

Andrea M. Matwyshyn  
[a-matwyshyn@law.northwestern.edu](mailto:a-matwyshyn@law.northwestern.edu)

Adjunct Professor of Law  
Northwestern University School of Law

Affiliate  
Manufacturing and Technology Policy Program  
University of Cambridge (UK)

## INTRODUCTION TO CORPORATE INFORMATION SECURITY LAW:

### SOURCES OF LEGAL PROTECTION FOR PROPRIETARY INFORMATION AND SOURCES OF AFFIRMATIVE LEGAL PRIVACY OBLIGATIONS OF INFORMATION SECURITY PROFESSIONALS AND THEIR CLIENTS

Leveraging legal mechanisms to maximize information security and protection for proprietary information generates a two-fold benefit:

1. Sound proprietary information security practices preserve strategic business advantage by hindering attempts by competitors to garner proprietary information for competitive advantage
2. When proprietary information includes third party data, in particular consumer data, sound information security practices help limit liability associated with security breaches by demonstrating the exercise of due care in data management.

## I . SOURCES OF LEGAL PROTECTION FOR PROPRIETARY INFORMATION

**Sources of protection: (1) contract law; (2) trade secret law; and (3) federal intellectual property and computer intrusion law**

### 1. Contract

**A. Development, Hosting and Services Agreements** memorialize the terms of services and data exchange between two parties. Generally these agreements include terms which, among other things, articulate standards of care and provide recourse for security breaches which arise from the service provider's conduct and address the following subjects:

- (1) **relationship:** whether the services are being provided as part of a joint venture, whether the developer is acting as an independent

contractor, and what fiduciary obligations exist as a consequence of this relationship

- (2) **specifications for the product or service being provided, including all security specifications:** specifics of code or website development or other service being provided, including encryption levels, content, functionality, benchmark dates for completion , and whether failures in performance rise to the level of constituting termination events for the contractual relationship
- (3) **confidentiality and noncompetition:** restrictions on sharing and use of proprietary information; restrictions on future work for competitors to minimize likelihood of proprietary information use, including that all proprietary information be returned of, if return is not possible, destroyed upon the termination of the relationship.
- (4) **recourse for breach and post term survival of confidentiality:** indemnification provisions providing remedies in law and at equity, including the ability to obtain an injunction to prevent use of proprietary information and technology
- (5) **consideration:** explicit designation of how costs associated with the relationship will be allocated and what benefits each party will receive, including which party will cover the costs of development and how compensation of the developer will be structured, i.e. whether developer compensation will be based on a lump sum or a stream of payments (calculated on a use, purchases or other basis)
- (6) **intellectual property representations and warranties and ownership:** representation and warranties regarding originality of developed assets, including that no third party proprietary information has been used in an impermissible manner, as well as which party will own the intellectual property and whether the developer retains any rights such as a license back
- (7) **liability:** allocation of liability in connection with the developed asset, including any liabilities which may arise as a result of infringement of third party intellectual property
- (8) **data control and use:** the terms of user datamining, if any, by the developer. Data control terms are becoming increasingly important because of convergence of development and services and possible liability associated with improper data uses. For example the In re:[Pharmatrak](#) case demonstrates the importance of carefully crafted contractual restrictions on data use by service providers.

- (9) **derivative works and corollary rights:** the terms of future developments in connection with the developed asset, including development of derivative works and, in particular, ownership of corollary intellectual property produced in the course of the main development activity. For example, in the context of internet related asset development, agreements should specify that any new domain names be registered in name of the entity commissioning development
- (10) **assignment:** especially if a continuing services relationship exists, whether and on what terms, the obligations under the agreement are assignable and can be contracted out to a third party for performance

**B. Employment Agreements (and Severance Agreements) with Key Employees** generally include terms that protect both employers and employees with regard to their respective information and obligations of confidentiality to each other in the course of the employment relationship. Key terms in employment agreements relating to information control include

- (1) **confidentiality:** description of the types of proprietary information to which the employee has access, standards of care the employee is required to use in handling proprietary information, permitted uses of proprietary information, and if the employee contributes proprietary information, the parallel restrictions on access, care and uses of employee information by the employer and agents of the employer. In particular, terms of return and/or destruction of proprietary information upon termination of the employment relationship are set forth.
- (2) **assignment of inventions / work for hire:** assignment provision transferring certain or, usually, all ownership interest in any new intellectual property created by the employee during the course of employment and setting forth the scope of permissible use of company resources for purposes not related to employment. These provisions usually stipulate that all new inventions or other intellectual property created by the employee during the term of employment which in any way use the employer's resources, arise out of the employee's work for the employer or are created on the employer's time constitute proprietary information of the employer
- (3) **noncompetition/nonsolicitation:** restrictions on the ability of the employee to accept employment from a competitor upon expiration or termination of the term of the employment agreement, as well as restrictions on the ability of the employee to recruit other employees or clients to follow him/her into

subsequent employment. The level of permissible competition restriction varies state by state, both as to the scope of allowable geographic, time and industry restrictions.

- C. Confidentiality agreements with all at-will employees and contractors** set forth standards of care and acceptable uses of proprietary information, including protocol for return and/or destruction of such information upon termination of the relationship between the employee or contractor and the entity. These confidentiality agreements create a systematic policy of proprietary information protection throughout the entity.

## 2. Trade Secret Law

- A. Each state has a trade secret statute** which can provide another source of legal remedy in response to security breaches of confidential proprietary information. In particular, former employees and contractors can be enjoined from releasing proprietary information obtained by them as a consequence of providing services to a client. The wording and scope of each state's trade secret statute (as enforced by the courts of that state and that federal circuit) varies but, generally speaking, in order to qualify for trade secret protection, proprietary information must
- (1) fall within the statutory definition of what constitutes a trade secret**, which may or may not extend to all proprietary information. For example, whether a client list is considered within the scope of protection afforded by state level trade secret statutes varies greatly across states. In [Illinois](#), proprietary information which may qualify for trade secret protection means information, including but not limited to, technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, or list of actual or potential customers or suppliers. In [Wisconsin](#), however, client lists are, in most instances, not protectable.
  - (2) satisfy certain security conditions under which protection is extended**, which also vary state by state. But, generally speaking, in order for proprietary information to qualify as trade secret information, the entity seeking to obtain protection must demonstrate that
    - a. the proprietary information in question is sufficiently secret** to permit the owner to derive economic value, actual or potential, from not being generally known to

other persons who can obtain economic value from its disclosure or use; and

- b. is the subject of efforts that are “reasonable”** under the circumstances to maintain the secrecy or confidentiality of the proprietary information in question. The definition of what constitutes reasonable efforts at information protection varies according to interpretation of the state and federal courts applying the particular state law. In general, a systematic policy of information protection is the best evidence of reasonable precautions for information protection.

**B. Consistent information protection policies that are disseminated, implemented and enforced on a regular basis throughout the organization are usually a key prerequisite** for obtaining the benefits of state trade secret protection. In order to argue that a particular piece of proprietary information that is the subject of litigation does not qualify under the definition of a “trade secret” under state law, frequently, a defendant must only demonstrate that information security policies in the plaintiff’s operations are inconsistent across the organization, are not adequately known to employees and contractors and/or are not consistently and regularly enforced.

- (1) Confidentiality agreements** (which should specifically itemize types of proprietary information and will, hopefully, explicitly include the particular proprietary information at issue in any litigation explicitly within this itemization) should be in place throughout the organization with all employees, even those who might not be expected to come in contact with proprietary information on a regular basis, all consultants and other contractors, and, in particular, all third party service providers, especially if they have access to customer data.
- (2) Physical security** of proprietary information should be demonstrably obvious. Specifically, employees (and third parties) should be provided with access to proprietary information only on a “need to know” basis and only to the extent necessary to fulfill their duties. Security measures should be in place throughout the organization – both on networks (e.g. password only access) and within physical space (e.g. locks/guards to file rooms) to prevent individuals from obtaining access to unnecessarily large amounts of proprietary information.

### 3. Federal law

#### A. Intellectual property protections

(1) **Copyrights** provide federal legal protection to [any original work of authorship fixed in a tangible medium](#). A copyright affords an exclusive ownership and use right for commercial exploitation to the author of the work.

- a. A creator possesses an **inherent copyright** simply by fixing an expression in a tangible medium; no filing is necessary. A creator **can also file the work with [Copyright Office](#)** of the Library of Congress.
- b. **Length of copyright varies by type of author.** If the author is an individual, protection is for the life of author + 70 years. If the author is a business entity, protection extends for 75 years for the corporate work (except 95 years for corporate works published before 1978). However, anonymous or pseudonymous works for hire get 95 years of protection from first publication or 120 years from creation.
- c. In the case of **code**, one strategy frequently used in legal practice to protect the information is to do a confidential filing, blacking out half the code.

(2) **Patents afford 17 years of protection [to new, nonobvious, useful inventions](#).**

- a. In order to obtain a patent, the inventor must **disclose the details of the invention to the [Patent and Trademark Office](#)** for assessment. This filing can be done on a confidential basis, but can be lengthy process.
- b. **Patent applications are costly to file and potentially costly to enforce.** Especially in the case of a small business, the costs associated with defending a patent against a “deep pocket” competitor can be great. Receiving a patent triggers publication of the specifics of the invention and may open up the inventor to predatory litigation. Particularly with regard to time sensitive inventions with short shelf-lives of competitive advantage, patent protection may not be worth the effort. The decision is idiosyncratic in each business circumstance.

**B. Criminal computer intrusion law.** Although outside the scope of the discussion here, enlisting the assistance of the FBI and other state and federal law enforcement officials may prove advantageous in certain types of data security situations, particularly in the course of a severe denial of service attack in order to mitigate costs. [Criminal computer intrusion law](#) includes the [Digital Millennium Copyright Act](#), [Computer Fraud and Abuse Act](#), [Electronic Communications Privacy Act](#), [Wire Fraud Act](#), and various state statutes.

## II. AFFIRMATIVE PRIVACY OBLIGATIONS

Three possible sources of privacy and security obligations exist – (1) legally imposed obligations, (2) self-imposed obligations; and, potentially, (3) industry imposed obligations. These obligations pertain in different degrees to each of three different types of data – 1. sensitive data; 2. U.S. personally identifiable data; 3. nonpersonally identifiable data.

### 1. Legal bases for privacy and security obligations

**A. Legally imposed.** One source of privacy and security obligations arises out of statutes passed in the United States and abroad regarding acceptable levels of care with regard to particular data collection and storage situations.

(1) **Sensitive data.** In the United States, children’s data, financial information, and health information qualify as sensitive data which require higher levels of care because of U.S. regulation. Foreign user data requires a higher level of care because of international regulation

a. **Children’s data.** Generally speaking, the [Children’s Online Privacy Protections Act \(COPPA\)](#) requires that affirmative consent be obtained in connection with online collection of data from children 13 and under. Upon receipt of verifiable parental consent, the data must be stored securely and segregated from adult data for, among other reasons, easy deletion upon request of a parent or guardian. Third party provider agreements (if any of the collection or storage process of children’s data is outsourced) should all contain strong confidentiality language and require that the provider exercise high levels of care and security, both electronic and physical, with regard to the data. COPPA also required that a website’s privacy policy provide clear disclosure and comport with standards for this disclosure set forth both in the statute and promulgated by the [Federal Trade Commission](#). However, COPPA provides for certain exceptions to the requirement of verifiable parental consent. The Federal Trade Commission is becoming increasingly aggressive in its COPPA prosecutions, recently instituting regulatory action

against [Hershey's](#) and [Mrs. Fields](#). [Certification authorities](#) have also proliferated.

- b. Financial information and data.** The [Gramm-Leach-Bliley Act \(GLB\)](#) governs collection and use of consumer data. GLB sets forth requirements for clear online and offline disclosure and includes restrictions on appearance of graphical user interfaces of websites which collect or provide access to personally identifiable financial information, such as online banking websites. GLB expressly requires that the contracts of all third party providers to whom collection of storage of data is outsourced contain certain data security provisions and strong confidentiality restrictions.
  - c. Health data.** The [Health Insurance Portability and Accountability Act \(HIPAA\)](#), like GLB imposes a higher standard of care on entities and divisions of entities which collect and use consumer health information. Among other obligations imposed by HIPAA, entities subject to HIPAA are required to have Chief Privacy Officers with adequate resources and corporate “goodwill” to implement adequate privacy policies throughout an entity.
  - d. Foreign data.** Foreign data must be collected and handled with a high level of care. For example, the European Union Data Directive and Canada’s the [Personal Information Protection and Electronic Documents Act \(PIPEDA\)](#), both set forth parameters for permissible data collection that are different from those allowed in the United States. As little as dropping a cookie on the machine of a European user can subject a U.S. entity to jurisdiction in Europe for violating the [EU Data Directive](#). Despite the [U.S./EU Data Safe Harbor](#) in place, many companies are still uncertain about the proper way to collect EU data, if at all. The Safe Harbor certification procedure has been perceived as overly burdensome by many entities and requests to the Department of Commerce for certification have been fewer than expected.
- (2) Other U.S. personally identifiable data and nonpersonally identifiable data.** No statutory duties exist at the moment, however, further regulation has been frequently debated. The Federal Trade Commission has, on occasion, prevented certain corporate actions which it deems to pose too grave a danger to consumer data. For example, it [investigated the data practices of DoubleClick, Inc. following its acquisition of Abacus Direct](#). Also, although not arising to the level of statute, the FTC has made a series of “suggestions” regarding good privacy practices and the [elements of disclosure contained within a good privacy policy](#). A useful resource for drafting privacy policies is the [OECD Privacy Statement Generator](#).

**B. Self-imposed.** The primary source of self-imposed obligations for data security and privacy arise because of an entity's [online and offline privacy policies](#). In general, although in many instances entities are not legally required to include a privacy policy on their websites, it is considered good business practice and good public relations to include a privacy policy on an entity's website. Therefore, many entities choose to do so voluntarily even in the absence of a specific legal obligation. Also, as described above, in certain limited circumstances depending on the types of data a website collects or the audience it targets, legal obligations to include privacy policies exist. By posting a privacy policy, an entity enters into a contractual agreement of sorts with its users and the Federal Trade Commission. If the privacy practices reflected on an entity's website do not accurately reflect the data collection and use which occurs, the entity is subject to both prosecution by the Federal Trade Commission and, potentially class action lawsuits on the part of users. These privacy promises are [usually binding even in bankruptcy](#). As mentioned previously, the FTC has articulated standards for drafting privacy policies. These standards provide for certain elements to be included in privacy policies: the disclosure should include a statement of what type of data is being collected, how it is being collected, how it will be used, and how the user can correct or delete the information. The FTC has been aggressive in its prosecutions of entities for violations of their stated privacy policies and has even engaged in preemptive enforcement on occasion. For example, although the Microsoft Passport system did not violate its privacy policy through a tangible "bad act" that could give rise to basis for suit, the FTC preemptively prosecuted Microsoft and entered into a [consent decree with Microsoft](#) regarding its data collection practices. Violations of privacy policies can be inadvertent. In one infamous breach of health data privacy and security, the employee of a pharmaceutical company sent out a mass email reminding users of Prozac to take their medication and included the email addresses of other Prozac users in the visible address fields. This action constituted a violation of both the patients' reasonable expectation of privacy in their health information and the company's website's stated privacy policy. The company, [Eli Lilly, is the subject of a consent decree with the FTC](#). Recently, the FTC stated that an entity's online privacy policy and offline privacy policy must match and create a consistent entity-wide policy of privacy practices.

**C. Industry imposed - negligence.** Although little caselaw addresses data security obligations, it is likely that industry by industry standards will evolve that will represent standards of minimum levels of care in the industry. As a consequence, if a breach of security resulting in harm through a disclosure of data in violation of statute or privacy policies occurs, an entity could face liability in a negligence action if the level of care it exercised fell below the minimum reasonable levels of care a reasonable entity or individual would have exercised in similar circumstances.

## 2. How to mitigate risk.

- A. View your contracts as a historical record of the transaction.** One way to mitigate risks is to have a tech savvy lawyer or active IT department involved in contract specificities. A contract should not be viewed as just “papering” a transaction, but rather it should be viewed as a historical record of the transaction and the terms of the business relationship of the parties. This historical record can be a powerful defense mechanism which can be used to protect against liability in litigation or regulatory action arising out of tortious or criminal acts of business partners. Especially if a business is not a technology industry business but relies on technology heavily, e.g. brokerage houses, by demonstrating due care in contractual practices an entity can avoid or substantially mitigate liability.
- B. Make your contracts specific.** All contracts should specify encryption and care standards, including physical security of all places where information in tangible or intangible form resides. Contracts can shift responsibility and costs associated with privacy regulation violations onto one party. In particular, in connection with enforcement of the terms of the agreement in the circumstance where the other party breaches its obligations, the terms of the agreement can and should include reimbursement for reasonable attorneys fees and court costs, especially when doing business with unfamiliar contractors.
- C. Think as far ahead as possible and in terms of what can go wrong.** Plan ahead for the worst case scenario. For example, although from a marketing standpoint, it may look like a good idea to have all databases interoperable and “talking” to each other, but this may not necessarily be best from a legal perspective of compliance with privacy regulation or insulation against liability. Consulting with internal legal staff or outside counsel throughout the contracting process facilitates prevention of problems to the extent possible. Avoiding problems through a thorough agreement is always cheaper on the front end than restructuring agreements and relationships through litigation later after problems arise.
- D. Institute good entity-wide data control and security practices.** Have developed data control policies with checks and balances. Have a policy in place of requiring that all employees and contractors sign strong confidentiality agreements. Circulate employee handbooks containing data control, security and confidentiality policies with regularity and frequency, and enforce them consistently. Perform background checks on employees and contractors. Have appropriate staff and officers, including a Chief Privacy Officer, in place.