Big Data and Privacy
By Bruce Wright
Privacy is being challenged by the burgeoning use of Big Data. The term “Big Data” has multiple definitions. This paper discusses the challenges to privacy posed by Big Data viewed as an Information Technology process that collects and parses huge sets of data through the conduct of analytical experiments for the purpose of extracting useful information. In particular, risks around Big Data are analyzed through the lens of FTC reports, and FTC and HHS enforcement actions. Read more

By Timothy S. Reiniger, Jeff Nigriny, and Kyle Matthew Oliver
In the physical world, we typically rely on government entities and employers to manage the identity credentialing process. DMVs, Passport offices, and human resource departments are the norm. The digital world, though, is serviced almost exclusively through commercial entities, often at the behest of government entities that would see the privatization of the Internet upheld. This paper explores the practical effect of Virginia’s liability safe harbor approach on Read more

Evolving Issues for Healthcare IT Contracting
By Alan L. Friel
The emergence of mega-suite vendors, more use of the cloud, increases in data breach frequency and cost and big data privacy impacts make healthcare IT (HIT) vendor arrangements more complex, and solid agreements with HIT vendors, more important than ever. Addressing key legal and business issues during the request for proposal (RFP) and contracting process reduce healthcare providers’ risks and help minimize expensive change orders. Read more

Analysis of Freedom of Information for its Effect on Society, Considering the Arab Spring
By Paul D. Callister and Kimberlee C. Everson
2011, the year of the Arab Spring, presents a unique opportunity to look back and study how the relative freedom and development of information environments affect stability in nations throughout the Middle East and world. Such study raises interesting questions about whether freedom of information and speech are ultimately stabilizing influences for society in terms of loyalty, violence and political unrest—questions all the more important as societies face the onslaught of Read more

Preserving Privilege: Important Steps Before, and During, Discovery to Maximize Protections and Minimize Costs
By Allen Kathir, Alexander Hastings, and Edward Rippey
Privilege protections encourage full and candid communication between legal counsel and clients. These communications plainly serve a valuable role—but, protecting privileged communications during discovery can become one of the most time consuming and expensive elements of large-scale e-discovery projects. And, in many respects, the emphasis on computer-assisted review and cost containment during first- and second-line document reviews has largely outpaced Read more

“Insider Threat” Cybersecurity and Privacy Best Practices
By Alan Charles Raul
Financial institutions have long been especially lucrative targets for insider attacks, but with the computerization of firm systems and assets, attacks can now be launched on a grander scale than ever before. Insider attacks on firms’ electronic systems can result in financial and intellectual property theft, damaged or destroyed assets, and firm-wide Read more
By Bruce Wright

Privacy is being challenged by the burgeoning use of Big Data. The term “Big Data” has multiple definitions. This paper discusses the challenges to privacy posed by Big Data viewed as an Information Technology process that collects and parses huge sets of data through the conduct of analytical experiments for the purpose of extracting useful information. In particular, risks around Big Data are analyzed through the lens of FTC reports, and FTC and HHS enforcement actions, viewed as being reflective of the challenges posed by the current business environment. The conclusion reached is that privacy in the Big Data environment can be enhanced by the use of currently available technology, combined with new legislation.

Big Data Defined

The first step in understanding the privacy problems posed by Big Data is to understand what Big Data is. Similar to the descriptions of the elephant given by the blind men in the well known parable of the elephant and the blind men, the definition of Big Data is imprecise. One definition of Big Data states:

“Big Data is often described as extremely large data sets that have grown beyond the ability to manage and analyze them with traditional data processing tools. ...The concept has evolved to include not only the size of the data set but also the processes involved in leveraging the data. Big Data has even become synonymous with other business concepts, such as business intelligence, analytics, and data mining.”

Another definition of Big Data states:

“Big Data is not a solution; it is not a market, not even a particular technology. Big Data is the datafication of everything—every activity in business, government, and even private life is now digitized and stored and can be analyzed. Our thoughts and feelings are captured in Twitter, Facebook, blogs, and status updates; our keystrokes and mouse movements are captured and analyzed; the smallest movements of jet engines and mobile phones in sensor logs, and even fast-changing activities in marketing and product design or stock trading activities every millisecond, are captured.”

For the purposes of this article, Big Data deals with collecting huge sets of data and manipulating that data through conduct of analytical experiments in the hope of extracting useful information. These characteristics of Big Data pose some unique problems for organizations, their Information Technology departments, and to the privacy of individuals. An understanding of how Big Data works is helpful in

1 Frank Ohlhorst, Big Data Analytics: Turning Big Data into Big Money, Chapter 1, (John Wiley & Sons 2013).
order to understand those problems.

**Hadoop - the Elephant**

Hadoop was created by the non-profit corporation Apache. Hadoop is one of the core products that Big Data is built around and is often synonymous with Big Data. Hadoop is software created “for distributed storage and distributed processing of very large data sets on computer clusters built from commodity hardware”, and was named after the toy elephant of a child of one its major developers. ³

Hadoop, along with other Apache products designed to work with Hadoop, is capable of rapidly processing massive amounts of data. It does this by splitting up a single large computer processing job into multiple component parts that can be processed on multiple computers, and the results then reassembled into a single result through use of MapReduce. Another name for this type of operation is massive parallel processing. Dramatic increases in information processing speed are one of the benefits of Hadoop. ⁴

Another benefit of Hadoop is that it can be used with both structured and unstructured data, also known as “raw data”. Structured data can be pictured as the databases that are repositories of information composed of table and rows. Similar to a phone book a structured database contains predefined characteristics, such as columns of street addresses and rows of client information such as name, address, and telephone number. SQL is the primary software language used to work with structured data. Unstructured data is information such as clickstream data, Facebook data, YouTube data, and blogs. NoSQL is the language used to work with unstructured data. Combining and quickly analyzing structured and unstructured data is an attractive concept for marketers and others. Big Data and Hadoop can facilitate new insight into the relationships between structured and unstructured data. For example,

“...a food company might suddenly ask, "Do the cooking videos we post to YouTube increase in-store sales?" With a raw data technology like Hadoop and NoSQLdb, the company doesn't have to build the model first. Instead, they bring in YouTube viewing and in-store sales data, plus customer demographics and profile data, and begin to experiment with it....Bringing these two worlds together accelerates a company's rise to the next level of best practice, creating competitive advantage and operational effectiveness. These two data worlds are not competing with one another—they are not two ways to do the same thing; they are each part of the way to do something entirely new. So they are complementary. From a data governance perspective, it creates a unique situation.”⁵

Data Governance

Broadly speaking, data governance means the implementation of safeguards that ensure data is used effectively and also that data is stored, used, and protected appropriately in a manner that complies with laws and regulations. The Oracle Big Data Handbook provides some guidelines. Those guidelines encompass a number of objectives including the following topics:

From an information lifecycle perspective data should be kept only as long as legally required, and legally and contractually allowed. Data should not be collected then kept in perpetuity. From a data quality perspective there should be safeguards in place that ensure the data is accurate. From a data security perspective data access should be limited to those that have a legitimate right to view the data and there should be security protections in place that ensure the data is protected from inappropriate viewing from both inside and outside the organization. 6

ISACA, (Information Systems Audit and Control Association), is an international organization of information technology governance professionals. ISACA states in its whitepaper Privacy and Big Data, that Information Technology auditors should ensure that

“Sufficient big data privacy governance exists, such as:

- Data anonymization/sanitization or de-identification
- Adequate, relevant, useful and current big data privacy policies, processes, procedures and supporting structures
- Senior management buy-in and evidence of continuous commitment
- Appropriate data destruction, comprehensive data management policy, clearly defined disposal ownership and accountability
- Compliance with legal and regulatory data requirements
- Continuous education and training of big data policies, processes and procedures.” 7

Ensuring that organizations meet ISACA’s suggested governance criteria would help to ensure that some the risks posed by Big Data are met.

6 Id. at Table 12-2.
The Unique Risks of Big Data

The unique character of Big Data is that it is a complex new technology that by definition utilizes massive amounts of structured and unstructured data. Those attributes heighten the risks associated with Big Data. The FTC has identified the following three broad risks around Big Data:

Security – Big Data by definition uses massive amounts of data, various forms of data, data that may not be masked to conceal who it relates to. These features combine to make security over Big Data a unique problem and a unique risk. If there is a data breach or other unauthorized access, it is by definition a massive breach or unauthorized access.

Sensitive Information – Because Big Data uses both structured and unstructured data, there is almost no limit on what information is analyzed in experiments. Data could contain health data or genetic data, or could contain any other type of sensitive data. Since both structured and unstructured data can be used in conducting Big Data analytical experiments, particular attention needs to be focused on who has access to the data, who has access to the experiment results, and how the data and experiment results will be handled now and in the future. Combined with the heightened security risk around Big Data, if there is a breach, that breach could contain massive amounts of sensitive information. This risk is compounded in that even if data is masked it sometimes can be re-associated with a specific person.

Discrimination and unethical data practices – Big Data analytics can result in discriminatory outcomes. Big Data might include the collection and use of individual’s data without disclosure of how the data is being collected and used.  

The Current Environment

The Federal Trade Commission (FTC) has emerged as one of the major protectors of consumer privacy in this fast moving Big Data environment. The U.S. Department of Health and Human Services (HHS) is also active in enforcing privacy requirements around the privacy of health information.

“The FTC uses a variety of tools to protect consumers’ privacy and personal information. The FTC’s principal tool is to bring enforcement actions to stop law violations and require companies to take affirmative steps to remediate the unlawful behavior. This includes, when appropriate, implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and provision of robust notice and choice mechanisms to consumers.”

---


Data Brokers are companies that assemble and sell, or share, consumer’s personal information. The FTC recently issued a report on Data Brokers. Some of the major findings detailed in the report follow:

1. Data Brokers collect consumer data from numerous sources, largely without consumers’ knowledge. Data Brokers collect data from commercial, government, and other publicly available sources.

2. The Data Broker industry is complex, with multiple layers of Data Brokers providing data to each other.

3. Data Brokers collect and store billions of data elements covering nearly every U.S. consumer: Data Brokers collect and store a vast amount of data on almost every U.S. household and commercial transaction.

4. Data Brokers combine and analyze data about consumers to make inferences about them, including potentially sensitive inferences.

5. Data Brokers combine online and offline data to market to consumers online.\(^\text{10}\)

A review of recent cases and commentary provides an overview of some of the challenges around maintaining privacy in an environment where there is a tension between privacy and profits, questionable business ethics practices, loss and theft of equipment, and unknowledgeable or untrained personnel involved in handling sensitive data on equipment requiring both technical proficiency and an understanding of the equipment’s vulnerabilities.

1. FTC and Spokeo –

Data Broker Spokeo violated the FCRA (Fair Credit Reporting Act) by providing consumer reports to businesses, recruiters, human resource departments, and others without meeting its obligations under the Act. Spokeo was fined $800,000 and entered a consent agreement to end its unlawful practices.\(^\text{11}\)

2. FTC and Instant Checkmate –

“Data broker Instant Checkmate, Inc. agreed to settle FTC charges that it violated the FCRA by providing reports about consumers to users such as prospective employers and landlords without taking reasonable steps to make sure that they were accurate, or without making sure their users had


a permissible reason to have them. The case imposes a $525,000 fine.”  

3. FTC and Infotrack Information Services –

“Data broker, Infotrack Information Services, Inc., agreed to settle FTC charges that it violated the FCRA by failing to provide adverse action notices to consumers, as well as by providing reports about consumers to prospective employers and landlords without taking reasonable steps to make sure that they were accurate. InfoTrack and its owner agreed to pay a $1 million fine.”

4. FTC and Goldenshores Technologies –

Contrary to its privacy policy and user agreement this business’ application product (commonly termed an “App”) collected location information from devices that used it, and transmitted that data to advertisers.

5. FTC and Jerk.com –

Using data mostly obtained from Facebook, a well known popular social networking company that, (not so well known), provides its user’s data to developers, Jerk allowed the posting of deleterious information to identifiable peoples profiles, including children, and the labeling of them as “jerk” while making it difficult to have the profile deleted. Jerk advertised that it would remove data, but made that difficult, requiring a $30 membership fee or a $25 contact fee to do so, and then often not removing the information after a fee was paid. The FTC issued a summary decision “that requires the company and Fanning to delete all personal and customer information collected during the operation of the now-defunct website within 30 days, and prohibits them from selling or disclosing any of that information. The order also prohibits them from misrepresenting the source of any content on a website, including personal information, and from misrepresenting the benefits of joining any service.”

6. FTC and WhatsApp -

The FTC also expects companies to perform the promises that they make to consumers in their privacy policies. Facebook purchased WhatsApp, a popular instant messaging application and shortly afterwards watered down the protections in the WhatsApp privacy policy for users that existed prior to the purchase. The FTC subsequently notified Facebook that the WhatsApp privacy policy still applied

---

13 Id.
and that Facebook would be bound by its terms.  

7. FTC and Accretive Health -

An employee’s laptop with data sensitive health and personal information, including patient names, dates of birth, billing information, diagnostic information, and Social Security numbers, of 23,000 patients was stolen from the employee’s car. Accretive also used real data in training sessions and did not always remove the data from the computers used after the training was complete. Accretive agreed to take steps to improve information system security and to have its information security assessed on a biennial basis assessed for 20 years.  

8. FTC and GMR Transcription -

The FTC reached a settlement with a transcription services company for not protecting the PII of consumers. Transcribed files containing sensitive information were indexed by a search engine and made available on the Internet. The information included notes from medical examinations of children and other highly sensitive medical information, such as information about psychiatric disorders, alcohol use, drug abuse, and pregnancy loss.  

9. HHS and Adult & Pediatric Dermatology, P.C. -

A settlement with a dermatology clinic regarding violations of the HIPAA Rules in regards to a thumb drive stolen from a workforce member’s vehicle, containing health information on about 2,200 patients. HHS found that the ePHI data were improperly released, the loss of data was not reported as required, and a required risk assessment was not done. HHS Required a fine of $150,000 implementation of a corrective action plan.  

10. HHS and WellPoint -

HHS fined WellPoint $1,700,000 because WellPoint did not adequately implement technology to verify that a person or entity seeking access to ePHI (electronic personal health information) maintained in its web-based application database was the one claimed and for over five months WellPoint impermissibly disclosed the ePHI, including the names, dates of birth, addresses, Social Security

---

Numbers, telephone numbers, and health information, of approximately 612,000 individuals whose ePHI was maintained in the web-based application database.  

11. HHS and Affinity Health -

Affinity Health was fined more than $1,215,000 because it disclosed health information of more than 344,000 people by not removing information from the hard drives of copiers before turning them over to a rental company.  

12. According to an FTC Commissioner, “…one firm, LeadsPlease.com, reportedly sells the names, mailing addresses, and medication lists of people with diseases like cancer or clinical depression. Another data broker, ALC Data, reportedly offers lists of consumers, their credit scores, and their specific ailments.”

These cases and commentary provide a lens through which to view Big Data in the environment in which it exists today. Billions of data elements of varying types are collected by Data Brokers without consumers knowledge. The data collected are bought and sold among brokers and businesses, and combined and analyzed to make inferences about individuals. These activities are taking place in organizations with varying levels of computer security control and IT sophistication at a time when security breaches are not unusual. It follows that a Big Data related release of a huge amount of sensitive data that can be easily paired to individuals is likely.

The FTC in its Data Broker report provided some suggestions for legislation directed towards protecting privacy in the Big Data environment:

- Legislation requiring data brokers to give consumers (1) access to their data and (2) the ability to opt out of having it shared for marketing purposes.

- Legislation to provide consumers with transparency when a company uses a risk mitigation product that limits a consumer’s ability to complete a transaction. These data brokers should in turn give consumers the right to access the information used and correct any erroneous information, as appropriate.

- Legislation requiring data brokers offering people search products to: (1) allow consumers to access their own information; (2) allow consumers to opt out of the use of this information; (3)

---

clearly disclose to consumers the data brokers’ sources of information, so that, if possible, the consumer can correct his or her information at the source; and (4) clearly disclose any limitations of the opt out, such as the fact that close matches of an individual’s name may continue to appear in search results.  

Additionally the FTC called on data brokers to implement best practice recommendations,

“...practice privacy by design, which includes considering privacy issues at every stage of product development. As part of privacy by design, data brokers should strive to assess their collection practices and, to the extent practical, collect only the data they need and properly dispose of the data as it becomes less useful. This is particularly important in light of companies’ increased ability to collect, aggregate, and match consumer data and to develop secondary uses for the data in ways that consumers could never have contemplated when they provided the information. Sound data collection and disposal practices also reinforce data security, as collecting and storing large amounts of data not only increases the risk of a data breach or other unauthorized access but also increases the potential harm that could be caused. ....Data brokers also should implement better measures to refrain from collecting information from children and teens, particularly in marketing products.”  

The FTC also recommended,

“...that data brokers take reasonable precautions to ensure that downstream users of their data do not use it for eligibility determinations or for unlawful discriminatory purposes. For example, while the data segment of “Smoker in Household” could be used to market a new air filter, a downstream entity also could use the segment to suggest that a person is a poor credit or insurance risk, or an unsuitable candidate for employment or admission to a university. This would be especially pernicious if the segment included a high concentration of minorities. Of course, the use of race, color, religion, and certain other categories to make credit, insurance, and employment decisions is already against the law, but data brokers should help ensure that the information does not unintentionally go to unscrupulous entities that would be likely to use it for unlawful discriminatory purposes. Similarly, data brokers should conduct due diligence to ensure that data that they intend for marketing or risk mitigation purposes is not used to deny consumers credit, insurance, employment, or the like.”

The FTC’s legislative recommendations if enacted will provide some transparency into Big Data collection and usage practices, and also provide people with some control over the uses of their data.


24 Id. at 55.

25 Id. at 56.
The FTC also mentioned privacy by design in its best practices recommendation. A privacy by design factor to enhance privacy in the Big Data world is disassociation.

**Disassociability - Data Anonymization and Data Encryption**

In addition to the FTC’s recommendations, problems such as hacking, equipment loss, and inadvertent release, can be ameliorated by anonymizing and encrypting data. Anonymization and encryption are methods for disassociation. According to a recent draft paper by the National Institute of Standards and Technology (NIST), disassociation is one of the objectives of privacy engineering. “Disassociability captures one of the essential elements of privacy-enhancing systems, that the system actively protects or “blinds” an individual’s identity or associated activities from unnecessary exposure.”  

The main arguments against anonymizing and encrypting data are that anonymization and encryption can be complex to perform, and that data encryption ultimately slows down system performance. Those arguments are becoming obsolete. Oracle is one major database system provider that has overcome those obstacles, and reports that it has done so at both the hardware and software levels. In a 2013 whitepaper Oracle provided high-level details of the problem and how Oracle can provide both data anonymization (through data redaction), and data encryption:

“As data exposed in applications continues to rapidly expand, enterprises must have strong controls in place to protect data no matter what devices or applications are used...... Oracle Advanced Security with Oracle Database 12c provides two critical preventive controls. Transparent Data Encryption encrypts data at rest to stop database bypass attacks from accessing sensitive information in storage. Data Redaction reduces exposure of sensitive information in applications by redacting database query results on-the-fly, according to defined policies. Together these two controls form the foundation of a multi-layered, defense-in-depth approach.”

Oracle accomplishes data encryption at both the software and hardware level. Speaking of Oracle’s Transparent Data Encryption (TDE) the whitepaper discusses performance characteristics:

“TDE’s cryptographic operations are extremely fast and well integrated with related Oracle Database features. TDE leverages CPU-based hardware cryptographic acceleration available in Intel® AES-NI and Oracle SPARC T4/T5 platforms to increase performance by up to 5x or more.”

---


28 *id.* at page 4.
Data anonymization may also be accomplished in Oracle through data redaction without affecting system performance:

“One important performance characteristic of Data Redaction is that it supports only data transformations with proven high performance. These are a subset of all the possible operations that could be used to transform data in non-production environments. This specific subset avoids long running and processor intensive operations.

Data Redaction also leverages performance optimizations of the Oracle Database that are only possible by being part of the database kernel. The implementation ensures that data transformations are fast in-memory computations. Policy information is cached in memory, and policy expressions are evaluated only once per execution, so there is no per row performance impact.” 29

The technology exists to efficiently anonymize and encrypt data without significantly slowing down system performance. Given the heightened risks around privacy in the Big Data environment organizations should consider the use of such technology when working with Big Data. The challenges to privacy in the Big Data environment can be met to a large extent by filling in the gaps in current law with new legislation as proposed by the FTC, by following the FTC’s suggested best practices, and by use of anonymization and encryption technology.

Bruce A. Wright Esq. is a Senior Risk Management and Compliance Consultant at Allstate Insurance Company in Northbrook Illinois. He received his B.A. and B.S. degrees from Michigan State University, his MBA in Information Technology and Management from the University of Texas at Dallas, and his J.D. from the John Marshall Law School in Chicago Illinois. He is a Certified Public Accountant, a Certified Information Systems Auditor, a Certified Internal Auditor, and a member of the Illinois Bar. He is also on the Board of Directors of the American Bi-Centennial Chapter of the Society of the Sons of the American Revolution. His avocations include genealogy and sailing on Lake Michigan.

29 Id. at page 9.

Timothy S. Reiniger, Jeff Nigriny, and Kyle Matthew Oliver

In the physical world, we typically rely on government entities and employers to manage the identity credentialing process. DMVs, Passport offices, and human resource departments are the norm. The digital world, though, is serviced almost exclusively through commercial entities, often at the behest of government entities that would see the privatization of the internet upheld. This paper explores the practical effect of Virginia’s liability safe harbor law approach on participant claims in both federated and user-centric identity management systems in the United States.¹ The law seeks to provide a common legal foundation for identity providers, identity trust frameworks, and the use of trustmarks as emerging approaches to addressing the risk of being held legally responsible for the losses incurred by others based on faulty third party assertions of identity.

In an open environment, identity trust framework providers and identity providers face an exorbitant amount of risk based on their central position.² They are not currently compensated for this risk, and it would be difficult to alter models to adequately address this through solely commercial means. As such, the system inadvertently incentivizes trust framework providers to push participating identity providers to lower assurance levels and regardless of their compliance capability – as a means of reducing the trust framework operator’s own risk exposure.

There are a number of common liability concerns that, prior to this law, have remained ill-defined and uncertain with respect to court treatment.³ Should identity providers have legal protection if they have complied with the defined standards and credentials are nonetheless issued or used incorrectly? What is the liability of an identity provider for an identity credential that is issued incorrectly when following the Commonwealth of Virginia approved standard or when in breach of the standard? Who has the liability when a relying party disseminates or provides access to valuable or protected data based on a false identity assertion?

¹ The text of the law is available at: http://lis.virginia.gov/cgi-bin/legp604.exe?151+ful+CHAP0483
³ See the draft Report of the ABA Identity Management Legal Issues Task Force (Part I), “Solving the Legal Challenges of Online Identity Management,” at 32 (“Thus, a key aspect of the liability risk is the uncertainty regarding the responsibility that attaches to any given act or failure to act by a participant in an identity system, particularly one that operates across multiple sectors and jurisdictions. This uncertainty only increases the liability risk and in many cases has dissuaded companies from participating in federated identity systems.”) available at: http://apps.americanbar.org/dch/committee.cfm?com=CL320041
In particular, usage of identity credentials across sectors and communities of interest, both public and private, presents challenges not shared by the current bilateral identity credential scenario, where both parties are bound by contract concerning the distribution of liability. Like the credit card industry, the federated identity credential has unlimited relying parties; but unlike the credit card industry, these relying parties have no direct contractual relationship with the identity providers to underpin liability risk allocations. In the absence of a contractual relationship or a statutory framework, the identity management marketplace is uncertain as to how courts will allocate liability.

The identity credential market has reached a point at which legal uncertainty is itself a barrier to potentially beneficial progress, and state government may be especially well-suited for resolving this kind of uncertainty. A safe harbor strategy using an identity trust framework approach is designed to reduce legal uncertainty but without imposing prescriptive requirements that would be hard to change in response to market changes and technology obsolescence.

I. Legislative Frameworks for Federated Identities: Electronic Identity Liability Protection for Identity Providers, Identity Trust Framework Providers, Identity Credential Holders, and Relying Parties

Federated identity management contemplates a system of user-centric control over the use and usage of identity credentials and identity attributes. Therefore, liability determinations are necessarily contextual according to: 1) legal control of the use of the identity credential and identity attributes for particular purposes, and 2) legal control over the usage of the identity credential, identity attributes, and resulting outcomes (i.e. data being accessed, collected, used, or disseminated).

A. Liability Risk Based on Use and Usage Control over the Identity Credential and Identity Attributes

1. Identity Credential and Attribute Use Control

The initial determining factor for risk allocation in the identity context is legal control over the use of the identity credential and identity attributes (i.e. regulated or permitted conduct). For what type of purpose or act may the identity credential be used? A holder’s use of an identity credential, by which to identify and authenticate himself to relying parties, has three general purposes: 1) access to data, networks, facilities, and services; 2) attribution of messages; and 3) adoption/approval of documents and transactions.

The Level of Assurance (LOA) at which the identity provider issues the credential informs the relying party about the credential’s fitness for the particular purpose or use. For parties relying on identity credentials, determining the applicable assurance level is contextual (e.g. whether the individual
accessing a network, sending a message, or signing a document needs to be strongly authenticated or not). The LOA describes the strength of the identification and authentication processes.

In closed enterprise-centric identity systems, regulation of user control conduct is imposed by federation operators such as CertiPath and SAFE that typically run trusted third party registries.4

2. Identity Credential and Attribute Usage Control

Another determining factor for risk allocation in the identity context is legal control over the usage of the identity credential and identity attributes. How is the identity credential actually used? This intersects with the larger issues of data ownership rights and data protection obligations. For example, the obligation to protect data either accessed at rest or transported with the usage of a credential can be described as consisting of four main duties:

a. Confidentiality (unauthorized access, use, disclosure)
b. Integrity (authenticity; unauthorized alteration, contextual integrity of identity)
c. Availability (public access; accidental or unauthorized destruction; authorized access)
d. Authentication/non-repudiation (Chain of custody; Evidentiary proof)

These ownership rights and duties run with the data. Accordingly, all subsequent data holders do so subject to these contextual interests and obligations. Similarly, identity information and privacy challenges are best approached in a contextual manner.

3. Examples of Liability Risk for Use and Usage of Identity Credentials and Identity Attributes

With respect to use control, identity management essentially involves two fundamental processes: (1) the process of identifying a person, and (2) the process of later verifying that a particular person claiming to be that previously identified person is, in fact, such person for a particular purpose (“authentication”). Process risks generally involve privacy, performance, accuracy, and compliance.

Authentication is a transaction-specific event. “When an individual seeks access to an organization’s systems, he or she ‘authenticates’ him or herself by providing the credential issued during the enrollment process. The authentication process provides a level of assurance as to whether the other

---

4 Demonstration of use control is a legal requirement in contexts such as proving holder status of a transferable records or attribution of an electronic signature. Possible future work on electronic commerce – Proposal of the United States of America on electronic transferable records, United Nations Commission on International Trade Law (June 18, 2009), p. 5. See also, UNIFORM ELECTRONIC TRANSACTIONS ACT (UETA) Section 16, Official Comment 3 (Nat’l Conf. of Comm’rs on Unif. State Laws 1999).
party is who they claim to be. The level of assurance and associated authentication credentials required depends on the level of risk inherent in the transaction or interaction.”

The American Bar Association Identity Management Legal Issues Task Force has conducted comprehensive studies of identity system participant risks and potential liabilities relating to identity proofing and authentication. Harms from a federated identity management operation typically result from faulty identification, faulty authentication, inadequate security for or misuse of personal data, or failure to follow established procedures. They can lead to two broad categories of harm. First, a relying party may suffer harm when the relying party acts (a) in reliance on a false identity credential or identity assertion that it thought was valid resulting in unauthorized access, or (b) fails to act in reliance on a valid identity credential that it mistakenly believes to be false. Second, an identity credential holder may suffer harm when (a) her personal information is misused or compromised by the identity provider or a relying party to whom it has been disclosed, or (b) when she is improperly denied access or the ability to conduct a transaction.

For identity providers, the liability issue is primarily focused on whether its processes allowed for the creation of inaccurate identity assertions to third parties (i.e. identity credentials) or improper credential management. The identity proofing procedures may have been performed improperly or not in compliance with the requirements of the represented Level of Assurance. In the authentication process, the identity credential is supposed to prove: 1) that the identity proofing actually occurred and 2) the strength or assurance of proof that the credential actually belongs to the named holder. Authentication is the addition of these two proof elements.

“The Identity Provider is primarily responsible for the validity and integrity of the identification process and the resulting identity credential, the accuracy of the identity assertions, and the privacy and security of personal information about Subjects in its control. Identity proofing responsibilities often ascribed to the Identity Provider [by a given set of applicable operating rules] may typically include the duty to:

1. Properly and accurately collect and verify information regarding selected identity attributes for Subjects in accordance with the procedures specified in the applicable Operating Rules, including –
   a. Collect data of sufficient quality and quantity (either directly or through reliable third parties) necessary to permit it to perform the proofing required by the applicable Operating Rules;

6 Supra note 3.
b. Ensure that all identity assertions are accurately based on current valid information that is properly verified (e.g., an employer should not issue an identity credential for a terminated employee);
c. Where appropriate, use reasonable procedures to detect omissions or misrepresentations by the Subject or other third parties;

2. Ensure that all identity assertions are accurately based on current valid information that is properly authenticated (e.g., an employer should not issue an identity assertion for a terminated employee);

3. Comply with disclosed policies, practices and procedures for the identification and authentication processes (so that Relying Parties can identify assurance levels and determine the level of trust they should have in the resulting authentication and identity assertions);

4. Protect the privacy and security of Subjects personal information (and provide Subjects with appropriate notice, choice, access, and control of their personal data) in accordance with the applicable Operating Rules and in accordance with applicable law.”

“Credential issuance and management responsibilities often ascribed to the Identity Provider by the applicable Operating Rules include the duty to:

1. Properly issue each credential, and where appropriate, operate a credential management service;
2. Properly perform all identity assertion and authentication processes;
3. Ensure that the transfer of the credential and identity assertion is secure to prevent interception or compromise by unauthorized persons, and to protect credential integrity;
4. Provide to the Subject a capability to revoke a credential (to limit identity theft opportunities in the event that the Subject’s authenticator is compromised or the Subject no longer wants to participate);
5. Provide to all Relying Parties a capability to validate each credential (so the Relying Party can determine whether the credential is still valid and can be relied upon);
6. Where the Identity Provider retains and holds a Subject’s credential –
   a. Take reasonable steps to prevent the unauthorized access to or use of the credential
   b. Assume responsibility for third party unauthorized use of such credential.”

With respect to usage control, after authentication, a third process (referred to as “authorization”) is used by a relying party to determine whether to grant access rights, accept a signed document, or participate in a transaction or exchange of confidential information.

There are a number of common liability concerns related to identity credential usage. What is the liability of the identity credential holder for failing to protect the secret password or private key

---

7 Supra note 3, Part I at 19.
8 Id. at 20.
necessary to initiate an authentication process? What is the liability of the relying party for relying on a fraudulent assertion resulting in identity theft or fraud? Or what is the relying party’s liability for misusing or failing to adequately protect the credential holder’s personal information? Does the credential holder bear the risk of losses due to identity theft facilitated by his or her own negligent actions in the identity management system?

B. Liability Allocation for Identity Credential and Identity Attribute Use and Usage: Three Scenarios

Significant barriers to the creation of a digital identity credential market in the United States, as identified by The National Strategy for Trusted Identities in Cyberspace (NSTIC), include: 1) “The absence of a common framework to help establish trusted identities across a diverse landscape of online transactions and constituents,” and 2) “[u]ncertainty regarding the allocation and level of liability for fraud or other failures.” The European Commission recently has reached the same conclusion. As a response, the Virginia law accommodates a three scenario liability approach that is linked to control of the use and usage of the identity credential and attributes.

1. Federated Identity with Closed Enterprise Management: Identity Provider Maintains Use and Usage Control

The closed scenario (in which only service providers that are contractually bound to the identity provider are permitted to rely on a credential) currently is the predominant practice in federated identity management. The credential holder has the right to use the credential, and therefore has some form of control over the credential, pursuant to a contractual agreement with the identity provider. The credential provider controls the access rights, including usage restrictions and revocation. No express warranties are made to relying parties. In effect, the credential provider licensees use of the credential to the credential holder, who maintains physical possession. The credential holder must immediately notify the provider should the credential be lost or stolen.

Control requirements for credentials typically are met by the use of trusted third party registries in the form of Federation Operators such as CertiPath, and SAFE Bio-Pharma Association. “Perhaps the most difficult challenge for contract-based System Rules is the non-participant.”

---


(“New privacy protections will shift the current model of application-specific collection of identity information to a distributed, user-centric model that supports an individual’s capability to manage an array of cyber identities and to manage and assert personal attributes without having to provide identifying data.”).

10 In 2014, the European Union upgraded its e-signature directive to the status of a regulation and expanded the scope to include e-seals, electronic identification (eID), and eID trust services, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

11 Supra note 3, Part III at 12.
In the absence of legislation that standardizes the identity system legal relationships and renders liability allocation predictable, CertiPath has instituted what it labels a Third-Party Assurance Model. An important objective of this model is to provide relying parties, who would not normally have third-party beneficiary rights because of a lack of contractual privity, a means of recovery for damages against participating identity providers.

2. Federated Identity with Open Enterprise Management: Identity Credential Provider Maintains Use Control and Identity Credential Holder Has Usage Control

Usage of identity credentials across sectors and communities of interest, both public and private, exposes the current bilateral contractual scheme employed in closed systems as wholly inadequate to open systems. Cross-sector uses and usage pose two main challenges: 1) unlimited relying parties and 2) relying parties without a direct contractual relationship (or privity) with the identity providers to underpin liability risk allocations. Digital identity providers, trust framework providers, and relying parties are uncertain as to how courts will allocate liability in the absence of contract terms and statutory identity-related tort duties. The digital identity marketplace needs a more predictable way to know how courts will determine liability if damages occur to relying parties and consumers.

Relying Party Recovery for Economic Loss is Currently Limited

Because there is no contractual privity between an identity provider and a relying party in an open system, recovery for pure economic loss in Virginia is barred on tort and warranty theories by the Economic Loss Doctrine and VA CODE ANN § 8.01-2203. Moreover, product liability theories, including UCC warranty provisions, do not apply because an identity provider renders a service and not a good when asserting identity for authentication purposes.

As to whether there is an independent tort recovery theory that relying parties could apply against identity providers, no Virginia statute currently creates an independent tort duty or obligation in connection with third party online identification and authentication services. Nevertheless, identity providers are concerned that, in the absence of statutes, courts might find sources of duty in other tort theories. For example, courts might recognize claims of misrepresentation against identity providers akin to holding accountants liable to third parties that have relied on negligently prepared financial statements.

12 For a discussion of the difficulty in applying contract requirements to third party beneficiaries, see Jeff Nigriny and Randy V. Sabett, The Third-Party Assurance Model: A Legal Framework for Federated Identity Management, 50 JURIMETRICS 509-537 (Summer 2010) at 530.

13 Id.

As a possible tort theory for the recovery of economic losses in the identity context, the ABA Identity Management Legal Issues Task Force has studied the possibility of identity provider exposure for negligent misrepresentation. “The tort of negligent misrepresentation creates liability for 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. An incorrect assertion of one or more identity attributes, for example, might qualify as a negligent misrepresentation. 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. 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.”

Safe Harbor Legislation Creates Legal Certainty for Identity System Participants

A safe harbor is intended to reduce legal risk, as opposed to a legal mandate which actually creates additional risk. A legal mandate is a statute or regulation that prescriptively identifies a specific legal requirement with penalties for its violation. By contrast, a safe harbor does not prescribe requirements, nor is there a penalty for noncompliance. Rather, a safe harbor describes a set of facts and the policies and practices implemented by an organization, such as an identity trust framework operator, and the operator’s interpretation that under those facts the policies and practices of the participating identity provider are compliant with the identity trust framework. Identity providers that implement those policies and procedures are assured that they will not be penalized.

The Virginia law’s safe harbor makes both the identity provider and trust framework operator subject to a negligence duty of care for defective performance of the identity proofing and assertion. At the same time, the legislation addresses the concern about the risk of very large potential liability to an indeterminate class of parties that may reasonably rely on the identity assertions and trustmarks. Relying parties are deemed to be only those individuals or entities that rely on the validity of the identity credential or trustmark as defined by whether they have been issued in accordance with the given trust framework’s standards, rules, and procedures.

15 Supra note 3, Part II at 6-7
3. User Centric Identity Management: Identity Credential Holder Maintains Use and Usage Control

The NSTIC promotes a user-centric identity management approach in which the identity credential holder has both use and usage control. The NSTIC seeks to achieve this through laws and standards that will enable user-centric control of identity credentials and data. Each disclosing party should be able to choose the method of authentication, and each receiving party should choose the level of assurance at which the disclosing party must be identified. In view of the need to support online government services and maximize government-business identity provider interoperability, a goal of the NSTIC user-centric identity management system is to integrate privacy-enhancing rules and technologies in applicable trust frameworks.

Safe Harbor with Gross Negligence as a Liability Backstop in a Privacy-Enhancing Identity System

Because the user-centric identity system represents the least ongoing control by the identity provider over credential use and usage, and therefore results in the largest potential liability to the identity provider for indeterminate relying parties, the law legislation provides for an additional category of safe harbor in the form of Virginia-approved identity trust frameworks that will be the basis for providing civil immunity protection.

Even the most diligent identity verification process may be undermined by an individual intent on wrong-doing. The identity management marketplace needs to understand its liability if a digital identity credential is issued to an individual claiming an identity under false pretenses. To this end, the Virginia law provides that the identity trust framework provider and identity provider are immune from suit unless either “commits an act or omission that (i) constitutes gross negligence or willful misconduct, or (ii) does not adhere to the rules and policies of its respective trust framework that meets or exceeds Commonwealth identity management standards.” (Section 59.1-552 C.)

The primary means by which either type of protected entity would be judged is the respective trust framework’s criteria under which they have been certified. However, the legislation further contemplates a fail stop; a scenario where either a trust framework or identity provider has actual

---

16 Supra note 9 at 2, 3, 5, 12, and 22.

17 The Virginia Supreme Court has defined gross negligence and willful misconduct in the context of an exception to civil liability limitation. “Gross negligence involves conduct that ‘shocks fair-minded people,’ and willful and wanton negligence involves such recklessness that the actor is aware that his conduct probably would cause injury to another.” Cowan v. Hospice Support Care, 268 Va. 482, 603.S.E.2d 916 (2004) (quoting Etherton v. Doe, 268 Va. 209, 213-14, 597 S.E.2d 87, 90 (2004). Gross negligence “is a degree of negligence showing indifference to another and an utter disregard of prudence that amounts to a complete neglect of the safety of such other person.” Id at 487. Willful and wanton negligence, more specifically, involves “acting consciously in disregard of another person’s rights or acting with reckless indifference to the consequences, with the defendant aware, from his knowledge of existing circumstances and conditions, that his conduct probably would cause injury to another.” Id.
knowledge that the identity credential holder’s usage would be noncompliant with a given relying party’s assurance requirements. While the Commonwealth of Virginia could adopt a trust framework that permitted such a general authentication use, there is a backstop to enforce the gross negligence minimum of due care in the event of a known inappropriate usage.

Precedence for this approach has been expressed in many places. At the Federal level, the NSTIC has identified liability limitation for identity credential providers as an important issue for implementing user-centric identity management. Specifically, the National Strategy posed the question whether there should be liability limitations on identity providers for relying party damages caused by fraudulent usage of identity credentials. “The Identity Ecosystem Framework should also clarify service provider accountability in order to overcome the uncertainty and fear of unbounded liability that have limited the market’s growth. For example, it must answer questions such as whether or not identity providers should have legal protection if they have complied with the defined standards and credentials are nonetheless issued or used incorrectly.”18

The Code of Virginia contains several precedents for the use of a gross negligence or willful misconduct exception to civil immunity as a means of giving service providers, including information providers, a liability backstop:

1. Va Code Ann § 8.01-220.1:2 – acts or omissions by teachers within the scope of employment and taken in good faith in the course of supervision, care or discipline of students.
2. Va Code Ann § 8.01-226.4 – hospice volunteers
4. Va Code Ann § 8.01-226.5:1 – school principals or other school board employees who, in good faith, supervise the self-administration of asthma medications.
5. Va Code Ann § 17.1-293 – Circuit Court Clerks when providing remote access to information over the internet.
7. Va Code Ann § 54.1-2524 – the Virginia Department of Health Professions when providing remote access to the Prescription Monitoring Program for controlled substances.

As an example of a commercial safe harbor adopted as a means of encouraging a market capability, ship owners enjoy statutory limitation on recoverable loss and damages involving cargo and passengers. The vessel owner and demise charterer, whether individual, partnership or corporation,

18 Supra note 9 at 31.
may claim the benefits of the limitation statute, which allows limiting liability to an amount equal to the value of the vessel remains.\(^{19}\)

II. Societal Implications of Trust Framework Approach

The expansion of the market for digital identity credentials, particularly the lowering of barriers to entry for less highly capitalized credential and trust framework providers, stands to benefit not just commercial but also social interests. The so-called digital divide already separates many communities and even entire regions from substantial access to goods and services both virtual and physical.\(^{20}\) If reliance on digital identity and remote authentication increases without significant improvements in access to identity credentials (and to the technology that will increasingly be needed to secure and use them), then generations of inequalities and unnecessary harm in these marginalized communities will be perpetuated and magnified.\(^{21}\)

Virginia faith communities and other social-justice-oriented nonprofits are thus presented with an intriguing opportunity in light of the Commonwealth’s new digital identity law. Churches, synagogues, mosques, and other faith-based organizations are already significantly involved in the web of public-private partnerships that represent the social safety net, particularly in urban areas. Many such organizations become de facto access sites for services, or points of key referral to more appropriate providers.\(^{22}\) It may be, therefore, that faith communities are well positioned to participate in a federated credentialing program or even to form their own trust framework.

In addition to their involvement in networks of social service provision, another strength of this model is the fact that many if not most churches and other faith-based organizations are already connected to each other by denominational structures. Even faith groups not formally associated with each other tend to be well connected in local communities, participating jointly in cooperative social programs and informal community development. Such connections could form the basis of a trust framework

\(^{19}\) An example of this is the Titanic loss, in which recovery was limited to the value of the lifeboats. Oceanic Steam Navigation Co. v. Mellor (The Titanic), 233 S.Ct. 718 (1914).

\(^{20}\) “Digital divide” has become a somewhat loaded and contested term. For current access figures and some discussion of implications, see Kathryn Zickuhr & Aaron Smith, Home Broadband 2013, Pew Research Center’s Internet & American Life Project (August 2013). For an older but more sophisticated discussion of what constitutes access, see Jos DeHaan, A Multifaceted Dynamic Model of the Digital Divide, 1 (7) IT & SOCIETY 66-88 (Summer 2014).

\(^{21}\) For a discussion of the societal implications of access relations and resulting new forms of economic divisions, see JEREMY RIFKIN, THE AGE OF ACCESS 11-15, 236-240 (Tarcher Putnam, 2000) (“The right not to be excluded – the right of access – becomes more and more important in a world increasingly made up of electronically mediated commercial and social networks. As more of the date-to-date communications among people, as well as much of lived experience, take place in the virtual worlds of cyberspace, questions of access will become paramount and the right not to be excluded will become critical.”).

\(^{22}\) For an example of churches as key referral points for mental health services, see Mark R. McMinn, Michael J. Vogel & Laura K. Heyne, A Place for the Church within Professional Psychology, 38 (4) JOURNAL OF PSYCHOLOGY AND THEOLOGY 267-274 (Winter 2010).
federation, just as they have in other industries (higher education being the most obvious example in the non-profit sector). In other words, the faith community represents an already connected network of local brick and mortar locations for digital credentialing agents and/or kiosks.

One reason faith groups might desire to become not just identity credential issuers but identity trust framework providers is out of an ethical commitment to respect the autonomy and privacy of identity holders. Unlike commercial credential providers, nonprofit credential providers would presumably feel less pressure to generate large amounts of revenue from the activity, especially at the expense of those most in need. They may be perceived by some as more trustworthy keepers of private data than either commercial or government trust framework providers. Another interesting and related application for faith-based communities is the digital credentialing of international and domestic emergency responders. Here again, faith groups are already deeply involved in the work in question, with many denominations operating relief organizations in the developing world.

III. Trustmarks

Enabling the development of identity-related information policy rules through trust frameworks and trustmarks has several advantages over a traditional regulatory approach: 1) it avoids cross-jurisdictional authority and choice of law challenges, 2) it provides greater flexibility and customization to suit the particular network and participant situations, and 3) it is easier to enforce against rule violators.

A trustmark is associated with a specific trust framework and signifies compliance with the trust framework’s policies and procedures. As such, the trustmark is granted to identity providers and identity attribute providers that have undergone a specified certification process. The scope of such a trustmark is limited to the processes for determining and asserting identity. It does not extend to the truthfulness of the underlying information upon which the identity assertion is made. Nor does it extend to the trustworthiness of the individual to whom the identity credential has been provided or his behavior when involved in an electronic transaction (i.e. actual usage).

Therefore the Virginia law specifically states that “use of a trustmark on an Identity Credential provides a warranty by the identity provider that the rules and policies of the trust framework of which it is a member have been adhered to in asserting the identity and any related attributes contained on the identity credential. No other warranties are applicable unless expressly provided by the identity provider.” (Section 59.1-551.) The law creates, for the first time, an implied warranty of fitness (i.e. assurance) for a particular authentication purpose relative to the provisioning of identity services.
Negligent endorsement

Subject to limitation by the economic-loss doctrine, a trustmark provider could face exposure for seal of approval or negligent endorsement type liability. Again, because the “trustmark” is not currently defined by any state or federal statute, liability is ambiguous.

The ABA Identity Management Legal Issues Task Force has studied this issue and confirmed the possible applicability of this tort theory in the identity ecosystem. “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, magazines which endorse products such as Good Housekeeping, and trade associations which lend their mark to products have all been held liable for negligent misrepresentation when the products that enjoyed their 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.”

Conclusion

Commercially provided digital identity services is a new area operating in a very old business law environment. Trust framework providers, identity providers, attribute providers all represent third and even further removed parties to a transaction while playing a pivotal role in the transaction’s enablement. Yet, there has been a lack of coordination of technology, policy and law resulting in a type of digital identity credential market failure.

The Virginia safe harbor law seeks to alleviate this uncertainty by creating a legal framework for the identity industry along the lines of that which is afforded in other areas such as the credit card industry and shipping. It is not designed to remove liability, but to make liability predictable and manageable through codification in policy and procedural documentation made public by the identity provider.

For the first time in an identity system in the United States, the Virginia law provides for tort and warranty liability that will enable relying parties and consumers to recover for economic losses. This need is especially acute with cross-sector relying parties that are not directly bound by any contracts with identity providers. At the same time, both public and private sector digital identity credential providers need to know what the liability will be for damages caused by the usage of a credential

23 Supra note 3 at Part II, pages 7-8.
issued to an individual claiming to be someone else. The legislation addresses the fear of identity providers and identity trust framework providers that relying party liability currently is so potentially unbounded and burdensome as to make online authentication services unduly risky to identity providers and, as a result, prohibitively expensive to consumers.

Timothy Reiniger and Jeff Nigriny were the principal authors and negotiators of the Virginia digital identity law.

Tim Reiniger is an attorney currently serving as Special Advisor on Digital Identity for the Commonwealth of Virginia. As Director of the Digital Services Group of FutureLaw, LLC, in Richmond, Virginia, he specializes in digital identity law and policy, cyber risk management, and information assurance. Tim can be reached at treiniger@futurelaw.net.

Jeff Nigriny, CISSP is the President and founder of CertiPath, Inc. With 18+ years in the IT industry focused primarily on information security, Jeff has become an internationally recognized expert in matters of digital identity credentialing, identity and access management, and information assurance. Jeff can be reached at Jeff.Nigriny@Certipath.com.

The Rev. Kyle Matthew Oliver began his career in the department of engineering physics at the University of Wisconsin-Madison where he was an Advanced Fuel Cycle Initiative fellow, programmer and systems analyst in the Computational Nuclear Engineering Research Group. He is now an ordained priest in the Episcopal Church and serves as digital missioner in the Center for the Ministry of Teaching at Virginia Theological Seminary. Kyle can be reached at koliver@vts.edu.
Evolving Issues for Healthcare IT Contracting

By Alan L. Friel

The emergence of mega-suite vendors, more use of the cloud, increases in data breach frequency and cost and big data privacy impacts make healthcare IT (HIT) vendor arrangements more complex, and solid agreements with HIT vendors, more important than ever. Addressing key legal and business issues during the request for proposal (RFP) and contracting process reduce healthcare providers’ risks and help minimize expensive change orders.

As will be more fully detailed below, healthcare organization (HCO) legal counsel and information technology (IT) professionals can take a number of steps, and keep certain issues in mind, when seeking proposals for IT vendors, selecting a vendor and negotiating and documenting the vendor agreement. Before a vendor is even selected, the HCO should develop a strategic IT roadmap that will guide the company in its IT procurement and contracting in a manner that is consistent with its overall short, medium and long term business plan and its understanding of how current and projected changes to the healthcare system, and its particular service markets, will affect its technology needs in the coming years. Heightened regulatory obligations applicable to HCOs will also drive IT requirements.

In addition, the need for flexibility to deal with the very real possibility of potential changes business and regulatory circumstances, including potential merger transactions and changes in the law, should be kept in mind. Using the RFP process, a vendor can be selected that meets the HCO’s most material business, technical and legal requirements. It is crucial to them carefully scrutinize and negotiate the boilerplate of the HIT vendor’s services agreement, and its often voluminous ancillary documentation, in order to assure that the HCO’s expectations can be met throughout the term of the agreement. These agreements are typically long, dense and heavily weighted to the vendor’s advantage. This article discusses the most material provisions of these agreements and the issues with respect to them that the HCO should be negotiating and can reasonably seek.

Develop and Follow a Roadmap

Healthcare providers have complex IT needs. Further, as modern HCOs develop more integrated HIT systems, they are increasingly turning to consultants to develop overall HIT strategic plans, which may include engaging a primary “mega-suite” vendor (some consultants are getting into this business themselves) to outsource development, implementation, scalability and operation of a myriad of HIT product and service portfolios through multi-vendor supply chains. A strategic roadmap will help in managing electronic health records, revenue cycle management, patient access and care tools, analytics and reporting systems and data processing and storage over time. Whether the HCO executes the plan by directly contracting with and coordinating multiple vendors, or relying on a mega-
suite vendor, care needs to be taken in structuring and documenting the parties’ rights, obligations and remedies to help avoid vendor problems and disputes and to better manage them when they occur. As new HIT services and vendors are added overtime, the roadmap should also help guide system-wide interoperability and functionality requirements.

**Use the RFP Process Wisely**

While RFPs can be time consuming, the RFP process is an opportunity to pre-establish desired deliverables, including material legal term expectations, as well as to undertake due diligence on the vendor’s track record, its data protection and service continuity programs and controls and its relevant resources and capabilities. This is particularly important regarding data privacy and security since vendor risk assessment prior to engagement, with appropriate controls documented in the service agreement, is crucial to a HCO meeting its own obligation to have and follow a defensible and appropriate risk assessment and corresponding program. Chief Information Officers should work together with legal and IT risk management to develop RFP parameters that set the stage for strong contractual protections for the HCO when the vendor relationship is formed and documented.

Vendor references should also be requested and checked. Trial licenses may be available and helpful in evaluating which products and services to select based on performance and interoperability. Also consider simultaneously negotiating with the two top RFP respondents so you are not stuck if the agreement negotiation does not yield commitments to the expectations that were called for in the RFP, or at least have a second choice you can turn to if negotiations with the first choice fall apart. Finally, as the standard agreements for HIT vendors are weighted heavily in the vendor’s favor, ask for a version with the “gives” that have been agreed to with other HCOs in comparable transactions. Occasionally, where a deal is very significant in spend, you can even get some sort of favored nation commitment on certain key terms.

**Carefully Scope the Fees, Services, Deliverables and Dependencies**

The scope of the services and technology licenses, as well as the deliverables specifications and any interoperability, scalability and interface requirements and any permitted dependencies that limit the vendor’s responsibilities, are material business points that should have been called out in the RFP. At minimum, they need to be carefully articulated in the agreement, and the definition of key elements such as authorized users, facilities, supported equipment, third party equipment, product, services, support services, vendor software, third party software, components, modules, interfaces, specifications, documentation, interoperability, releases, updates, upgrades, versions, enhancements, and material changes are crucial and determine what will be delivered for the contracted price and what the vendor will be responsible for or not. In some cases third party standards can be used to set element definitions, such as the definition of interoperability established by the Health Information
Management Systems Society or by the Institute for Electrical and Electronic Engineering, the standards your existing systems operate on and applicable Health Information Exchange requirements.

The fees for the various services and deliverables should also be well defined, advisably with renewal term increases pre-determined. Beware of hidden fees and add-ons, such as implementation fees related to “free” enhancement or updates. A change order process should also be agreed upon to address inevitable changed circumstances and is preferable to set the basis for rates for change orders in advance as opposed to then current market rates.

Pay particular attention to dependencies outside of the HCO’s control that limit the vendor’s responsibility, such as third party equipment or software changes, which may result in additional costs to the HCO and/or be exclusions to the vendors’ interoperability and/or warranty or maintenance obligations. If the vendor is relying on third party solutions for interoperability with other technology, try to make the vendor contractually responsible for that.

Obtain assurances that the vendor will be timely compliant with known and projected regulatory obligations that affect HIT systems, such as ICD-10, and build in a reasonable manner to accommodate unforeseen government or insurance industry mandates. Also address scalability as the HCO’s needs may increase or decrease over the life of the system, and how fees and services will be revised accordingly.

Work out the details of implementation, including schedule and training. Consider if there needs to be integration with systems that will be replaced and detail the vendor’s obligations regarding that conversion. Ensure that there will be adequate customer support, and additional future training as may be desired, and the cost therefor.

Finally, look closely at all the related agreements and governing documents that can affect the engagement, which may include end user licenses agreements, master services agreements, work orders, bills of material, service level agreements, maintenance agreements, hosting agreements, development agreements, various specifications documents and addenda, user guides and operating manuals, and even travel policies. Collateral agreements and documents can materially impact the main agreement and the parties’ obligations.

**Build Flexibility into Licenses and Consider Ownership of New IP**

The license should be as broad as possible, including as to permitted users, equipment, facilities and territory, and should be applicable to affiliates and assignable in a merger or change of control. It is a good idea to specify that the fees for expanding the license in the future and to try to limit the remedy for exceeding a license, especially if inadvertently, to those additional license fee rates.
If custom software is being developed, articulate who owns it and what the non-owner can do with the new intellectual property. Even where the HCO owns the new intellectual property, it is likely to be derivative of vendor and third party materials and dependent upon the continued ability to use and update them, which will need to be addressed. If the HCO is expecting to obtain proprietary deliverables it owns and controls, it also needs to consider how use of open source software in the creation of those deliverables may result in the derivative software being required to be made available to the open source community, and thus may want to restrict use of “copyleft” software.

Also consider providing for the possibility that the vendor does not remain financially or otherwise able to fulfill its obligations and could even go out of business, and address these risks through appropriate insolvency provisions, and potentially take over rights with software code and developer manuals held with a commercial software escrow that the HCO can access upon a triggering event.

**Plan for Changes, Transitions and Termination**

Obtain termination rights for material breaches, chronic service failures, undesired vendor changes and changes in your circumstances and legal obligations. Try for a termination for convenience right, even if it includes a reasonable kill fee. Provide for an orderly exit process on termination, including appropriate transition support and data delivery or destruction, and establish the cost thereof.

**Address Data Protection**

HIT programs necessarily generate and/or process, store and transfer data. Firstly, agreements need to establish who owns what data as between the parties and who can use what data for what purposes. This has regulatory data privacy and security implications discussed below. In addition, a HCO should require that all its data be exportable upon demand on usable formats. A negotiated point will be what if any additional charges the vendor may impose for doing so. The contract needs to specify what data is to be available, and on what basis, which may require consultation with the HCO’s clinicians for services related to clinical care. Contracts need to provide for the retention and destruction of data consistent with the HCO’s information governance policies and needs, and particularly when vendors and/or their sub-suppliers are no longer performing services.

HCOs have a host of privacy and data security obligations that will apply to their HIT service providers, including regarding personally identifiable information of employees and consumers, credit card data, and protected healthcare information (i.e., most individually identifiable health information held by entities subject to state and federal healthcare privacy and security laws) (PHI). The HCO is ultimately responsible to the data subjects and regulators for its vendors. The HCO’s overall data risk assessment should be applied to each vendor, the vendor’s policies and practices assessed and the vendor appropriately contractually obligated.
In addition, information governance obligations should be specified, including data segregation, residency, redundancy and backup obligations and response times for providing access to or delivering stored data, and in what formats, and for its retention and destruction and certification of destruction. Residency is particularly important for cloud services and other outsourced processing and storage, since many countries outside of the U.S. prohibit data access from, or transfer to, the U.S. absent commitments that exceed U.S. legal standards, even if the data originated from the U.S. Consider addressing redundancy and backup by permitting the HCO to periodically backup its data on its own, or another vendor’s, servers, or in the case of mega-suite vendors requiring them to multi-source this task with its sub-suppliers.

Under HIPAA (Health Insurance Portability and Accountability Act), as supplemented by HITECH (Health Information Technology for Economic and Clinical Health Act), a party with data transmission to or from a covered entity (or its business associates), with routine access to PHI, is a “business associate” subject to privacy and security obligations with regard to PHI. An appropriate business associate agreement (BAA) setting forth its privacy and security obligations as to the PHI, including what it can do with PHI and how it will secure it, is a necessary part of the vendor engagement, any breach of which should be a material breach of the vendor agreement that is not subject to limitations of liabilities or damages. Mega-vendors should be required to have a form of BAA that meets defined standards signed by its sub-suppliers, and should remain ultimately liable for any breaches by their sub-suppliers.

Although HIPAA allows for covered entities to disclose PHI to business associates for the purpose of de-identifying it to HIPAA de-identification standards (including limiting re-identification), which would render no longer PHI and then subject to expanded use by the vendor, care should be taken in defining the de-identification obligations. Further if it is the vendor accessing PHI and doing the de-identification itself, rather than receiving de-identified data sets, accepting a payment or even a discount in exchange for PHI access for purposes unrelated to performing necessary services for the covered entity would seem to violate HIPAA’s prohibition on remuneration for PHI absent a defined exception that apply to other situations (e.g., cost-reimbursement of sending prescription refill reminders). In addition, as state and federal medical data privacy and data security laws are evolving, with new state legislation introduced frequently and enacted not irregularly, the vendor’s data rights and obligations need to be subject to future applicable law and the HCO should have the ability to restrict usage and increase obligations in the future if it deems so necessary or otherwise appropriate.

HCOs have notification obligations to data subjects and regulators under federal and state law in the event of a data security breach of unsecured PHI, and accordingly the vendor agreements need to provide for vendors to give the HCO immediate notice of suspected incidents and spell out the vendors’ cooperation and remediation obligations.

Where a mega-suite vendor has been engaged, HCOs need to keep in mind that they, not the master vendor, remains ultimately responsible for conducting a HIPAA / HITECH risk assessment of using a
multi-vendor supply chain and having the mega-suite vendor implement the controls deemed necessary by the HCO throughout that multi-vendor supply chain. Transparency and contractual standards on how subcontractors and other suppliers and service providers are selected, engaged and monitored is recommended. Even for a single-source vendor, contracts should require that the vendor workforce with access to the HCO’s data is limited except as necessary to perform the services and that staff is responsibly selected, appropriately trained and effectively monitored and managed.

Agreements need to accommodate for evolving compliance obligations and vulnerabilities not yet contemplated by allowing for the addition of additional controls and obligations, or the ability to terminate.

**Establish Milestone, Testing, Approval and Revision Terms**

Performance and fees can be broken into deliverable obligations at various milestones, including scoping, development, acceptance, installation, training, implementation, go-live and operation and maintenance periods. Each milestones can have detailed deliverable specifications and a submission, testing and acceptance process can be established. The HCO should have the right to request revisions until acceptance is obtained, and the ability to terminate for cause if acceptance cannot be timely obtained with minimal revisions. Penalties can also be provided in the event of schedule delays in meeting milestones. Consider also an ability to terminate without cause at each milestone, which can sometimes come with a kill fee.

**Obtain Guarantees and Warranties, Provide for Maintenance and Service Levels, and Consider Enhancements**

The agreement should establish minimum acceptable levels of service consistent with detailed specifications and free of material errors or downtime other than during established regularly scheduled maintenance (during appropriate dates and times where usage is minimal). Following a typically limited warranty period, a maintenance contract may be required to continue the service level commitment. Beware of exclusions to maintenance obligations. Maintenance should include doing everything necessary to maintain compatibility with crucial third party equipment and software as such may change or be updated or enhanced. Maintenance contracts can also include making additional enhancements and improvements, especially up to a certain time allotment not otherwise used to perform routine maintenance. This is advisable to address changes to the HCO’s HIT environment, which is likely to expand and change over time. Beyond any allotted time for this have the contact set a predetermined cost for additional work.

A service level guaranty should spell out how acceptable service and downtime will be measured, ways the vendor will minimize service outages, how problems are reported and managed, the minimum time for the vendor to respond to and solve differing levels of problems and provide for credits for failures and a termination right for chronic failures. The more critical the system, the higher the
service level commitment should be and the more severe the remedies for failing to meet it. For mega-suite vendors, the vendor’s service levels should apply to all of its sub-supplies, though the mega-suite vendor should be ultimately responsible. One value of a multi-vendor supply chain managed by a master vendor may be the vendor’s ability to rapidly move services to another sub-supplier in the event of a problem and that can be established as response obligation. Dedicated contact persons or numbers available 24/7 are recommended, as is a ticketing system and regular reporting on ticket status while service is being remedied.

The HCO should seek the service warranty to include compliance with functional, performance, and compatibility specifications, virus and malware protection, and prevention of unauthorized access or use. Beyond a basic service warranty and service level guarantees, additional warranties related to compliance obligations, non-infringement, confidentiality and interoperability can be negotiated. Copies of vendor data protection and breach response, business continuity management and disaster recovery, information governance and other relevant policies and processes can be attached as exhibits to agreements and the vendor can represent and warrant that it will follow them throughout the term, with material changes subject to approval, and comply with all applicable laws as well as specifically articulated key contractual obligations, including the BAA terms.

**Negotiate the Liability, Remedies, Insurance and Indemnity Terms**

Contracts need to clarify which party is responsible under what circumstances for what with respect to compliance with law, third party infringement claims and data protection. This can get nuanced depending on what each party is contributing and doing. For instance, both parties may be contributing software, content and data, for which they should be responsible for to the extent it is used by the other as permitted. Vendors typically want to exclude liability for clinical decisions based on erroneous data, though that can be countered by limiting the exclusion to where data errors do not arise out of failure to meet certain performance and testing requirements or from gross negligence or intentional misconduct.

Remedies limited to fees paid to the vendor (often for a partial look-back such as 12 months) offer inadequate protection for continuity, data protection and integrity, compliance with law and intellectual property infringement risks, for failure to fulfill confidentiality obligations and for patient harm or death arising out of failure of the vendor to meet a defined standard and/or certain defined obligations. Damages arising out the vendor’s breach of representations, warranties and obligations related to those matters should ideally not be capped or subject to other damages limitations. This is often one of the most hotly negotiated points, with the vendor arguing that the pricing assumes that it will have limited liability and the HCO countering that the vendor must be stand behind its core obligations. Where the lines are drawn will depend on leverage, and accordingly setting expectations on these issues as part of the RFP can help minimize the negotiations.
Some intellectual property infringement and errors and omissions risk, and increasingly data privacy and security incident risk, maybe insured by vendors, and agreements can require certain specified types and levels of coverage be maintained with the HCO added as a named additional insured (with any insureds dispute exclusion not applicable). The HCO can itself insure against the risk of data loss, damage or compromise, but policy terms need to be carefully checked as exclusions and limitations can affect the practical value of such coverage. It is recommended that HCO’s policies pre-qualify the HCO’s law firm of choice (and its rates) as acceptable under defense and incident response coverage.

Establish Oversight, including Self-Auditing

Ideally, contracts will provide for audit rights. For some large providers that resist such oversight, and for mega-suite vendors who undertake contractual responsibility for a multi-vendor supply chain, self-assessment and certification should be considered. Where appropriate, require copies of vendor audits (e.g., SOC 2 / SOC 3), certifications (e.g., ISO 27001, FedRamp, etc.) and self-certifications (PCI-SAQ, EU Safe harbor, etc.) and evaluate the vendor’s ongoing risk profile. These types of requirements should be specified as a deliverables in the RFP. Many vendors have existing self-assessment and certification programs that can be reviewed for adequacy during the RFP process.

Vendors may also want audit rights to ensure the licenses are not being exceeded. Such inspection rights should be at vendor’s cost (absent significant finding of infringement) and reasonably limited not to interfere with the HCO’s business or systems.

Keep Mergers in Mind

Mergers, acquisitions and divestitures can require that the parties HIT systems be shared during a transition period, typically through an information technology transition agreement, and then some legacy systems and vendors phased out. Standard vendor agreements often require approval of assignments, which should not be the case for a HCO’s assets sale, merger or change of control. HCOs also need the ability to make vendor agreements available for review as part of potential transaction due diligence, so that should be carved out of the confidentiality provisions. Finally, as such a transaction may result in the jettisoning of some HIT systems and service providers after an initial transition period, it is advisable that such a transaction provides the basis in the agreement for a termination by the HCO, and transition services from the vendor, with minimal financial impact on the HCO.

Conclusion

Taking these considerations into account will help HCOs codify the parties’ agreement and their respective obligations. Thereafter, IT vendor management should be employed to ensure that vendors perform and comply and that changes in the vendor’s or the HCO’s business or legal obligations are evaluated and mitigated as necessary. A strong and flexible agreement will make doing so easier.
Alan L. Friel is a former General Counsel of a technology company and partner at BakerHostetler in its Los Angeles office. He represents clients in information technology and intellectual property transactions and regarding privacy and data security matters. Mr. Friel is an adjunct Professor at both University of California Los Angeles and Loyola Marymount School of Law. He has been named one of the most influential lawyers in digital media and e-commerce by the Los Angeles Business Journal and recognized by Chambers, Legal 500, and American Lawyer Media. Mr. Friel may be reached at 310.442.8860 or AFriel@BakerLaw.com.
2011, the year of the Arab Spring, presents a unique opportunity to look back and study how the relative freedom and development of information environments affect stability in nations throughout the Middle East and world. Such study raises interesting questions about whether freedom of information and speech are ultimately stabilizing influences for society in terms of loyalty, violence and political unrest—questions all the more important as societies face the onslaught of the internet, mobile devices and cell phones. Are non-democratic regimes “better off” by monopolizing and controlling the flow of information over new information channels? Are democratic societies, particularly developing democracies, more stable when the flow of information over such channels is relatively unrestricted? While these questions are not definitively answered, valuable insights into the relationship of information environments and stability are gained by the theory and empirical study advanced by this article.

On December 17, 2010, Mohamed Bouazizi, a Tunisian street vendor, lit himself ablaze in protest to unfair police licensing practices and at the same time touched off a wave of protests that would come to be known as the Arab Spring.1 The effects of the events were international in scope, spreading throughout the Middle East, but those effects were not, as shall be seen, evenly distributed.

By June of 2011, regime changes had been forced upon four Middle Eastern governments: Tunisia, Egypt, Libya, and Yemen.2 Other Middle Eastern governments escaped but confronted demonstrations.3 Many have believed or suspected there was a link to modern communication

1 Mohamed Bouazizi, ENCYCLOPAEDIA BRITANNICA, [link]
technologies and the social disruption in the Middle East. A few have found links between technologies and that disruption.\(^4\)

The purpose of this paper is to examine the possibility that freedom of information is a stabilizing influence in societies. This paper will do this in two ways (I) through economic analysis and (II) through statistical analysis of the relationship of distress in a selection of states with and without large Muslim populations during 2011, the year of the Arab Spring. Part I offers a theoretical explanation, based on upon existing theory in legal literature known as Market for Loyalties Theory, of the phenomena occurring around the states’ control and loss of control of their respective information environments. It also raises questions about whether this control over the information environment and instability can be measured. Part II seeks to link freedom of information to state instability in the context of Muslim countries in the year 2011. This article will conclude that there exists a moderate correlation between freedom of information and stability after controlling for other socio/economic variables. Furthermore that correlation is consistent with the theoretical economic analysis proffered in the first part of the article.

I. Economic Analysis: The Market for Loyalties

As originally conceived by Monroe Price, there is market where the medium of exchange is not cash, but loyalty.\(^5\) The major item or service for sale in this market is identity—the ideology, hopes, dreams, land claims, aspirations and sense of belonging of a people. The buyers are citizens, subjects and peoples, and the sellers are governments and power holders (political parties, revolutionaries, terrorists, and even brand names). Understanding this market is important because it offers an explanation of why governments and non-state powers regulate the control of information.\(^6\)


Governments and power holders create monopolies in the market for loyalties to ensure they can get enough loyalty to guarantee service in the military, payment of taxes, political support for the regime, tolerance of corruption, and keeping talented and wealthy citizens and subjects in the country. The Market for Loyalties, as developed by Monroe Price, is set forth next.

<table>
<thead>
<tr>
<th>Economic Term</th>
<th>Market for Loyalties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sellers</td>
<td>Governments and power holders</td>
</tr>
<tr>
<td>Buyers</td>
<td>Citizens</td>
</tr>
<tr>
<td>Price/currency</td>
<td>Loyalty</td>
</tr>
<tr>
<td>Goods</td>
<td>Identity</td>
</tr>
</tbody>
</table>

Understanding the relationship of loyalty to “identity” is essential to understanding this market. Perhaps the most loyal of all groups are suicide bombers and terrorists—they are willing to sacrifice everything—and for what? Identity. “Camaraderie, power, status, honor, identity, purpose, . . . powerful emotional experiences, and the prospect of heavenly rewards” are listed as the diverse “output” offered by religious terrorist groups. Indeed, “ideology is not the only, or even the most important, factor in an individual’s decision to join. [O]peratives are often more interested in adopting a new identity than in supporting a terrorist group’s stated goals.” Indeed as terrorist researcher and author Jessica Stern notes, “Finding an identity with dignity is absolutely key” to the motives of terrorists. The message of identity may consist of a party platform, ideology, or national ideals and aspirations. It may be as ephemeral as the hope for a better future or as concrete as the desire for a national homeland. Identity is valuable to buyers as it contains both the legacy of their past history and the promise of their dreams for the future (whether it is for wealth, a better life, or memorialization as a martyr).

Loyalty is the “coin of the realm.” It is how identity is paid for by citizens and subjects, the buyers of the market for loyalties. The consumer “pays” for one set of identities or another in several ways that, together we call “loyalty” or “citizenship.” Payment, however, is not expressed in the ordinary coin of the realm. It includes not only compliance with tax obligations, but also obedience to laws, readiness to fight in armed services, or even continued residence within a country.

Loyalty then is price in any price and quantity of goods (PxQ) analysis.

---


All other factors being equal, when monopoly forces are removed from the market, the price (in this case loyalty) slides down the economic demand curve to a point of stabilization as dictated by a competitive market. New producers of identity enter the market and offer it for less price in terms of loyalty. An example might be the effect of punk rock on the former Soviet Union. Being a punk rocker did not demand military service or taxes, but it did demand loyalty in dress and hair style, commitment to certain music, and in some cases devotion to anarchism. Loyalty that would have gone to being a model Soviet citizen was now going to punk rock. See Figure 1 below, which illustrates the societal phenomenon of loyalty price dropping. While the price may be stabilizing in the loyalty market, the effect is anything but—loyalty levels necessary for military service, good citizenship, tolerance of corruption, adherence to a political party, and even staying in the country, drop. There is a destabilizing effect from loss of monopoly or oligopoly control over the market for loyalties. This is why autocratic and oligarchic forms of government seek to control information flow—without it they cannot sustain the levels of loyalty necessary to stay in power and run the country. An example is North Korea, which issues radios and TVs pre-wired to government broadcast stations.11

Figure 1: Demand curve illustrating the drop in loyalty in the market between the monopoly and competition points

In Figure 1 there has been a drop in price (a drop in loyalty). However, it is an oversimplification to say that the size of the vertical drop is what determines the total instability at a societal level. Rather a geometric calculation is performed based on the area of price/loyalty and goods/identity.

To correctly do the analysis on a societal level, it is the comparison of the two areas $P_M \times Q_M$ (Price times Quantity at the Monopoly Point) and $P_C \times Q_C$ (Price times Quantity at Competition Point) that determines whether the market is inelastic and unstable. See Figure 2. The real question is whether there is less overall loyalty in the market for a particular society and that comparison is based upon a two dimensional figure ($P \times Q$).

The sizes of the two areas (one for the monopoly point and the other for the competition point) are determined, in turn, by the shape of the demand curve. Interestingly, the shape of the curve is determined by the presence of “substitute goods” in the market—for instance in the absence of internet access points in the market, radios and televisions stations can serve as substitutes, providing alternative channels for information.\(^\text{12}\) The more channels there are for information, the flatter (or in economic terms, the more elastic) the demand curve and the less of an impact the loss of monopoly control has on instability in the market for loyalties. See, for example, Figure 3. By way of analogy, the demand curve for motorcycles might be relatively elastic if there were plenty of inexpensive small cars (such as the British three wheel Reliant) and motorized bicycles (“mopeds”) also available in the market.

Market for Loyalties predicts that countries with many forms of substitute goods—identities streaming from a broad array of information channels—books, movies, radio, etc.—will have a flatter demand curve, and hence the appearance of new information technologies, with lack of central control, will have less significant consequences in the market for loyalties. Ultimately, in a market with many substitute goods, the disruption of a new entrant grows infinitesimally small. “Hence, a state in which a diversity of identities flourishes is a supremely stable one, at least mathematically, with

\[ i = f \left( \frac{k}{p} \right) \]

“where ‘i’ is the instability, ‘k’ represents the level of new competing identities being introduced, and ‘p’ is the penetration of previously competing identities, or substitutes, into the market.” Paul D. Callister, The Internet, Regulation and the Market for Loyalties: An Economic Analysis of Transborder Information Flow, 2002 U. ILL. J. TECH & POL’Y 59, 96-97.

Eventually, in a state that opens itself to competing identities, if “p” were to approach infinity, the level of disturbance will grow infinitesimally small (at least with respect to the instability caused solely by the introduction of new identities):

\[ \lim_{p \to \infty} \frac{k}{p} = 0 \]

It would not be correct to state:

\[ \lim_{p \to \infty} f \left( \frac{k}{p} \right) = 0 \]

This is because a portion of the formula, namely the other factors which impact elasticity and instability, are unknown. All that is known is that the instability resulting from the introduction of new identities will approach zero if, in theory only, the number of previously introduced identities approaches infinity.
respect to the instability caused by the introduction of new identities.”15 This means that the effect of a new political newspaper, radio station, web site, etc., in the United States may be relatively inconsequential with respect to diminishment of loyalties in the market, especially compared to the impact of a new media source in a country like pre-invasion Iraq or North Korea.

This analysis assumes that diverse technologies will produce diverse messages of identity, which is one of the “goods” referred to in Market for Loyalties analysis. This may not always be the case, since it is theoretically possible for some group to seize all of the channels of communication and wield them into a single message, but common experience tells us, at least in the West, that the different information technologies diversify the messages of identity streaming into the market for loyalties. For example, the arrival of blogging and Twitter news feeds has not consolidated news into a single viewpoint, but diversified the points of view. Indeed, the phenomena of citizen journalism has facilitated diversity of viewpoints.16 Thus, the more information technology channels, the more messages, and the flatter the demand curve—which ultimately means less disruption whenever a new message of identity or information technology enters the market.

At the same time as a loss of control over information may be occurring, it would seem that suppliers requiring the least sacrifice—in terms of loyalty price—would win the most followers. The market should be settling, with all but the former autocratic power becoming comfortable with this new state of affairs. However, other forces operate to keep loyalty prices so high that opposition groups still can find followers willing to commit violence and even act as suicide bombers. The reasons for this are manifold. While loyalty prices should drop after removal of monopoly control, there may be new buyers in the market—disenfranchised peoples who long for identity. After the invasion of Iraq, such is the case with disenfranchised Shiites, Kurds, and the marsh dwellers of the south. They increased demand rather than lessened it. In a sense, countries with comparatively large numbers of jobless or underemployed young people, who represent new buyers in the market, may see loyalty prices spike upward, even as informational controls are lessened because the same forces that have liberated information have also liberated new buyers into the market.17 The opening of information channels is accompanied by violence. The loyalty price remained high because demand for identity was high. In such markets, new identities, such as being a martyr, with high loyalty prices may compete and attract followers because there simply is not enough identity available in the market.

Other factors such as tribalism can operate to create a sort of retail/wholesale market in which the tribes act as middlemen who have entered into exclusive dealing relationships with the central

---

15 Id. at 97 n.178.
16 See Serena Carpenter, Source Diversity in U.S. Online Citizen Journalism and Online Newspaper Articles (paper at International Symposium on Online Journalism, April 5, 2008), https://online.journalism.utexas.edu/2008/papers/OnlineCitizenJournalism_Carpenter.pdf. “Overall, online newspaper journalists were more likely to incorporate a greater number of sources . . . and a greater diversity of viewpoints.” Id. at 2.
17 See discussion of “marginal consumers,” Callister, supra note 8, at 139-40.
government or opposition groups.\textsuperscript{18} The transaction costs for leaving the tribe (death, shunning, etc.) are so high that the whole arrangement actually works to keep loyalty prices high.\textsuperscript{19} This was also the case in Iraq after the fall of Saddam Hussein—tribalism acted to keep loyalty prices high.\textsuperscript{20} So while removing controls over information flow should lead to a drop in the loyalty commanded by the previous power-in being, other forces such as new buyers in the market and tribalism may cause loyalty prices to remain high, even high enough to facilitate suicide bombings (perhaps the ultimate form of loyalty in this analysis).

Within the context of freedom, it would seem that freedom of information flow is desirable and that it would fall within the scope of fundamental human rights, such as in the Universal Declaration of Human Rights.\textsuperscript{21} A cold fact remains, however, from a market analysis, that the removal of censorship and controls over information flow can lead to destabilizing effects from either a radical drop in the loyalty price or an increase in demand brought about by new entrants into the market place.

So far this is only theorizing. The question presents itself: what evidence is there that freedom of information is stabilizing or destabilizing to the state? To answer that, we move from economics to statistics.

\section*{II. Statistical Analysis of Information Flow and State Instability in Countries During 2011, the Year of the Arab Spring}

The idea is to see if there is any evidence (or correlations) that states with more freedom of access to information were better off (at least with respect to state destabilization) than their counterparts during the events that made up the Arab Spring. To do this, the information environments and relative stability of a wide swath of Muslim countries were studied, including countries that had large but not predominantly Muslim populations, like India and the Philippines. Furthermore, to properly scale measurements, countries and regions without significant Muslim populations were studied. For example, the analysis below evaluated Japan, which happened to lead in book titles published, and Hong Kong, which led in films produced.

\textbf{Method}

This correlational study is an examination of the relationship between freedom of information access (as suggested by greater channels of information technology) and state destabilization (defined in terms of an index measuring demonstrations, protests and violence) during the year of the Arab Spring,\textsuperscript{18} See \textit{id.} at 140-146.\textsuperscript{19} See \textit{e.g.}, Rajiv Chandrasekaran, \textit{Iraqi Wild Card: Tribal Loyalties Hard to Predict}, \textit{WASH. POST}, Jan. 19, 2003, at A1. To betray one’s tribe would have serious repercussions. In fact, when [Saddam] Hussein’s sons-in-law returned to Iraq from Jordan, after betraying secrets about Iraqi weapon’s program, they were killed, not by “police or the military, but [by] members of their own tribe seeking to redeem the family’s honor.” \textit{Id.}\textsuperscript{20} See discussion of “Wholesale and Retail Markets” Callister, \textit{supra} note 8, at 140-45.\textsuperscript{21} United Nations, The Universal Declaration of Human Rights, art. 19, \url{http://www.un.org/en/documents/udhr/} (last visited Dec. 9, 2013).
2011 in a sample of selected countries. The intention was to determine whether countries without monopoly control over their information environments were better off than their counterparts during the events that made up the Arab Spring, at least with respect destabilization. While the study is primarily descriptive in nature, it is also intended that cautious inferences might be made to countries beyond those selected in the sample or to periods of time beyond the year of data collection, 2011.

Sample

Data was collected from a purposefully selected sample of 26 countries, intended to include countries with both highly controlled information environments and comparison countries that allow their citizens more free access to information. The sample was chosen to include both Muslim and non-Muslim dominant countries; however, Muslim-dominant countries were included at a higher rate due to their tendency to more strictly control their information environments. The countries included in the study are listed below.22

Measures

To empirically examine the relationship between freedom of information access and state destabilization, both constructs first needed to be measured. It was theorized that an average of normalized versions of Thomson Reuters Westlaw’s Demonstrations and Protests (DP) and Violence or Civil War (VC) indices (described below) would serve as a reasonable proxy for the construct of state destabilization because they illustrate citizens in acts of disloyalty—demonstrating, committing acts of violence, inciting civil war, etc.

To measure state instability, and create the DP and VC indexes, the following method was devised:

- Using Thomson Reuters Westlaw create a “Demonstrations and Protest” (DP) Index for 26 countries:
  - Search number of articles with the country name in the title for 2011.
  - Of those, search number of articles containing "demonstration" or "protest" or "riot."
  - Subtract false positives in first 20 hits to create a multiplier to determine the number of articles to be finally counted.
  - Normalize the scores by population and adjust the highest score to a 1.0 and the lowest to 0.0 with all other scores adjusted according to their respective relationships.

- Using Thomson Reuters Westlaw create a “Violence or Civil War” (VC) Index for 24 countries

---

o Search number of articles with the country name in the title for 2011.

o Of those articles, search the number of articles containing the following in the results:
  (SHOOT! OR SHOT OR BOMB! OR INSURGEN! OR TERROR! OR REBEL "CIVIL WAR" OR
  KILL! OR FIGHT! OR ATTACK! OR KIDNAP! % TEAM % FOOTBALL % CRICKET).

o Normalize the scores by population and adjust the highest score to a 1.0 and the lowest
to 0.0 with all other scores adjusted according to their respective relationships.

- Combine the DP and VC scores by averaging them into a “DPVC” index

The combined results were once again normalized adjusting the highest score to a 1.0 and the lowest
to 0.0 with all other scores adjusted according to their respective relationships. The DVPC index for the
countries in the study are ranked as follows:

<table>
<thead>
<tr>
<th>Country</th>
<th>DPVC</th>
<th>Country</th>
<th>DPVC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yemen</td>
<td>1.000</td>
<td>Saudi Arabia</td>
<td>0.1547</td>
</tr>
<tr>
<td>Syria</td>
<td>0.9008</td>
<td>Thailand</td>
<td>0.1166</td>
</tr>
<tr>
<td>Bahrain</td>
<td>0.7421</td>
<td>Kuwait</td>
<td>0.0997</td>
</tr>
<tr>
<td>Tunisia</td>
<td>0.5832</td>
<td>Malaysia</td>
<td>0.0995</td>
</tr>
<tr>
<td>Egypt</td>
<td>0.5193</td>
<td>Indonesia</td>
<td>0.0957</td>
</tr>
<tr>
<td>Libya</td>
<td>0.3855</td>
<td>Turkey</td>
<td>0.0899</td>
</tr>
<tr>
<td>Morocco</td>
<td>0.3834</td>
<td>Iran</td>
<td>0.0869</td>
</tr>
<tr>
<td>Algeria</td>
<td>0.3617</td>
<td>India</td>
<td>0.0686</td>
</tr>
<tr>
<td>Sudan</td>
<td>0.3040</td>
<td>Philippines</td>
<td>0.0530</td>
</tr>
<tr>
<td>China</td>
<td>0.2542</td>
<td>Australia</td>
<td>0.0157</td>
</tr>
<tr>
<td>Pakistan</td>
<td>0.2419</td>
<td>Singapore</td>
<td>0.0076</td>
</tr>
<tr>
<td>Jordan</td>
<td>0.1702</td>
<td>Hong Kong</td>
<td>0.0067</td>
</tr>
<tr>
<td>Oman</td>
<td>0.1620</td>
<td>Japan</td>
<td>---</td>
</tr>
</tbody>
</table>

Initial analyses revealed that the relationship between the DPVC and the other variables of interest
was non-linear (curved) and the distribution of the DPVC was skewed right. This problem was resolved
by taking the natural logarithm of the DPVC before analysis. For simplicity, this logarithm of the DPVC
is referred to as LDPVC in this paper.

Freedom of information access was more challenging to measure because it encompasses many
factors (e.g., the availability of books, internet access, cell phone usage). When several variables jointly
measure one construct, one possible approach is examine each variable’s impact on the outcome of
interest independently, although inter-correlations among these related variables can make
interpretation challenging. Another approach is to combine the measures into one overall index or
variable. This can be done either by averaging the items or by creating a weighted score based on the
theorized or empirically derived relevance of each variable. Averaging the items requires the
assumption that all items are equally important in measuring information access. The process of
creating a weighted score, however, requires either more substantive theory than we currently have
available or a larger sample of countries than is realistically obtainable for the desired variables. Thus, for this study, we examined both the relationship of individual variables to the LDPVC and the relationship of the average to the LDPVC. This study includes the following twelve indicators of freedom of information access, each normalized onto a [0,1] scale. These variables, along with their values for each country, are ranked as follows:

<table>
<thead>
<tr>
<th>Country</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Libya</td>
<td>0.411</td>
</tr>
<tr>
<td>Iran</td>
<td>0.0685</td>
</tr>
<tr>
<td>Tunisia</td>
<td>0.1233</td>
</tr>
<tr>
<td>China</td>
<td>0.137</td>
</tr>
<tr>
<td>Syria</td>
<td>0.1507</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>0.1507</td>
</tr>
<tr>
<td>Yemen</td>
<td>0.1918</td>
</tr>
<tr>
<td>Sudan</td>
<td>0.2466</td>
</tr>
<tr>
<td>Oman</td>
<td>0.3151</td>
</tr>
<tr>
<td>Bahrain</td>
<td>0.3151</td>
</tr>
<tr>
<td>Morocco</td>
<td>0.3836</td>
</tr>
<tr>
<td>Singapore</td>
<td>0.3562</td>
</tr>
<tr>
<td>Algeria</td>
<td>0.411</td>
</tr>
<tr>
<td>Malaysia</td>
<td>0.4247</td>
</tr>
<tr>
<td>Jordan</td>
<td>0.4521</td>
</tr>
<tr>
<td>Egypt</td>
<td>0.4658</td>
</tr>
<tr>
<td>Thailand</td>
<td>0.4932</td>
</tr>
<tr>
<td>Kuwait</td>
<td>0.5342</td>
</tr>
<tr>
<td>Indonesia</td>
<td>0.5753</td>
</tr>
<tr>
<td>Turkey</td>
<td>0.589</td>
</tr>
<tr>
<td>Philippines</td>
<td>0.6301</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>0.8356</td>
</tr>
<tr>
<td>India</td>
<td>0.8356</td>
</tr>
<tr>
<td>Australia</td>
<td>0.9863</td>
</tr>
<tr>
<td>Japan</td>
<td>1</td>
</tr>
</tbody>
</table>

These indicators, of course, are to some degree representative of economic and industrial development, and not simply economic freedom. We remove much of the variance attributable to development for these indicators by controlling for the confounding factor, GDP. However, inferences about what the indicators represent should be made cautiously.

A further consideration is that many of these freedom of information access variables are highly correlated with other variables that predict state destabilization, such as the average age of the population. A statistically significant and large correlation between a freedom of information access variable such as cell phone usage, for example, may simply be attributable to the fact that cell phone users tend to be young and acts of violence within a country are more common among the young. Similarly, the correlation between phone lines, newspapers, or films and violence may be simply an artifact of increased wealth leading to a desire for more access to goods, and thus more unrest and violence. It is also possible that the connection between information access and instability is an

indirect result of the relationship of both variables with increased democracy, or is moderated by unemployment related stress. In other words, the correlation between the LDPVC and the access variables may be only spurious if potential confounding variables are not accounted for.

For this study, four potential confounding variables were included: GDP per capita,\(^{24}\) the proportion of the population ages 1-14,\(^{25}\) the unemployment percentage,\(^{26}\) and the Economic Intelligence Unit’s Democracy Index.\(^{27}\) Normalized indices for these confounding variables, by country, are given in the footnote below.\(^{28}\)

**Analytic Approach**

One approach to understanding the relationship between two variables, after accounting for one or more other variables, is the examination of partial correlations. Partial correlations are analogous to regression coefficients in a multiple linear regression but can be more interpretable when the strength of a relationship is of primary importance. A partial correlation is interpreted similarly to a bivariate Pearson correlation except that the partial correlation indicates the strength of a relationship after the relationship of another (or several other) variable has been accounted for. In this study, the partial correlation of each freedom of information access variable with the LDPVC was examined, after controlling for the four confounding variables.

The relationships of each indicator of freedom of information access with the LDPVC were examined one at a time rather than simultaneously (as is often done in multiple regression analysis) for several reasons. First, the sample was very small and thus the statistical power was limited. Second, the freedom of information variables themselves were highly correlated.\(^{29}\) If the entire set of variables

---

25 Id.
26 Id.
28 Countries by Control Variables (Normalized 1-0)

<table>
<thead>
<tr>
<th>Country</th>
<th>Mean</th>
<th>Min</th>
<th>Max</th>
<th>1-0</th>
<th>0-0</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDP per capita</td>
<td>0.687</td>
<td>0.510</td>
<td>0.618</td>
<td>0.000</td>
<td>1.000</td>
</tr>
<tr>
<td>Population Age 1-14</td>
<td>0.844</td>
<td>0.200</td>
<td>0.432</td>
<td>0.000</td>
<td>1.000</td>
</tr>
<tr>
<td>Unemployment Percentage</td>
<td>0.257</td>
<td>0.154</td>
<td>0.498</td>
<td>0.017</td>
<td>0.983</td>
</tr>
<tr>
<td>Economic Intelligence Index</td>
<td>0.284</td>
<td>0.220</td>
<td>0.352</td>
<td>0.019</td>
<td>0.981</td>
</tr>
</tbody>
</table>

(see next page)
were examined simultaneously in a multiple linear regression, or analogous correlational model, then problems of collinearity and multicollinearity would make coefficients unstable and inflate standard errors. In essence, both variables might appear unimportant if included in a model jointly because their shared relationship with each other might mask the effect each had with the LDPVC. On the other hand, examining relationships one at a time incurs the risk of assuming that one variable causes another when, truthfully, the variables may be related only through another variable not included in the estimation. In a correlational study, as presented here, however, causative claims are made cautiously, if at all. The goal is simply to examine the strength of relationships.

These relationships among variables are complex and interpretation will often be at the discretion of the analyst.

Findings

Visual examination using scatterplots of the relationships between the variables and the LDPVC suggest the presence of an outlier, Bahrain. Bahrain has unusual amounts of unrest given its access to

<table>
<thead>
<tr>
<th>Bivariate Correlations among Indicators of Information Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Literacy Rate</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Literacy Rate</td>
</tr>
<tr>
<td>Phone Lines</td>
</tr>
<tr>
<td>Cell Phones</td>
</tr>
<tr>
<td>Radio Stations</td>
</tr>
<tr>
<td>TV Stations</td>
</tr>
<tr>
<td>Internet Users</td>
</tr>
<tr>
<td>Number of News</td>
</tr>
<tr>
<td>Newspapers Circulation</td>
</tr>
<tr>
<td>Book Titles</td>
</tr>
<tr>
<td>Films Produced</td>
</tr>
<tr>
<td>Public Libraries</td>
</tr>
<tr>
<td>Freedom of the Press Index</td>
</tr>
</tbody>
</table>
information. This may be due to the fact that “The Sunni-led government has struggled to manage relations with its large Shia-majority population.”

Bahrain is a highly polarized society, with divided loyalties. Bahrain is also noteworthy because while it ranks first in cell phones, internet users, and number of news dailies, it rates much lower in such fundamental information variables as literacy, freedom of the press, book titles, movies produced, and public libraries (See Figure 4). In other words, except for newspapers (which lack freedom of the press), Bahrain’s pre-cell phone and internet information environment is relatively weak. As a result of social polarization and the disparity of information variables, Bahrain was removed from the analyses. Indeed, Bahrain, illustrates what happens in the Market for Loyalties, when monopoly control is lost (as a result of new technologies)—loyalty drops for the régime and new suppliers of identity may rush into the market.

Figure 4: Studied countries charted by logarithm of the Demonstrations, Protest, Violence and Civil War (DPVC) Index against the Average Access Index, which measures information environment variables

For the remaining 25 countries, partial correlations with LDPVC, after controlling for the four confounding variables, as well as bivariate correlations with LDPVC, were found for each access variable and the average of the access variables. Because this sample is not random and represents a

---

large proportion of all countries, p-values should be examined cautiously. It may be most appropriate, in fact, to focus on the size of the correlations rather than the p-values and limit inferences to the countries included in the study. As illustrated in the footnote, before adjusting for controls all access variables have moderate to large correlations with LDPVC, with the possible exception of the public libraries variable. After controlling for population age, unemployment, the democracy index, and GDP, at least four variables no longer have practically important correlations with LDPVC and all the correlations are smaller, as expected. Before adjusting for controls, all of the individual indicators of freedom of information access appear to have a moderate to strong relationship with LDPVC ($-.297 < r < -.772$). After adjusting for controls, about half the indicators continue to have at least a moderate relationship with the LDPVC ($r < -.200$).

Particularly surprising is the Freedom of the Press index. This variable is nearly perfectly correlated ($r = .890$) with one of the controls, the democracy index. The simple bivariate correlation of freedom of information access to Information Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Without Controls</th>
<th>With Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bivariate Correlation</td>
<td>Partial Correlation</td>
<td></td>
</tr>
<tr>
<td>p-value</td>
<td>p-value</td>
<td></td>
</tr>
<tr>
<td>Literacy Rate</td>
<td>-0.547</td>
<td>-0.035</td>
</tr>
<tr>
<td>Phone Lines</td>
<td>-0.714</td>
<td>-0.402</td>
</tr>
<tr>
<td>Cell Phones</td>
<td>-0.572</td>
<td>-0.329</td>
</tr>
<tr>
<td>Radio Stations</td>
<td>-0.42</td>
<td>-0.025</td>
</tr>
<tr>
<td>TV Stations</td>
<td>-0.397</td>
<td>-0.251</td>
</tr>
<tr>
<td>Internet Users</td>
<td>-0.749</td>
<td>-0.194</td>
</tr>
<tr>
<td>Score Number of News Dailies</td>
<td>-0.593</td>
<td>-0.416</td>
</tr>
<tr>
<td>Newspaper Circulation</td>
<td>-0.764</td>
<td>-0.287</td>
</tr>
<tr>
<td>Book Titles</td>
<td>-0.772</td>
<td>-0.276</td>
</tr>
<tr>
<td>Films Produced</td>
<td>-0.678</td>
<td>-0.368</td>
</tr>
<tr>
<td>Public Libraries</td>
<td>-0.297</td>
<td>0.078</td>
</tr>
<tr>
<td>Freedom of the Press Index</td>
<td>-0.639</td>
<td>0.024</td>
</tr>
<tr>
<td>Average Access Index</td>
<td>-0.856</td>
<td>-0.364</td>
</tr>
</tbody>
</table>
the press is large at $r = -0.639$. However, the partial correlation after adjusting for controls has dropped nearly to zero ($r = 0.024$). This is not surprising given the variable’s high correlation with democracy. Interpretation, however, becomes problematic. The results simply suggest that, once a country’s democratic index is accounted for, freedom of the press has no additional identifiable relationship with LDPVC. Within our studies there were no countries that were strong with respect to democracy and weak with respect to freedom of the press, or vice versa. Thus, it is difficult to separate the two constructs from each other. We simply can conclude that both variables are related to the LDPVC jointly. The other access variables in the model suffer from similar, though much weaker, relationships with the control variables. This high correlation between the Freedom of the Press Index and the Democracy index also impacts the partial correlation of the Average Access index with LDPVC. When a partial correlation is calculated that does not control for Democracy but does control for the other three confounding variables, we find a much stronger correlation of $r = -0.585$ ($p = 0.003$).

**Discussion**

Returning to Market for Loyalties theory, it predicts that states with greater freedom of information access should experience less destabilization as a result of events such as the Arab Spring. Specifically, the more new and substitute identities have been introduced into the Market for Loyalties, the more elastic the demand curve, until ultimately little disturbance is caused by the introduction of new identities. The assumption in this paper is the more diverse the information channels, the greater the number of identities introduced into the Market for Loyalties and the less shock from events, such as the immolations that touched off the Arab Spring. This study, however, measured destabilizing events—demonstrations, protests and violence—across an array of mostly Muslim countries. The findings of negative bivariate correlations (although weaker when controlling for GDP per capita, the proportion of the population ages 1-14, the unemployment percentage, and the Economic Intelligence Unit’s Democracy Index) among what can be called the free access of information variables suggests that indeed environments with freer access to information have more elastic Market for Loyalties, and hence they are more stable.

**Conclusion**

The conclusions that can be drawn from this non-random study of countries predominantly from the Muslim world are limited to that particular context, but they may be interpreted in light of Market for Loyalties Theory. It may be that the correlations would not manifest themselves in developed, Western countries, but according to Market for Loyalties Theory this would not be surprising if such countries had all attained relatively elastic identity demand curves.

It is also important to emphasize that the year of the Arab Spring was studied to highlight the destabilizing effects of the immolations across much of the Arab world. There were key event triggers that dramatically contributed to instability in many, if not most, of the Arab countries and some non-
Arab Muslim countries as well. This means our study may be fairly context specific even when limited to the Arab world.

Besides studying Muslim countries, it would be interesting to study the developing world in general to see if states with restrictions on access to technology proved to be less stable in the face of events such as those that inflamed the Arab Spring. It would also be interesting to see if concepts such as loyalty, identity, and instability in the market could be more precisely identified and measured, adding further credence to Market for Loyalties Theory.

In the final analysis, what do we know? We know that there is moderate correlation between instability as measured by LDPVC and our freedom of information variables, after controlling for GDP per capita, population distribution, unemployment, and the Democracy Index. Furthermore, Market for Loyalties Theory can offer an interpretation of the data. Perhaps freedom of information does promote stability after all. This is significant because the theoretical and empirical evidence may be supporting our most fundamental democratic value—suggesting that freedom of information, including freedom of speech, is not just a moral imperative, but sound policy.

In the beginning of this paper, we asked, “Are non-democratic regimes ‘better off’ by monopolizing and controlling the flow of information over new information channels?” Very cautiously, we suggest that the answer, at least within our very limited and imperfect study, may be “no.” We also asked, “Are democratic societies, particularly developing democracies, more stable when the flow of information over such channels is relatively unrestricted?” Again, qualifying our answer by admitting the limited nature of our study and the need for more research, we submit that the answer may be “yes.” These are important questions, and it is the authors’ sincere hope that others will take up this new inquiry for empirical and theoretical study.

Paul D. Callister is Professor of Law and Director of Library, University of Missouri-Kansas City School of Law.

Dr. Kimberlee C. Everson is Assistant Professor, Quantitative Methods, Department of Educational Administration, Leadership, and Research, Western Kentucky University.

32 “If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion or force citizens to confess by word or act their faith therein.” West Virginia State Bd. of Educ. v. Barnette, 319 U.S. 624, 642 (1943). See also United Nations, The Universal Declaration of Human Rights, art. 19, http://www.un.org/en/documents/udhr/ (last visited Dec. 9, 2013) (besides guaranteeing freedom of expression, guarantees freedom to “receive and impart information.”).
Privilege protections encourage full and candid communication between legal counsel and clients. These communications plainly serve a valuable role — but, protecting privileged communications during discovery can become one of the most time consuming and expensive elements of large-scale e-discovery projects. And, in many respects, the emphasis on computer-assisted review and cost containment during first- and second-line document reviews has largely outpaced the development of tools and techniques aimed at simplifying privilege review. Therefore, as with many e-discovery challenges, it is important to consider creative solutions to address privilege concerns. This article suggests certain approaches — before and during discovery — to help ensure that privileged materials are cost-effectively identified and protected.

Protecting Privilege During “Peace Time”

Protecting privilege starts before an investigation or litigation is even anticipated. Individuals within a company with access to sensitive information may not realize that sharing it over e-mail with colleagues leads to increased risk and cost if discovery arises. In addition, individuals may misunderstand the scope of privilege and engage in discussions that they incorrectly believe are protected from disclosure. Therefore, educating individuals with access to sensitive information concerning privilege protections is an important first step in situating an entity for an efficient and accurate privilege review.

This education should normally cover two points. First, individuals should understand the scope of privilege. To warrant privilege protections, a communication generally must be exclusively and confidentially shared between an attorney and a client (and the clients’ agents) for the purpose of securing a legal opinion, legal services, or assistance in some legal proceeding.¹ Some individuals may conflate privilege protections with the duty of confidentiality or be under the misimpression that merely copying an attorney on an e-mail is sufficient to establish privilege, even when the e-mail does not involve legal advice. However, privilege protections are different from, and largely more narrow than, the duty of confidentiality — which is a broader ethical obligation to preserve confidences. Further, simply copying an attorney on an e-mail may not itself be sufficient to establish privilege. In short, properly educating individuals on the scope of privilege will help prevent overshar ing sensitive information under the false impression that it is protected from disclosure.

¹ This article discusses privilege using principles that are generally applicable in United States federal court. However, it bears noting that the scope of privilege varies greatly based on the jurisdiction in which the protection is asserted — even within the United States.
Second, in addition to understanding the scope of privilege, individuals should be aware of various best practices that help to strengthen a claim of privilege and increase the likelihood that privileged material will be identified during a privilege review. The following list illustrates various practices that may help advance these goals:

**Label Communications**: Appropriately using the label “privileged and confidential” in e-mail messages will help flag the communication as privileged during collection and review. Importantly, however, such a label does not itself establish privilege, and overuse of this label on communications that do not relate to legal advice will lead to confusion during review and may dilute the claim of privilege. In addition, misuse of this label could lead to increased costs because any document with this label will likely require human review.

**Involve Outside Counsel**: Including outside counsel on e-mail communications discussing legal issues helps to bolster the claim of privilege (e.g., if outside counsel is involved, likely the communication involves legal advice) and assists in flagging the e-mail during a subsequent privilege review (e.g., any e-mail involving an e-mail address ending with a domain name associated with a law firm has a high likelihood of containing privileged material).

**Keep it Separate**: Avoid comingling business and legal advice. The involvement of a lawyer in discussions will not necessarily create a privileged communication if the lawyer is not providing legal advice or acting in his or her role as an attorney. Mixing business and legal discussions can make it more difficult to identify communications as privileged during the review and encourages distribution to individuals to whom privilege protections may not apply.

**Limit Distribution**: Limit written communications seeking legal advice to those who need to know the contents, and consider explicitly stating why an individual is included (e.g., “John Smith is included because he is a senior manager with a relevant functional responsibility”). This practice helps establish that the purpose of the communication was limited to seeking legal advice and helps ensure that custodians who may be unlikely to possess privileged materials (and therefore may receive limited attention during a privilege review) are not the recipient of a one-off privileged communication that could be inadvertently produced.

**Use the Telephone**: Sometimes picking up the telephone is the best solution to preserving privilege. Indeed, one of the reasons there has been an increase in privilege issues in e-discovery is the proliferation of written communication. Often discussions between attorneys and clients that would have been handled over the telephone are now conducted through e-mail messages, which have no limit to the number of individuals who receive the initial message or are subsequently forwarded copies. This “use the telephone” approach frequently becomes particularly important with multinational corporations that operate in numerous jurisdictions, some of which have relatively weak protections.
By educating individuals on the scope of privilege and best practices during “peace time,” a company may be better positioned to preserve privilege when discovery begins. In the end, however, no amount of education will perfectly position a company to identify and exclude privileged material during discovery. As a result, it is important to develop a cost-effective discovery plan that minimizes the potential for inadvertent production of privileged material.

**Reducing Costs and Protecting Privilege During Discovery**

Once an investigation or litigation commences, attorneys should work with their client to develop a discovery plan that addresses the privilege review and ensures reasonable steps are taken to identify and protect privileged materials. In addition to ensuring that discovery deadlines are met and costs are contained, a discovery plan may be critical for “clawing back” inadvertently produced privileged material. Under Federal Rule of Evidence 502, a party may “claw back” inadvertently produced privileged material when it has taken “reasonable steps to prevent disclosure” and acts to promptly rectify the error.\(^2\) A discovery plan that is well-documented and tested will allow parties to demonstrate to a court that it took reasonable steps to identify and protect privileged information. That said, while the importance of a discovery plan that addresses privilege is clear in the abstract, creating such a plan can be difficult — especially in light of rapidly-changing technology.

The well-settled and often accepted approach to privilege review relies on using keyword searches to identify potentially privileged material. The keywords normally focus on words that are commonly associated with privileged material (e.g., “privileged and confidential,” the name of in-house attorneys) or web domains associated with e-mail addresses of individuals who commonly engage in privileged discussions (e.g., the web domain for outside counsel). So long as the search terms are reasonably comprehensive, likely to capture privileged material, and tested by appropriate sampling, courts will generally accept this approach.\(^3\) Nevertheless, this traditional approach can be time consuming and expensive, especially because search terms must be crafted, results refined, and hits reviewed by attorneys.

Therefore, in light of the growing emphasis on increased efficiency and cost containment, there has been increased focus on using predictive coding technologies to conduct a privilege review. In addition to relying less on human review (thereby reducing associated costs), the algorithms used with predictive coding can adapt to natural variations in human language and may allow for a more comprehensive and accurate privilege review. For instance, rather than rely on specific search terms

\(^2\) See Rule 502(b).

\(^3\) See, e.g., *Jacob v. Duane Reade, Inc.*, No. 11 Civ. 0160(JMO)(THK), 2012 WL 651536, at *4 (S.D.N.Y. Feb. 28, 2012) (holding that preparation of attorneys’ names whose communications could be privileged, use of search filters, and quality control reviews was reasonable); *Mt. Hawley Ins. Co. v. Felman Prod., Inc.*, 271 F.R.D. 125, 136 (S.D.W. Va. 2010) (finding failure to perform simple keyword searches and test the reliability of keyword searches was not reasonable).
that only capture precise matches, predictive coding may recognize privileged material based on the context of a communication and other information from the entire data set.

That said, predictive coding technology has not developed as rapidly in the privilege context as compared to its use in other contexts and some drawbacks remain. For instance, because the amount of privileged material compared to the data set as a whole is often relatively small, it can be difficult to create a strong seed set of privileged documents. Added complications may arise if the data set contains foreign language materials because cultural and linguistic differences will be amplified in a small seed set, making it more difficult to create a strong sample of privileged documents on which the algorithm can rely. In light of these potential concerns, it may be advisable to turn to well-established techniques to verify the results of a computer-assisted privilege review. For example, after deploying predictive coding during a privilege review, it may be advisable to run searches for certain words (e.g., “privileged and confidential,” names of in-house counsel) and domain names (e.g., searching for e-mail addresses from outside counsel) to verify that the documents the computer-assisted review identified as non-privileged do not contain privileged materials.

Although a hybrid approach that combines predictive coding and traditional search tools may be the best current practice in some instances, it is likely only a matter of time before predictive coding is the primarily (and potentially only) tool deployed during a privilege review. Indeed, federal courts have already approved the use of computer-assisted privilege reviews.⁴ For instance, the Tax Court recently approved the use of predictive coding for identifying non-privileged documents.⁵ The court explained that “[p]redictive coding is an expedited and efficient form of computer-assisted review that allows parties in litigation to avoid the time and costs associated with the traditional, manual review of large volumes of documents.”⁶ In allowing predictive coding, the court noted that the petitioner wanted to use this technology to conserve time and costs and represented that it would retain e-discovery experts to meet with and conduct a search acceptable to opposing counsel.⁷ Notably, another federal court has taken it a step further and suggested that the exclusive use of this technology may be mandatory in privilege reviews. Specifically, in Green, the court warned that if the defendants did not meet their discovery deadlines, the court’s Rule 502(d) order could be amended to prohibit any human review of privileged materials and require only the use of computer-assisted review.⁸

Whether traditional search terms, predictive coding, or a combination of the two are used to perform a privilege review, a privilege log generally must be created to identify the withheld materials. This second step in the privilege review process has historically imposed significant cost, as creating the

---

⁵ See Dynamo Holdings Ltd. P’Ship v. Commissioner, 143 T.C. 9 (2014), Id. at 4.
⁶ Id. at 5.
traditional document-by-document privilege log can be an incredibly time-intensive and resource-consuming effort. Categorical privilege logs have emerged as a way to improve the traditional privilege log. These logs group documents and describe them in categories, instead of individually. Categories may include communications exclusively between a party and its trial counsel and work product created by trial counsel, or non-party agents after action commencement. Use of these categorical privilege logs is becoming more mainstream, with more courts recognizing their advantages. And, some local and court rules across the nation endorse this approach. Combined with an efficient discovery plan that appropriately harnesses available technology during the privilege review, these categorical privilege logs can often be an important element in efforts to accurately and cost-effectively assert privilege claims.

Conclusion

With the proliferation of electronic communications, ensuring that privileged communications remain protected during discovery is becoming one of the most important and expensive elements of e-discovery projects. As technology continues to develop in this area, it is important for attorneys and their clients to consider creative solutions — both before and during discovery — to harness available technology and take advantage of other solutions to ensure that privileged materials are cost-effectively identified and protected.

Allen Kathir (akathir@cov.com) is a litigation associate at Covington and Burling, LLP and a member of the firm’s E-Discovery Practice Group. Alexander Hastings (ahastings@cov.com) is a government contracts and litigation associate and a member of the firm’s E-Discovery Practice Group. Edward Rippey (erippey@cov.com) is a partner at the firm, handles complex commercial litigation, and is Chair of the E-Discovery Practice Group.

---

Financial institutions have long been especially lucrative targets for insider attacks, but with the computerization of firm systems and assets, attacks can now be launched on a grander scale than ever before. Insider attacks on firms’ electronic systems can result in financial and intellectual property theft, damaged or destroyed assets, and firm-wide disruption to internal systems and customer operations. Preventing and detecting attacks, however, has proven to be difficult, as insiders are often able to capitalize on their familiarity with firm systems to launch attacks without attracting notice. A systemized, targeted program is therefore necessary to combat insider threat risks.

The core components of an insider threat mitigation program mirror those denoted in the National Institute of Standards and Technology (NIST) Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. This structure encourages firms to individually assess threats most relevant to their firm and to develop a risk-based approach to resource allocation. The structure is also flexible enough to allow firms to scale implementation based on their business models and available resources.

However, unlike in a general cybersecurity program, each component in an insider threat mitigation program has a distinctly human element. While external cybersecurity threats can usually only be prevented or detected through technical tools, insider threats commonly exhibit human behaviors that foreshadow the attacker’s intent. An appropriately trained insider threat mitigation team can leverage technical tools, such as network monitoring software, and counterintelligence skills to detect and investigate suspicious insider behavior. While all personnel in a firm have a role in maintaining an effective insider threat program, an insider threat mitigation team is essential to coordinate firm-wide prevention efforts and alert relevant personnel to suspected or detected threats. Best practices for insider threat mitigation therefore involve both technical cybersecurity defenses, which typically reside within information technology, and human expertise, that resides across the firm.

While sophisticated monitoring tools and personnel screening techniques are critical in ensuring the effectiveness of an insider threat mitigation program, they are not without legal risk. Although privacy and employment laws in the United States are generally permissive of employers’ efforts to protect their assets, electronic communications privacy laws and background check restrictions at the state and federal level impose some procedural hurdles. Laws abroad – particularly in the European Union – are more restrictive, and in some cases may prohibit employers from taking certain insider threat precautions. Firms should therefore use the framework within this document
as a starting point, but must also consult with local counsel throughout the development and implementation of an insider threat program.

I. Mitigating the Insider Threat

Losses and damage caused by “insiders,” such as employees, contractors, and others authorized to access business information and systems have long been a problem for businesses in virtually every industry. The recent Edward Snowden incident demonstrates that even the most secure organizations can face devastating losses caused by a knowledgeable and motivated system administrator who is not contained by adequate internal safeguards or sufficiently rigorous administrative standards and expectations. In response, the National Security Agency (NSA) cut back the number of system administrators by 90%, imposed a “buddy” system for certain access, and disciplined NSA personnel who shared their passwords with Snowden.¹

Historically, insider activities at financial institutions most often involved employees who abused their access privileges or committed fraud to steal funds from customer accounts or the firm. However, because firms’ operations and assets have been so thoroughly computerized, insider attacks on systems and networks are now a significantly greater threat than seen in the past. The most serious insider threats in the digital age—and those that firms should prioritize and invest the most resources to prevent—involve individuals who misuse their access to systems, networks, and information in a manner that compromises the confidentiality, integrity, functionality, reliability or availability of those systems, networks, or information. The results of inadequate protections can be loss, alteration, or destruction of a firm’s operational capabilities, as well as material loss of customer data, business records or intellectual property.²

Despite their technical modality, insider threats are, at their core, a human issue. Cybersecurity defenses focused on monitoring employee activities may prevent some attacks from causing significant harm to an organization, but human intelligence, monitoring and good management oversight are necessary to identify the potential warning signs of insider activity and the appropriate method to intervene before an attack occurs and mitigate the effects if an attack does take place. An effective insider threat program, therefore, uses both cybersecurity defenses and designated intelligence personnel to detect and contain insiders who pose a risk to the firm and mitigate the risk through administrative, investigative, technical or disciplinary safeguards and responses.³

**Who are the insiders?**

An insider is any individual with the ability to access an organization’s internal systems and resources. However, individuals who have intentionally carried out insider attacks tend to have similar motivations. Financial gain has always been a popular motivator, made all the more appealing by digitized systems that lend themselves to stealing vast quantities of customer data or intellectual property (“IP”) assets to aid larger fraud schemes. Other insiders, motivated by malice against employers or a desire to seek revenge, seek to disrupt, undermine or destroy company systems. Still others work on behalf of other entities, seeking to steal or destroy data to help the entity gain a competitive advantage or to harm the victim company’s interests or reputation.

A number of studies have also noted that perpetrators of insider attacks share common characteristics. For instance, one study found that 80% of insiders who stole confidential or proprietary information were male and over half held technical positions. Other studies have attempted to identify the psychological traits prevalent in insider spies. However, other surveys of insider threat case studies have suggested that insiders do not fit any particular demographic or occupational profile. This lack of an agreed set of characteristics makes it difficult to uniformly apply a set of rules for insider threat discovery.

Moreover, using such traits to profile insiders carries some degree of legal risk, particularly in EU member states that restrict automated decision-making based on such profiles. Therefore, firms should carefully weigh the legal risks of this type of profiling against its potential benefits before adopting it as a practice in their insider threat mitigation programs. Indeed, almost all efforts to identify and deter insiders from engaging in malicious activities will involve substantial legal issues – as well as considerations of company morale and cohesiveness. The bottom line is that an employee can become an insider threat from almost any background or starting point.

**Understanding the Investigative Challenge of Insider Threats**

Surveys of insider case studies reveal that individuals’ concrete behaviors, rather than their demographic or psychological characteristics, are often the best indicators of their risk of being an insider threat. Suspicious behaviors can manifest themselves both as network security violations (e.g., failed log-in attempts, downloading large amounts of data, altering coding on sensitive files) and as personnel issues (disputes with co-workers or superiors, threats, chronic absenteeism). To

---

monitor for both types of behaviors, firms should utilize network monitoring software and implement reporting mechanisms for employees and supervisors to report suspicious activity.

Network monitoring software is a critical tool for detecting internal and external cyber threats, but it is useful only to the extent that key staff can properly interpret the data it generates. To decide what kinds of patterns are anomalous and therefore potentially suspicious, the firm must first establish a network activity baseline. An individual familiar with the company’s network usage should observe network activity over a given period of time and document all relevant data points, which may include communications between devices within the firm, virtual private network (VPN) users, ports and protocols, firewall alerts, printing activity, and bandwidth usage.

Once a baseline is established and the monitoring software is implemented, designated members of the insider threat team should monitor the network for anomalous activity, such as unfamiliar IP addresses attempting to access the network, unusually large data transfers, failed log-in attempts, and large printing jobs or data transfers of privileged files. If a team member identifies anomalous activity, he or she should first investigate to see whether a legitimate explanation for the activity exists (e.g., forgotten passwords or training activities requiring printing of privileged materials). If no legitimate explanation is uncovered, the team member should consult with the full insider threat team to discuss whether further monitoring or an expansion of the investigation is warranted.

While an insider threat team can rely on software to monitor network activity in real time, it must rely on the firm’s employees (managers and co-workers) to continuously monitor for personnel issues that may signal an insider threat risk. Firms should therefore develop an Insider Risk Mitigation Policy and corresponding training and awareness programs for all personnel. The Policy should explain how personnel can avoid creating security vulnerabilities, such as keeping user credentials private, logging off all networks before leaving a device unattended, and restricting access to any sensitive files that they create.

The Policy should also clearly set forth the consequences for perpetrating, or assisting in the perpetration of, an insider attack. In addition, employees should receive training on how to identify indicators of insider threat risks. Such training should stress the importance of reporting any suspicious behavior, policy violations, personnel conflicts or any other signal of an insider threat risk, and describe the confidential and, in jurisdictions where it is permitted, anonymous mechanisms for reporting, such as whistleblower hotlines. Information from the Policy should be incorporated into training for new employees, and the firm should send periodic reminders of employees’ duty to safeguard against and report threats.

Putting the policy and human component together with network and system monitoring into a single holistic model is one of the key challenges of building an effective program. The model described below and represented in the associated graphic is one possible way of structuring a predictive
model that combines psychosocial and tradition cyber data to raise red early flags for further analysis. The confidence level that a firm puts in the predictive accuracy of the model will vary depending on the indicators captured, the ability of managers to correctly assess their employees and how well malicious insiders are able to hide their true actions. In addition, prioritization is a key concept within the model as not all possible data can be collected continuously, and some (e.g., HR records) may not be available in real time, hence firms need to adopt an incremental approach to data collection, analysis, and decision making in which different data are collected and analyzed for different individuals depending upon their position and insider threat risk determined by the model.  

**Structuring an Insider Threat Mitigation Program**

While it may be virtually impossible to completely eliminate insider attacks, an insider threat mitigation program can greatly reduce their prevalence and impact. As previously mentioned, cybersecurity defenses alone cannot adequately protect against insider threats. Rather, successful programs take a holistic approach involving a combination of technology, legal, policy, physical security, awareness and training, and counterintelligence resources. Senior representatives from these various functions can serve as members of an insider threat “working group” that can provide governance, oversight and direction that accounts for the business model of the firm and all the functions that it performs. Although distinct from the insider threat team, which should be solely responsible for conducting insider threat investigations and routine monitoring, the working group should be consulted when developing new insider threat policies or responding to detected threats. Not surprisingly, this kind of integrated approach is most effective when it is allocated sufficient personnel, technology, and financial resources; therefore, visibility of the program to, and support from, top-level management is also essential.

The location of an insider threat team within an organization can vary. While some maintain a counter-intelligence unit, others create teams within their human resources or cybersecurity units. While structures can vary, it is the unit’s separate identity that that is most important. Because insider threats may arise at all levels and throughout all functions of an organization, this separation enables an insider threat team to conduct independent, unbiased investigations. That being said, it is important to reiterate the critical point that the organization responsible for addressing the insider threat is able to call on the capabilities of other functions within the firm to accomplish its mission, such as information technology (“IT”) for system activity monitoring, human resources (“HR”) for background checks, and line managers for behavioral monitoring.

---

The insider threat team should also facilitate communication across different functions within the firm. Too often, individual units will respond to suspicious insider behavior in isolation: for example, a report that an employee angrily confronted a supervisor would typically be referred to HR, which may intervene or continue to observe the employee for signs of escalation of the dispute. However, heightened HR monitoring alone would not detect suspicious network activity that could signal an imminent insider attack. In this case, an insider threat team should be notified to ensure comprehensive monitoring by IT, security, and other relevant departments has been implemented. This coordinated, interdisciplinary approach ensures that threats are promptly addressed by both the insider threat team and the associated supporting functions no matter how they manifest.

Personnel assigned to insider threat mitigation are obviously not immune from posing an insider threat risk themselves. Organizations must therefore establish internal controls to maintain the integrity of their insider threat program. The firm should designate personnel to oversee the proper handling and use of records concerning the insider threat program, and to ensure that records generated by the program are accessible only on an as-needed basis. Senior personnel should be responsible for regularly scheduled compliance reviews to ensure that program staff are following the insider threat policy guidelines and any applicable legal, privacy and due process/civil liberties protections. The results of these reviews should be reported by internal audit staff to senior management and/or the Board to ensure they are involved, aware, and that issues are resolved in a timely manner. To prevent unwarranted invasions of privacy, senior management should develop special access procedures for extremely sensitive information that might be sought in insider threat investigations, such as law enforcement records or records from past investigations.

**Implementing an Insider Threat Mitigation Program**

Although developed as an aid for cybersecurity defense programs, the National Institute of Standards and Technology (NIST) Cybersecurity Framework’s “core” components – Identify, Protect, Detect, Respond, Recover – are a useful framework for implementing an insider threat mitigation program and can also serve as a consistent set of terms for communication and integration into a firm’s enterprise risk management program. The principles of taking a risk based approach, which is threat informed, based on the resources available and supportive of the overall business model of the firm hold true whether creating or improving a cybersecurity program or an insider threat mitigation program.

An insider threat program cannot be developed by the firm in a vacuum, however. Because insider threat prevention and detection necessarily require some degree of intrusion into insiders’ background and work habits, firms must take into account privacy and employment laws when developing program policies and procedures. Workplace risks stemming from insider programs may be even more pronounced in jurisdictions with more prescriptive privacy protection laws, such as
the EU. In the U.S., legal concerns and potential litigation involving defamation, retaliation or wrongful termination are also important factors to consider.

Regarding implementation steps firms can take to put the core elements of this document into practice, we suggest firms follow an approach similar to what is described in the NIST Cybersecurity Framework. The steps outlined for prioritization, scoping, assessing, and improving a cybersecurity program are universal—as is the application of a continuous improvement process that is critical to keeping security and risk programs fresh and relevant. In addition, as firms implement the NIST Cybersecurity Framework many of the steps will repeat and overlap with other risk practices. Below are the seven steps, modified slightly to call out key items specific to insider risk, that firms should follow in putting the core elements of this document into practice.

**Seven Steps**

1. **Prioritize and Scope:** The organization identifies its business/mission objectives for its insider threat program, high-level organizational priorities and associated risk tolerances.

2. **Orient:** Once the scope of the program has been determined for the business, the organization identifies related systems and assets, regulatory requirements, legal constraints and overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets.

3. **Assess Current State:** The organization develops a current state for their insider threat program.

4. **Conduct a Risk Assessment:** The organization analyzes the operational environment in order to discern the likelihood of an insider driven event and the impact that the event could have on the organization.

5. **Create a Target State:** The organization develops a future state for their insider threat program.

6. **Determine, Analyze, and Prioritize Gaps:** The organization compares the current state to the future state to determine gaps. Next it creates a prioritized action plan to address those gaps that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the target state.

7. **Implement Action Plan:** The organization determines which actions to take in regards to the gaps identified in the previous step. It then monitors its current practices against the target state.

---

This is only meant to provide a general framework for implementing an insider threat mitigation program. Outside experts can provide more tailored, detailed assistance and feedback. In addition to private consultants, there are a number of non-profit and government resources that can provide assistance. The CERT Insider Threat Division of the Software Engineering Institute at Carnegie Mellon University, a federally funded research and development center, hosts workshops on developing insider threats, works with organizations on program development, and provides training and certification courses to insider threat program managers and assessors. More information can be found at http://www.cert.org/insider-threat/products-services/index.cfm. The Department of Homeland Security (DHS) and Department of Defense (DOD) also offer shorter awareness courses on protecting critical infrastructure against insider threats; for more information, contact the National Cybersecurity and Communications Integration Center Analysis team at NCCIC@hq.dhs.gov.

II. Legal Risks

Although insider threat mitigation programs can protect firms from potentially crippling theft and system damage, they may also expose firms to some legal risk. In the United States, firms’ monitoring practices are subject to the Electronic Communications Privacy Act (ECPA) at the federal level, as well as various state privacy and tort laws. While these laws generally contain exceptions that may permit workplace monitoring, such exceptions are often predicated on providing sufficient notice of monitoring practices. The Fair Credit Reporting Act (FCRA) also restricts the allowable scope of background checks on prospective employees. Other countries, particularly those in the European Union, more stringently regulate workplace monitoring and background checks. This section details the primary laws that may be applicable to an insider threat program in the United States. There may be other applicable laws and/or applicable regulations depending on the relevant facts and circumstances.⁹

A. Electronic communications monitoring

1. Federal law

The primary federal law governing electronic communications privacy in the US is the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510 et seq. Title I of the ECPA, also known as the Wiretap Act, prohibits the intentional “interception” and disclosure of wire, oral, and electronic communications, including email and telephone conversations, unless one of the Act’s exceptions apply. § 2511(1)(a). Courts generally interpret the term “interception” as the acquisition of communications contemporaneously with their transmission; thus, the restrictions of Title I apply to real-time monitoring programs, such as web traffic monitors and keystroke loggers.¹⁰

---

⁹ This article is not intended to provide and should not be construed as providing legal advice. Prior to instituting any insider threat mitigation program, companies should engage in a thorough legal analysis and with their own legal counsel.
¹⁰ See, e.g., United States v. Steiger, 318 F.3d 1039, 1048-49 (11th Cir. 2003).
Real-time monitoring can be potentially lawful under two exceptions to Title I of ECPA. Under § 2511(2)(a)(i), known as the “service provider exception,” it is not unlawful for a “provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service.” While few courts have closely interpreted this exception, it is generally understood that it permits employers that provide employees with internet and email service to monitor those services to the extent that they are used in the ordinary course of the employers’ business.

Employers that provide internet or email service through a third party, or those that wish to monitor internet use that falls outside of the ordinary course of business, may wish to rely instead on the “consent exception.” The consent exception allows the interception of communications where at least one party to the communication consents to the interception, and the communication is not used to commit a crime or tort. § 2511(2)(d). Although courts have disagreed as to the definition of “consent” in the absence of explicit warnings or policies about monitoring, they have consistently agreed that employees consent to monitoring when memorialized policies or banners on web browsers permit it.11

**Firms can therefore help protect themselves against potential liability under Title I of ECPA by developing a network use policy that clearly provides for the possibility of monitoring and requiring employees to provide their written consent to the policy.**

The Department of Justice has suggested that a banner notice on business-owned computers warning that network activity is subject to monitoring may be the most effective way to “generate consent to real-time monitoring” and “the retrieval of stored files and records pursuant to ECPA.”12

Title II of ECPA, also known as the Stored Communications Act (SCA), prohibits intentionally accessing communications in electronic storage without, or in excess of, authorization. 18 U.S.C. § 2701(a). Although courts have disagreed on the meaning of “electronic storage” as used in the SCA, for compliance purposes firms should consider all emails to be potentially within the statute’s scope. Firms that provide their own email services to employees, however, may access emails stored in work-provided accounts under an exception allowing access authorized by the entity providing the

---

11 See, e.g., United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002) (professor had consented to monitoring where university’s network use policy provided for periodic network monitoring); United States v. Greiner, 2007 WL 2261642, at *1 (9th Cir. 2007) (employee deemed to have consented to monitoring of remote network use where warning banner provided for monitoring).

email service. § 2701(c)(1). It is unclear, however, whether this “provider exception” applies to firms that use a third-party email provider. Therefore, such firms can further shield themselves from liability by obtaining employees’ consent to access stored emails. § 2701(c)(2).

As with the consent exception to Title I, firms should disclose their email access policy to employees and obtain their signed agreement to the policy. Employers should not, however, attempt to access employees’ private, web-based email accounts – by guessing passwords or otherwise – as courts have found that such efforts violate the SCA.

2. State Law


Nearly every state has enacted a law analogous to the federal Wiretap Act. While most state wiretap statutes mirror the federal law’s requirements and exceptions, a dozen states – California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania and Washington – require the consent of all parties to a communication for monitoring to be legal under the statutes’ consent exceptions. In theory, a firm could violate all-party consent wiretap statutes if it intercepts messages received by an employee from a third party who was not warned of the monitoring. However, the state courts that have considered the issue have interpreted their respective statutes to allow such interceptions. A court in Washington, for instance, noted that “A person sends an e-mail message with the expectation that it will be read and perhaps printed by another person….that person thus implicitly consents to having the message recorded on the addressee’s computer.” A Massachusetts court also dismissed a wiretap act claim brought against an employer, reasoning that the employer’s email monitoring was not unlawful because it was in the “ordinary course of business.”

Accordingly, while firms may wish to protect themselves against claims under all-party consent wiretap statutes by including a monitoring warning in all emails sent from company email addresses, such statutes may not pose significant legal risk in this context.

---

13 See also Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2003) (holding that an employer’s search of email stored on its own system fell within the service provider exception of § 2701(c)).
Most states recognize the tort of intrusion upon seclusion, which generally impose liability for intentional intrusions upon the plaintiff’s solitude or private affairs that would be highly offensive to a reasonable person.\textsuperscript{17} A number of plaintiffs have attempted to bring intrusion upon seclusion actions against employers for electronic monitoring, but the vast majority are unsuccessful because of the tort’s requirement that the employee have “an objectively reasonable expectation” of privacy in the place of intrusion.\textsuperscript{18} To bolster these defenses, however, employers should ensure that their notices of electronic monitoring are sufficiently clear and publicized such that employees cannot claim that they have a reasonable expectation of privacy in their online activities or telephone conversations in the workplace.

B. Background Checks and Screening

Criminal background checks, and to some extent, financial background checks, have long been a routine part of the hiring process at most firms. As individuals have increasingly shared information about themselves online, some firms have also begun to incorporate online searches into their screening processes as well. Taken together, background checks and screening can uncover information critical to determining whether a prospective employee poses an insider threat risk. However, the scope of such screening is not unlimited – federal and state laws in the United States regulate the gathering of information about certain aspects of candidates’ backgrounds. The following is a brief summary of laws and regulations that restrict what information employers can investigate in screening prospective employees.

1. \textit{The Fair Credit Reporting Act (FCRA)}

A candidate’s financial history may be indicative of not just his or her character, but also his or her propensity to commit insider theft or fraud. Employers may therefore wish to obtain a consumer report or an investigative consumer report about a prospective employee. In the United States, the procurement of such reports is governed by the Fair Credit Reporting Act (FCRA). Although FCRA only applies to consumer reports obtained from consumer reporting agencies (CRAs), some states – most notably California\textsuperscript{19} – impose similar restrictions for investigations conducted in-house as well.

\textit{Employers will therefore minimize their risk exposure by complying with FCRA standards for all types of financial background investigations and screening.}

\textsuperscript{17} See Restatement (Second) of Torts § 652A (1977).
\textsuperscript{18} \textit{Shulman v. Grp. W Prods., Inc.}, 955 P.2d 469, 490 (1998). Courts have also almost uniformly found that workplaces are not sufficiently private spaces for an intrusion upon seclusion to occur. \textit{See, e.g.}, \textit{Marrs v. Marriott Corp.}, 830 F. Supp. 274, 283 (D. Md. 1992); \textit{People for the Ethical Treatment of Animals v. Bobby Berosini, Ltd.}, 895 P.2d 1269, 1282 (Nev. 1995) (stating that “there is, generally speaking, a reduced objective expectation of privacy in the workplace”).
\textsuperscript{19} See, \textit{e.g.}, Investigative Consumer Reporting Act (ICRAA- CA Civil Code §1786. In some instances, the California law is broader than FCRA. Firms operating in California should consult local counsel to develop a background check policy.
FCRA does not generally restrict what information may be obtained in background checks, but rather how it is obtained. The law applies to any information obtained in a consumer report, which is broadly defined as “any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living. . . .” 15 U.S.C. § 1681a(d)(1). An employer must provide a clear, conspicuous, written notice to an applicant or current employee, and obtain his or her consent, to get a report. § 1681b(b)(2). Notice and consent to an applicant can extend to reports obtained throughout the course of employment, if the notice clearly states so. This type of “blanket authorization” may prevent the problem of disgruntled insiders acting out upon receiving notice that the employer has requested their consumer reports.

Should the firm decide to deny employment based on the contents of the report, it must inform the applicant of its decision in a “pre-adverse action” letter, and upon finalization of the decision, a second letter explaining the applicant’s rights, including the right to dispute the report with the CRA and the right to request a re-investigation. §§ 1681m(a); 1681b(b)(3). The FTC has also advised that applicants should be given a reasonable opportunity to review and discuss the report between when the first and second letters are sent.

Investigative consumer reports, though more onerous to obtain, may reveal even more information about a job candidate or employee. In addition to the information included in consumer reports, investigative reports contain information obtained from interviews with neighbors, friends, associates, or acquaintances of the report subject. FCRA imposes extra requirements for such reports: notice must be provided within three days after a report is requested, § 1681d(a)(1)(A), and must include a summary of the individual’s rights under FCRA. § 1681d(a)(1)(B). Additionally, upon a timely request, the employer must provide a complete and accurate disclosure of the nature and scope of the investigation. § 1681d(b). Although there are no prohibitions against obtaining blanket authorizations from prospective employees to procure investigative reports in the future, such authorizations carry greater practical compliance risks, as they may not sufficiently describe the “nature and scope” of future investigations or give meaning to a future employee’s rights.

Notably, however, the Fair and Accurate Credit Transactions Act of 2003 (the “FACT Act”) amended FCRA to allow employers to hire outside investigators to conduct investigations into certain types of employee wrongdoing. The amended FCRA provision exempts communications that would otherwise be “investigative consumer reports” from the notice requirements for such reports if the purpose for the communication is to investigate suspected misconduct related to the employer or to comply with federal, state, or local laws; rules of a self-regulatory organization; or any preexisting

---

21 FTC Staff Opinion Letter, Lewis (05-11-98).
written policy of an employer. 15 U.S.C. § 1681a(y)(1). However, to qualify for this exemption, the report must not be made for the purpose of investigating creditworthiness, and it cannot be provided to any person except the employer, the government, a self-regulatory organization, or as required by law. Id. However, if an employer takes adverse action based on this type of report, it must provide the affected employee with a summary of the nature and substance of the report, although it need not disclose its sources of information. § 1681a(y)(2).

2. **EEOC Guidance on the Consideration of Criminal History**

While no law forbids the consideration of an individual’s criminal history in making employment decisions, the Equal Employment Opportunity Commission (EEOC) has issued guidance stating that such consideration may violate Title VII of the Civil Rights Act of 1964, because national data suggests that criminal history exclusions have a disparate impact on certain racial and ethnic minorities.\(^{22}\) The Guidance provides that a policy of excluding applicants based on their criminal histories violates Title VII unless such exclusion is “job related and consistent with business necessity,” based on the nature and gravity of the crime, the time elapsed since the crime was committed, and the nature of the job. Moreover, where such screening is used, employers must provide an opportunity for the individual to demonstrate exclusion should not be applied to his or her particular circumstances. The Guidance also takes the position that arrest warrants cannot justify exclusion unless the conduct underlying the arrest renders the individual “unfit for the position in question.”

Recently, the EEOC has brought enforcement actions against two large employers for failing to provide robust, individualized assessments for those excluded by criminal history screening policies.\(^{23}\) Although the outcome of these cases has yet to be determined, and some states and entities are challenging the agency’s policy of requiring individualized assessments, for the time being firms must weigh the benefit of criminal screening for the job in question with the potential risks of violating Title VII.

*Firms may want to strike this balance by limiting their exclusion policies to crimes that could cause harm to the firm—such as cybercrime, fraud, insider trading, or theft—and provide excluded individuals with an opportunity to contest the exclusion.*

---


3. **Social Media**

While examining publicly-available social media profiles can be an informative part of applicant screening, firms should be mindful that nineteen states have enacted laws prohibiting employers from forcing applicants or employees to reveal their personal, private profiles. Such legislation prohibits employers from requiring and/or requesting employees or applicants to 1) disclose a user name or password from a personal social media account, 2) “friend” an employer, 3) access their personal profiles in the presence of an employer, and/or 4) change their privacy settings to allow employers to view a profile.\(^{24}\) A majority of these laws permit state agencies to fine non-compliant employers, and some create a private right of action for affected individuals.\(^{25}\)

*Accordingly, firms should instruct human resources and other personnel responsible for hiring to use only publicly-visible online information to screen job candidates and check up on current employees.*

All but three of these laws, however, contain language clarifying that the laws do not prohibit employers from complying with federal, state, or self-regulatory organization (SRO) obligations to screen employees. The three states that do not contain this limitation – California, Colorado, and Maryland – each have other exceptions that excuse compliance for investigations related to securities violations. Thus, these laws generally should not impede compliance with future federal government or SRO standards for cyber risk protection.

*Alan Raul is a partner in the Privacy, Data Security and Information Law practice of Sidley Austin LLP. They are based in the firm’s Washington, D.C. office. The author wishes to thank Marci Rozen, Esq., previously a Sidley associate, for her able assistance in preparing this article.*

---

\(^{24}\) See, *e.g.*, CAL. LAB. CODE § 980; MD CODE ANN., LAB. & EMP. § 3-712; 820 ILCS 55/10; NEV. STAT. REV. § 613.135.

\(^{25}\) See, *e.g.*, N.J. STAT. ANN. §§ 34:6B-5-34:6B-10 (authorizing civil penalties of up to $1,000 for the first violation and $3,500 for each subsequent violation); WASH. REV. CODE § 49.44.200-205 (authorizing a private right of action to recover actual damages, a penalty of $500, and attorneys’ fees and costs).
Editor’s Message

With this issue, we are completing the sixth year of publishing each quarter the Information Law Journal (previously published separately as the Information Security and Privacy News and the EDDE Journal), and are continuing to welcome authors and readers from similar committees across the ABA, including members from the Administrative Law Section. This issue again presents articles from lawyers and technologists focusing on various aspects of leading-edge domestic and international practice.

The first article was written by Bruce Wright of Allstate, addressing the impacts to privacy from Big Data. The second article is from Tim Reiniger, Jeff Nigriny, and Kyle Matthew Oliver, covering the new digital identity law in Virginia. The third article is by partner Alan Friel of BakerHostetler, explaining the issues with healthcare IT contracting. The fourth article is by professors Paul Callister and Kimberlee Everson, looking at whether stability of society is based on the degree of freedom of information. The fifth article is from the team at Covington & Burling LLP led by partner Edward Rippey, discussing how to preserve privilege before and during the discovery process. The sixth article is from partner Alan Raul of Sidley Austin LLP, describing how to address the cybersecurity and privacy issues from insider threats.

Thank you to all of the authors. I continue to ask that all readers of the Information Law Journal to share with their fellow professionals by writing an article for this periodical. Our next issue (Winter 2016) is scheduled to be published in early December 2015. There are many of you who have not yet been able to share your experience and knowledge by publishing an article here but please consider doing so to widen the understanding of all of our readers. Every qualified submission meeting the requirements explained in the Author Guidelines will be published, so please feel free to submit your articles or ideas, even if you are not quite ready for final publication. The issue following Winter (Spring 2016) will be published in March 2016. As always, until then... and enjoy your tricks and treats.