legal Rules must either adopt an approach that complies with all such laws in all applicable jurisdictions, or alternatively alter the System Rules so as to avoid the need for compliance

3.6. Other Legal Factors

Several other factors may also affect the way in which existing laws impacts an identity system. These are factors which affect the way that existing laws and regulations will be applied, and include the following:

3.6.1. Nature of the Participant

The rights and obligations of parties to identity transactions may vary depending on the status of the participants. For example, many legal systems may hold merchants acting within the scope of their trade to a higher standard of care than the average party, while holding
consumers to a lower standard of care. Government entities may be held to a different standard that an equivalent private entity. Whether a party’s reliance on information contained in an identity assurance is “reasonable” may depend on the sophistication of the party, and the knowledge of other parties of that level of sophistication. And of course, many laws provide special forms of protection for consumers.

Thus, any contract-based System Rules must also recognize legal distinctions among participants arising under existing laws and regulations. These include, for example, special rules for consumers and government agencies that need to be taken into account.

3.6.2. Nature of the Information

Whether or not existing laws and regulations apply to identity systems may turn on the nature of the information being exchanged among participants in the system. For example, under EU data protection law, a participant in an identity system is prohibited from even asking for certain forms of “sensitive data” unless an exception applies. In a similar fashion, US law strictly regulates the transfer of certain types of information such as health or financial information, while allowing most forms of personal information to be transferred freely without the consent of the subject.

3.6.3. Nature of the Use

Another factor that will affect the interpretation and application of existing law within identity systems is the nature of the transaction in which an identity assertion or credential is used. For example, identity management for high value financial transactions may be strictly regulated by banking or commercial law, while identity systems within social commerce may be completely unregulated. [Consider what happens if a credential intended for one use is repurposed for another use]

3.6.4. Nature of the Harm

Parties to identity systems may not be permitted to modify or limit their obligation to compensate victims of certain forms of harm. For example, parties are generally never allowed to disclaim by contract liability for death or bodily injury caused by their negligence. If an identity system is used to control access to health care records, and reliance on inaccurate information negligently provided in an identity assertion is the proximate cause of death or bodily injury to a subject, the identity provider may not be protected from liability by a contractual governance mechanism among the parties.

4. Addressing the Problems of Existing Law Through Binding System Rules

Short of enacting comprehensive legislation (and attempting to harmonize it across all relevant jurisdictions), the primary approach to the problems with the existing laws and regulations noted above is to adopt contract-based System Rules that include what the participants view as appropriate Legal Rules.
Major existing identity systems have adopted this approach. This include SAFE-BioPharma, TSCP, IdenTrust, FICAM, ________________ and _____.

To the extent possible (and permissible) this involves modifying by contract the existing laws and regulations in all relevant jurisdictions so that a single consistent rule applies everywhere. [Some identity systems claim to do this. Perhaps the credit card brands do so as well??]. Where this is not possible the System Rules will need to ensure compliance with applicable local law. This requires:

- Developing contract-based System Rules that harmonize the cross-jurisdictional inconsistencies in existing laws and regulations; and

- Developing acceptable contract-based System Rules that address all the required issues for the identity system while at the same time complying with (or modifying by contract) existing applicable law in all relevant jurisdictions so that, to the extent necessary, the identity system is governed by a uniform set of rules.