VistaLaw Views

Scrambling for Compliance in Data Privacy: Retooling Your Vendor Contracts

June 2009

John J. Smith, VistaLaw International, LLC

In this issue: *If your company handles individually identifiable personal data, it is time to take a fresh look at your information security practices, and to take a pencil with eraser to your vendor or customer contracting processes. Why? Ever more comprehensive state, federal and private industry mandates and just good business practice. There are ways to evaluate and manage your risk.*

Regulations relating to the protection of personal proprietary data are burgeoning. They are now commonplace for e-commerce businesses, especially those engaging online with individual consumers and collecting, processing, storing, and transferring their personal data (such as credit card or social security numbers, or other "private" information identifiable with individual persons). Non-governmental standards within and across industry groups are also expanding, often as a prerequisite to transacting business online (e.g. credit card industry PCI standards), or as a condition of insurance.

Effective data security practices are simply good business and are necessary to prudent risk management, a "given" that comes with the territory of handling sensitive personally identifiable information. An indispensible part of risk management activity is contract management, requiring enterprises to take a close look existing and planned vendor and customer contracts in light of expanding regulatory mandates, and to retool contract practices as necessary.

Some Background: Existing Federal and State Laws

Comprehensive federal laws and regulations specific to certain industries or specific business practices (financial services, healthcare, credit lending) are now well established. The Federal Trade Commission is empowered to deal with "unfair or deceptive practices," and has recently launched new and energetic regulatory programs mandating privacy safeguards for businesses of all sizes and types. To date, forty-four states, the District of Columbia, Puerto Rico and the Virgin Islands have adopted consumer-oriented data privacy protections. Abroad some sixty countries have personal privacy laws. There are over 450 pending bills in state legislatures across the United States proposing yet more layers of data security regulation. Most states have adopted data breach notification and identity protection measures, but with few exceptions, they have adopted looser, aspirational standards (such as requirements of reasonableness, or consistency with prevailing industry standards, or best practices), and have imposed few concrete remedial requirements.

Recent Developments: Regulating Down to the Minutia

More recent developments reveal a steeper inclination among federal and state legislators and regulators for more proactive requirements. Newer regulatory initiatives are imposing detailed "prophylactic" programs requiring businesses to predict and prevent personal data loss and misappropriation, in contrast to the more reactive approaches of the past, like breach notification requirements. Many observers forecast a trend toward more and more comprehensive compliance standards and prescriptions (physical, administrative, operational, and technical) for businesses of all sizes and types and in all markets, what one party has aptly called "regulating down to the minutia."

The most prominent example of the "down to the minutia" approach can be found in the recently repromulgated rules of the Office of Consumer and Business Regulation of the Commonwealth of Massachusetts ("OCABR"). The Massachusetts regulations (officially the "Standards for the Protection of Personal Information of Residents of the Commonwealth," or simply "the Standards") are certainly the most rigorously detailed set of mandates for data security policies and practices in the country. Their importance extends well beyond the Bay State. They apply to any business anywhere that owns, stores,

processes or transfers personal information about Massachusetts residents. A breathtaking assertion of jurisdiction, not the first and likely not the last. Other state legislators are taking a close look at the Massachusetts model.

Under continually evolving federal and state standards, all enterprises now are expected to undertake "reasonable" organizational, physical, technical and administrative measures to protect sensitive personal data in their custody or control.

Highest Common Denominator: Guidelines for a Written Compliance Plan

Under continually evolving federal and state standards, all enterprises now are expected to undertake "reasonable" organizational, physical, technical and administrative measures to protect sensitive personal data in their custody or control. Under various federal and state regulatory schemes enterprises must as a first step perform a thorough risk assessment that identifies foreseeable risks to the security of personally identifiable information, based on the sensitivity of the information in question, all of which should be set down in a written security plan. The FTC has published a "Safeguards Rule" that could serve as a useful guide. Another, more comprehensive set of guidelines (actually compulsory standards) are the Massachusetts prescriptions. The Standards are instructive and, in a sense, serve as the "highest common denominator" for data privacy contract management practices.

The FTC Safeguards Rule (indirectly) and the Massachusetts OCABR Standards (very specifically) contemplate that enterprises identify and catalogue all contracts with third party service providers that might involve personal data. The Standards require companies to "verify that any third-party service provider with access to personal information has the capacity to protect such personal information … [and] ensure that such third party service provider is applying such personal information security measures at least as stringent as those required [under the Standards]."

Four Elements of Effective Contract Risk Assessment

There are four key requirements under the Standards, which are inferentially present in the FTC guidelines as well. First, companies will have to **scan and catalogue all contracts** involving transferred personal data, and regardless of whether they involve Massachusetts residents or residents of any other state purporting to protect its residents' data wherever housed. Why all? As a practical matter, it is seems unlikely that many businesses have organized data in static categories of personal and non-personal data, or have sorted personal data by state of residence, since segregating data by residence in most cases serves no business purpose and would entail exceptional additional costs. Companies may in the future have to incur such costs to segregate data to reduce the scope of cataloguing, however.

Four Elements
- Scan and catalogue all contracts
- Evaluate the relative vulnerabilities
- Undertake and document real-time due diligence
- Procure in writing reliable representations and undertakings

Recent developments indicate a trend toward ever more prescriptive regulation, requiring proactive business practices.

Second, companies should **evaluate the relative vulnerabilities** of those data within each identified contractual arrangement, identifying security risks and apparent effectiveness of any safeguards that are contractually specified to minimize risks identified. Concurrently, they must document this analysis in writing so as to demonstrate compliance, if called upon at some future point — for example as a part of an official investigation by a State Attorney General.

Third, businesses must **undertake and document real-time due diligence** to determine whether a counterpart to a contract actually provides effective data safeguards, and what kind and at what level. One cannot simply rely on generic representations and warranties relating to compliance with law, or even those provisions specifically addressing data security if they fail expressly to addresses the necessary security measures in particular.

This requirement presents some real practical challenges: how is one is expected to audit the representations of the other party, or to compel another independent party to adopt a comprehensive program of its own that meets all of the detailed administrative, operational, technical and physical security mandates of some distant regulatory body, such as the Massachusetts OCABR? Some contracts contain audit rights, sure, but often they are

limited to matters relating to royalties or specified performance issues. In a perfect world of sufficient leverage, every business could simply elect to conduct highly intrusive "due diligence" auditing of another company's most sensitive operations. Moreover, such due diligence may have to become an on-going undertaking for the life of the contract or the life of the data in question.

A requirement to "verify" and "ensure" is tantamount to forcing the reopening of existing contracts, since it likely imposes a wholly new obligation not contemplated by the parties during original negotiations. Without the addition of detailed new provisions to the vendor contract or an entirely new agreement with one's vendor, a business seeking to secure such verification is simply unable to perform due diligence to "ensure" the capacity to comply, or that the vendor's actual application of security measures are consistent with the OCABR "Standards" or other applicable requirements.

Fourth and finally, a company should **procure in writing reliable representations and undertakings** by the other party that its data security measures meet the specific mandates in administrative, operational, technical, and other areas dictated by the applicable regulatory regime. Not only will this require a full-blown educational effort to inform the vendor of the details of regulations in question, it will likely require additional consideration – money usually – to bring the parties to "yes."

What to Ask of your Attorney, CIO, or Contract Manager

So what does all of this mean to the in-house counsel, IT director, or regulatory compliance officer, or other party responsible for privacy and data security matters?

Tackle the most problematic or risk-laden contracts first, those involving data of the highest sensitivity or risk of loss or misuse.

These four elements are hardly self-effectuating requirements, but if a party has the appropriate leverage and the opportunity, here are some practical negotiating steps a company's contract manager might discuss with the company's in-house or outside legal counsel.

1. **Triage — break the problem down into manageable pieces.** Tackle the most problematic or risk-laden contracts first, those involving data of the highest sensitivity or risk of loss or misuse. It's just too expensive in time and money to protect all information types at the same high level. Address the new contract or contract renewals where leverage might be greatest. Triage is only the first step.

2. **Review and revise contract representations and warranties. "Flow Down" the obligations to the other party.** Whenever possible, seek to expand standard contract terms regarding compliance with laws to encompass expressly the OCABR Standards, or other specifically applicable standards. Also, make sure to excise other boilerplate terms that might operate to nullify an expansion or expanded interpretation of warranty obligations. Unless they are expressly included, customary warranty disclaimer and liability limitation language might confuse the interpretation, or even operate to read out any inference that the specific regulatory standards are included in a more generally worded representation or warranty. This will not come easy. Again failed efforts to conform contracts to regulatory agency expectations should be thoroughly documented.

3. **Don't rely on a vendor's negligence to cover your liability.** Recourse to a vendor through a negligence theory might prove impractical or even useless. Proving negligence depends on the applicable standard "duty of care," an elusive concept in cyberworld. And even when vendors follow industry standards or use all reasonable efforts, data gets lost, stolen or corrupted. Security flaws happen. The question is, who is to be on the hook for it? The hapless company entrusting personal data to a party in the business of providing data services, or the hapless data services provider which has taken all reasonable steps to safeguard the data?

Since few businesses can afford the luxury of maintaining different security practices for different state and federal regulatory regimes, they will of necessity default to the broadest, most comprehensive requirements and standards, the "highest common denominator" regulatory regime of the moment.

4. **Indemnification.** The best course, if you can get it, that is. A vendor of course will (not unreasonably) seek to avoid or to minimize the scope of its indemnification, offering instead assurances "commercially reasonable" steps to protect the data, or limiting the obligation to gross negligence or intentional acts. If at all possible, have the indemnification cover not only third party claims (like claims of injury from the data subjects themselves), but also administrative actions, and the costs of providing remedial measures (notification, free credit reporting services, etc.) in the event of a security breach. Securing adequate indemnification protections will become increasingly important as civil liability (including the possibility of class actions) inevitably fills the vacuum created by evolving regulations expanding personal privacy rights.

5. **Vendor Selection or Renewal.** Performing due diligence prior to selection of new vendors or new business opportunities with existing vendors would likely encounter less resistance than seeking to reopen concluded contract negotiations. Where a vendor refuses, and no other reasonable alternatives to the desired vendor product or service exist, it is important to document efforts to bring vendors in line with official expectations

6. **Document everything.** In almost all cases a company's compliance efforts will be judged in light of a company's size, resources, and the sensitivity level of the personal data in its care. Given the high likelihood that compliance efforts with third parties will fall short in one way or another with some of the detailed prescriptions, a company would be wise to create a convincing contemporaneous record of its negotiations with its third party service providers.

Finally and most regrettably, with an increase in regulation one may reasonably anticipate a concomitant increase in public agency investigations and enforcement actions, consumer litigation, and perhaps more disastrous, the risk of loss of business reputation. Businesses everywhere have to navigate through an ever more complex maze of legal obligations. Since few businesses can afford the luxury of maintaining different security practices to address different state and federal approaches, or to segregate data based on legal jurisdiction, they will of necessity default to the broadest, most comprehensive set of requirements and standards, the "highest common denominator" of the most comprehensive federal and state regulatory regime of the moment.

Good business practice is the best defense.

About the Author
John J. Smith is with the DC office of Vistalaw International, with over thirty years of experience as both in-house and outside counsel to companies engaged in the information technology sector.

About VistaLaw International
VistaLaw International, with offices in Paris, London, Madrid and Washington, D.C., is a legal services firm created by former in-house counsel dedicated to providing practical, cost-effective legal advice to global companies. VistaLaw's services include regulatory compliance reviews, corporate governance and structuring, drafting and negotiation of commercial contracts, and handling of merger and acquisition transactions.
For more information, visit **www.vistalaw.com**.

VistaLaw International LLC
International Square
1875 I Street N.W. Fifth Floor
Washington, DC 20006, USA
Tel: +1 202-429-5526