PRIVACY, DATA PROTECTION, AND THE LACK THEREOF

CHARLES M. HOSCH, *Dallas*
Clark Hill Strasburger

KATHRYNE MORRIS, *Dallas*
Clark Hill Strasburger

State Bar of Texas
30TH ANNUAL
ADVANCED ADMINISTRATIVE LAW
June 7-8, 2018
Austin

CHAPTER 16

Charles M. Hosch

Member
Clark Hill Strasburger
901 Main Street
Suite 6000
Dallas, Texas 75202
T: 214.651.4678
C: 214.632.2230
F: 214.659.4050
E: charles.hosch@clarkhillstrasburger.com

Charles M. Hosch is a privacy, data use, and cybersecurity lawyer with 35 years' experience in business transactions and complex business litigation. He is a Certified Information Privacy Professional (CIPP/US) through the International Association of Privacy Professionals.

Charles handles technology development and data management. He has long experience handling trade secrets, confidential and proprietary information, and privacy, and with writing, negotiating, litigating, mediating, and arbitrating technology agreements on each side of the table and docket. He is experienced in cybersecurity and guides clients who face security incidents. He often serves as outside general counsel to middle-market businesses and has written and negotiated hundreds of complex business agreements, across dozens of industries.

Throughout his career, Charles' practice has included advertising, marketing practices, and labeling, trademark and copyright protection, and business tort litigation including tortious interference, Section 43(a), defamation, common-law and digital misappropriation, RICO, fraud, the Computer Fraud and Abuse Act, and now "cyber torts." Over the years he has handled many "extraordinary remedy" cases, has resolved many emotional business disputes as a mediator, and has successfully tried "bet the company" matters which the clients could not afford to lose.

Charles teaches "***Trade Secrets and Business Torts***" at SMU Dedman School of Law, where he has taught continually since 1991. From 1997-2015, he co-taught ***Trademarks and Business Torts***. He is a frequent author and CLE speaker. A graduate of Harvard College and Harvard Law School, he has practiced his entire career with Strasburger & Price, now known as Clark Hill Strasburger.

Kathryne M. “Kate” Morris

Member
Clark Hill Strasburger
901 Main Street
Suite 6000
Dallas, Texas 75202
T: 214.651.2043
F: 214.659.4028
E: kate.morris@clarkhillstrasburger.com

Kathryne (“Kate”) Morris is a member of Clark Hill Strasburger’s Privacy, Data and Cybersecurity practice. She is certified by the International Association of Privacy Professionals (IAPP) as a Certified Information Privacy Professional, United States (CIPP/US) and Europe (CIPP/E).

Kate helps clients identify, evaluate, secure and manage their information security risks and intellectual property. Her practice focuses on technology transactions, privacy and data protection. She advises a wide range of businesses, manufacturers, financial institutions, energy providers, retail companies, and other organizations regarding cloud computing, e-commerce platforms, and mobile applications. In connection with this representation, Kate routinely leads due diligence and negotiations associated with information technology and business process outsourcing agreements, including enterprise-wide cloud migrations for companies and their affiliates, as well as professional services firms.

Additionally, Kate is well-versed in handling data security incident response and complex commercial litigation matters, including disputes over copyrights and trademarks, software licensing, breaches of commercial contracts and fraud, and many other issues and claims.

Kate is also a frequent speaker and writer on technology issues related to electronic discovery, data preservation, social media, and data privacy and security.

TABLE OF CONTENTS

PRIVACY, DATA PROTECTION, AND THE LACK THEREOF

I. INTRODUCTION AND OVERVIEW

According to Experian's Data Breach Industry Forecast 2018:

> The top data breach trends and forecasts of 2018 include the following:
>
> - The United States may experience its first large-scale attack on critical infrastructure, causing chaos for governments, companies and private citizens.
> - Failure to comply with new European Union regulations will result in large penalties for U.S. companies.
> - Perpetrators of cyberattacks will continue to zero in on governments, which could lead to a shift in world power.
> - Attackers will use artificial intelligence (AI) to render traditional multifactor authentication methods useless.
> - Vulnerabilities in internet of things (IoT) devices will create mass confusion, leading to new security regulations.

As organizations become more technology-dependent, the benefits of technology must be balanced against the risks, which include all of those listed above. Yet, most government agencies, like other organizations, fail to understand the differences between data security, data protection, and data privacy.

A. Briefly, a Lexicon: "Data," "Security," and "Privacy"

UK mathematician Clive Humby is often credited with the phrase, "***Data is the new oil***." The metaphor is inexact and not to be taken over-literally,[1] but it makes the vivid point that the emergence of cheap, nearly unlimited data storage and astonishingly fast, effective computing power over the past ten years or so now makes visible connections, trends, and patterns that have always been buried or obscured, at least up to now – translating into business opportunities that are breathtakingly valuable.

This has all happened so quickly that the lexicon has not had time to catch up. The word everyone hears now is "data;" but until recently the more commonly-used word was "information" (as in, "Confidential and Proprietary Information"). Similarly, most businesses and business lawyers are perfectly familiar with the need to take practical, reasonable measures to protect the confidentiality of their trade secrets and "Confidential and Proprietary Information," but now the term "cybersecurity" seems to subsume in one word what generations of lawyers knew to be a broad concept with many facets. And suddenly the word "Privacy" has become paired with "data," bringing its own broad and hard-to-place meaning.

It is helpful to understand, first, that "Data" can mean virtually any kind of information, in any quantity and quality, about any person or thing. It can extend to sales data, financial data, performance data of people or things, and all other kinds of "business" information. It can also extend to shopping histories, browsing histories, histories about attention spans, medical histories, banking records, educational records, and all other kinds of "personal" information. Then, once sliced and diced, the connections, trends and patterns that have emerged from the raw "business data" or "personal data" themselves become "data," often far more valuable than the raw ingredients from which they were drawn – like oil that has been refined.

It is helpful, second, to realize that "security" refers specifically to the protection of valuable assets against intrusion, trespass, or theft. The lock on your door is part of your "security" – it helps you control who comes in and who stays out. There will be no "privacy" without security, but they are not the same thing. "Security" is a requirement for any kind of data – business, personal, or otherwise – but is only required to a greater or lesser extent, according to its value and the regulatory environment surrounding it.

"Privacy," by contrast, refers to the collection, use, retention and/or disclosure of particular data – almost always *personal data*. "Privacy" rarely matters in connection with "business" data, *except* to the extent that personal data has *become* valuable business data – such as personal shopping and buying histories, for example (in which event it suddenly matters very much). If "security" refers to the lock on the door, "privacy" connotes the curtains on the windows. [2]

---

[1] See Adam Schlooser, "Here's why data is not the new oil," World Economic Forum Jan. 23, 2018, http://www.businessinsider.com/data-is-not-the-new-oil-adam-schlosser-of-the-world-economic-forum-2018-1

[2] A right of "Privacy" is usually thought to have been first identified in the seminal 1890 law review article of Louis Brandeis and Samuel Warren, "The Right to Privacy," published in the Harvard Law Review – an article which was inspired by Professor Warren's outrage at the publication of his daughter's photograph by a Boston newspaper on the occasion of her wedding. In the post-war period, the "right to privacy" was refined by Professor Prosser in his "four rights of privacy," these being 1) the right of seclusion, 2) the right to avoid being placed in a "false light," 3) the right to control one's own endorsement of others, and 4) the right to avoid public disclosure of embarrassing facts. Later, the "right to privacy" was explored in a series of Supreme Court cases

B. A Peculiar Trinity: The Relationship among Cybersecurity, Privacy, and Intellectual Property

Perplexing terms make it hard to keep straight what legal specialty(ies) occupy what space. Generally, the legal requirements have long been to take "reasonable" measures to protect trade secrets and confidential and proprietary information (data) and keep them confidential. *See* Defend Trade Secrets Act, 18 U.S.C. § 1839(3)(a); Texas Uniform Trade Secrets Act, Tex. Civ. Prac. & Rem. Code § 134A.002(6); Restatement of Torts Sec. 757, comment b (1939) (for New York and Massachusetts, the two remaining states who have not yet adopted some version of the Uniform Trade Secrets Act.)

What is "reasonable" under the circumstances generally depends on the value of the information (data) at issue. Security always comes at a cost both in dollars and in drag or inefficiency, not everything needs to be protected like Fort Knox, and so "perfect" security is not necessarily "optimum" security.[3] So determining what is "reasonable" for protecting trade secrets and confidential and proprietary information has long been a business-driven balancing of costs and value.

With respect to *business data*, that is still generally true in the "cyber" age. Once a business reflects on the likely cost of getting its systems hacked, the "reasonable" investment that will make good business sense will likely suggest itself. From there, the exact steps to establish "reasonable security" will be up to the Information Technology specialists.

With respect to *personal data*, however – especially *personal data* (like shopping patterns) that has been transformed into valuable *business data* – two things are different now. One is that a huge assortment of specific legal requirements for what constitutes "reasonable security" for *personal data* is present and growing. In many areas, the new regulatory environment is not leaving the matter at "reasonable" at all, but is requiring specific and often-detailed steps to be taken at the administrative, organizational, and technical levels. Lawyers must often translate and interpret these requirements to the information-security professionals, who will nod solemnly and do the best they can to comply with regulatory checklists. The lawyers must then do the same with everyone from the most junior employee to the most senior management. Meanwhile the true experts know that mere *compliance* will almost never be enough because the requirements are usually antiquated by the time they are released, and that agile, active, and anticipatory defense – over and above compliance requirements – is absolutely essential and always will be.

The second difference is that there is now an entire, new, and growing body of law on what use and disclosure may (or may not) be made of such *personal data* in various settings. Increasingly, the emphasis is on leaving sovereign control of such uses and disclosures in the hands of the individuals to whom the data refers (called "Data Subjects"), *rather than* in the hands of the businesses which have taken the risk and invested the money to collect it, to spot the trends, patterns, and connections within it, and to develop the algorithms to monetize it. This is the new and growing area of "Privacy Law;" and in its focus on what may be called the "Sovereignty of the Person," it looks to be trending toward an uncomfortable, near-titanic collision with the ancient laws of business which incentivize investment, creativity, and development – namely, the law of "Intellectual Property."

"Intellectual Property" shares a lot in common with "Data Privacy." Both address a variety of intellectual creations, discoveries, or developments, which are sometimes abstract and often valuable. In their common construction as "property," both reduce to the right to *exclude others* from access, use, or exploitation, as much or more as they do to permitting the actual "owners" to do as they please. But "Intellectual Property" is composed of essentially four separate legal schemes (patents, copyrights, trademarks, and trade secrets) which address four separate purposes in four totally different ways, which data "Privacy" addresses *personal data* alone. They overlap mostly with respect to *trade secrets* and confidential and proprietary information, particularly where personal data is involved.

Where a business has gone to trouble, risk, and expense to collect and develop information, an Intellectual Property focus will instinctively treat that information (and new information derived from it) as the business' trade secrets (or at least proprietary to it). The business will secure it, at least to a reasonable extent according to its value, and then will exploit and monetize it. A Privacy focus, however, will zero in like a laser onto where the information *came from*, and if it is *personal* information, will want to wrest control of it no matter how valuable it could be or how badly yanking it back would offend a roomful of businesspeople.

Given time and thought, the Intellectual Property mind can come to grips with *personal data* being less-than-freely available for commercial exploitation even if it has been sliced-and-diced at vast expense, much as

exploring the individual's relationship with the government, such as *Connecticut v. Griswold*. Now, "Privacy" is suddenly expanded to a whole panoply of statutory rights, in a variety of settings.

[3] *See Rockwell Graphic Systems, Inc. v. Dev Industries, Inc.*, 925 F.2d 174, 180 (7th Cir. 1991).

patent lawyers know that abstract ideas and natural phenomena cannot be patented, as copyright lawyers know that ideas cannot be copyrighted no matter how they are embodied, as trademark lawyers know that generic words can't identify source, and as trade secret lawyers know that information that is already readily available cannot be protected. With time and thought, too, the Privacy mind may consider that the currently-trending emphasis on personal control of personal data may be over-doing it, and making it too cumbersome for individuals to claim the benefits that modern business can offer them based on their own data. In the meantime, clarifying which specialist claims which role is at least a step in the right direction.

II. "REASONABLE SECURITY" IN TEXAS

A. "Personal Identifying Information" versus "Sensitive Personal Information."

There is an interesting difference between the definitions of "Personal Identifying Information" and "Sensitive Personal Information," and a difference between the ways they are treated.

"Person Identifying Information" means information that alone or in conjunction with other information identifies an individual, including that person's name, social security number, date of birth, or government-issued ID number; mother's maiden name; unique biometric data, including fingerprint, voice print, and retina or iris image; unique electronic identification number, address, or routing code; and telecommunication access device as defined by the Penal Code. Tex. Bus. & Com. Code § 521.002(1).

By contrast, "***Sensitive Personal Information***" means (A) a person's first name or first initial and last name, in combination with a social security number, driver's license number or other government-issued ID number, or an account number or credit or debit card number combined with any required security code, access code, or password that would permit access to an individual's financial account; OR (B) information that identifies an individual and relates to his or her physical or mental health or condition, provision of health care to him or her, or payment for the provision of health care to him or her. It does not include "publicly available information that is lawfully made available to the public from the federal government or a state or local government. See Tex. Bus. & Com. Code § 521.002(2).

There is a corresponding difference in the security obligations placed on Texas businesses – but an odd difference. With respect to "***mere*** ***personal identifying*** information, there appears to be no residual, express, statutory Texas obligation to implement and maintain security protections. (There are still such obligations in certain industries like healthcare and finance, and of course, if a business announces it will maintain such protections then it must follow through with its own announced intentions, both as a matter of contract and for FTC compliance.) For ***personal identifying*** information, the residual obligation in Texas rests on individuals not to commit identify theft. "A person may not obtain, possess, transfer, or use personal identifying information of another person without that person's consent and with intent to obtain a good, service, insurance, an extension of credit, or any other thing of value in the other person's name." Tex. Bus. & Com. Code § 521.051(a). (This reflects the Texas act's origin as a response to the problem of identity theft, which had exploded on the public consciousness when the act was passed in 2009. Indeed, most cybersecurity statutes in this country have been passed one at a time and with an isolated focus on a then-current problem. This has led to a maze of narrowly-focused, single-issue state statutes and requirements which are obsolescing so rapidly that they sometimes show signs of age by the time they take effect.)

With respect to ***sensitive*** personal information, however, the obligation is squarely on the business. "A business shall implement and maintain reasonable procedures, including any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business." Tex. Bus. & Com. Code § 521.052(a).

B. "Reasonable" – for Experts, Legislators, and Regulators.

In most cases, what is "reasonable" devolves into a battle of the experts. In the data-protection world, however, cybersecurity and data-protection experts are sometimes joined by legislators and regulators who seem anxious to be seen requiring the latest, up to date improvements.

In Texas, two specific statutory requirements help define what is "reasonable:"

1. Encrypt.

"Sensitive personal information" expressly ***excludes*** from the first part of its definition information which is ***encrypted*** (name, social security number, etc.). The encryption-exception does not appear to extend to healthcare information, but it does provide important guidance: encrypting "sensitive personal information" is almost always a good idea.

2. Destroy it Like You Mean It.

In Texas, businesses are specifically required "to destroy customer records containing sensitive personal information that are not to be retained, by (1) shredding, (2) erasing, or (3) otherwise modifying the sensitive personal information in the records to make it unreadable or indecipherable through any means." Tex. Bus. & Com. Code § 521.052(b) "Unreadable or indecipherable *through any means*" is an arresting phrase which seems to set a very high bar. Anecdotally,

the authors have been told that beating a hard drive into a misshapen mass with a dull axe will not suffice to make the information on it "unreadable or indecipherable;" it may raise exponentially the cost of recovering the information, but it can still be recovered.) As a related point, it is a well-known "best practice" in data protection not to collect or maintain sensitive personal information in the first place unless you actually need it, and not to keep it any longer than you need to. This is called "data minimization." ("The Principle of Data Minimization" may be beloved of Data Protection experts, but it may run exactly contrary to the objectives of the Marketing Department – who may not have use for it *today*, but can imagine needing it tomorrow, and who have a cliché of their own: "Better to have it and not want it than to want it and not have it.")

C. "Frameworks."

Increasingly, businesses in particular industries are required to conduct third-party assessments of their own data protection postures every other year or so, and to certify to business associates and others their level of compliance with statutory, regulatory, or contractual requirements. It is common to assess these by well-known "frameworks" whose methodologies are well known and accepted in various industries. Well-known frameworks include SOC 1, SOC 2, SSAE-16 or -18, https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc1report.html HITRUST CSF™ https://hitrustalliance.net/hitrust-csf/ , ISO 27001, https://www.iso.org/isoiec-27001-information-security.html and the NIST framework, https://www.nist.gov/cyberframework , among others. The Center for Internet Security has promulgated the "CIS Critical Security Controls," https://www.sans.org/critical-security-controls, which include:

- Inventory and control of hardware assets;
- Inventory and control of software assets;
- Continuous vulnerability management;
- Controlled use of administrative privileges;
- Secure configuration for hardware and software on mobile devices, laptops, workstations, and servers;
- Maintenance, monitoring, and analysis of audit logs;
- Email and web browser protections;
- Malware defenses;
- Limitation and control of network ports, protocols, and services;
- Data recovery capabilities;
- Secure configuration for network devices, such as firewalls, routers, and switches;
- Boundary defense;
- Data protection;
- Controlled access based on Need to Know;
- Wireless access control;
- Account monitoring and control;
- Implementation of a security awareness and training program;
- Application software security;
- Incident response and management; and
- Penetration tests and Red Team exercises

III. QUOTES AND CLICHES FOR DATA PROTECTORS

Cybersecurity-risk assessments and privacy-risk assessments share much in common, because true privacy starts with reliable security. In either case, preventing a crisis is far cheaper than managing one. For cost-effective prevention, consider the following steps:

A. Education, Training, Constantly Reminding, and Internal Monitoring: The Enemy Within.

Attacks by nation-states and international jackals claim the headlines. But shockingly, IBM has found that in 2016, sixty percent (60%) or more of cybersecurity failures were caused by insiders. About three-fourths of these involved malicious intent, and the other fourth were inadvertent. https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company. The lesson is clear: the single most cost-effective step to take is internal control, through regular education, frequent training, and constant reminders. The idea that one's own personnel could act with malicious intent may be hard to swallow, but there are the statistics; and it may well be that the best response is to have one's IT department keep a regular eye out for "oddities" and unusual patterns, both existing where they are not customary, and missing where they would be normal.

For a training/education return, one of the hardest problems to combat now is "phishing." "Phishing" is the practice of sending an email ostensibly coming from someone else, in order to get the recipient to take some act – like wiring money to the crook's account. Frequently "phishing" attacks come from overseas, particularly Russia and Ukraine. When it first reached the public consciousness, the most common defense was to teach Accounts Payable to watch out for misspellings, odd syntax, or other indications that English was not the sender's first language. Now, "phishers" have become so sophisticated that they are often able to spend months inside a target's system, studying with care the speech patterns of the senders they are about to counterfeit, so that when the "phishing" email arrives, it is virtually indistinguishable from the real thing. That is especially dangerous when the directions are what the recipient is accustomed to seeing every day, coming from this "same" person. Constant vigilance and the extra step of

double-checking wiring instructions by phone or other non-electronic means are now best practices.

B. Patch Now, Take a Coffee Break Later.

Many prevention steps are already "in the manual," just are not always carried out, much less quickly. Others are cheap and go a long way For instance, software vendors often send out software "patches" to correct bugs, but these often also address perceived security risks. The bugs may be easily endurable and the patches a nuisance to apply, so there is sometimes delay in applying them. But the security risks are not fanciful at all, and even low risks of occurrence may carry high cost if they do occur, which is all such patches should be applied immediately. It is surprising how often this must be repeated.

C. Strong Passwords, Changed Regularly.

"Password123" is hopelessly behind the times. Adopt strong passwords and change them regularly. Importantly: it is human nature to reuse passwords for different systems, perhaps with only slight differences. Today's computing power is increasingly able to detect patterns that once cracked for one, will allow access to all.

D. Dual-Factor Authentication.

All are accustomed to login information and passwords. Increasingly, however, tools like "Safecracker" which have long been available to network administrators for benign purposes like helping out an authorized user who has forgotten his password are now openly for sale on the Dark Web. The best, most affordable, least invasive defense is to have a separate program which generates an additional, time-limited code which must also be put in to allow access. Usually, this will be installed on a separate device. The process is called "Dual-Factor Authentication" – the first factor being the login and password, and the second factor being the time-limited code that comes from somewhere else. For example, where "dual factor authentication" is employed, the user enters her login and password onto her laptop, then uses an app on her cell phone to generate an additional multi-numbered code which she quickly enters onto her laptop before it times out. "Dual factor authentication" is not perfect, but it does vastly increase the cost and complexity of breaking into the system through formulaic logins and easy passwords.

E. Prepare an Incident Response Plan.

Fundamental to any kind of security plan is an Incident Response Plan, a detailed set of steps to take to identify, analyze, respond to, and then learn from any cyber incident. Like any plan, the more thought and effort goes into the IRP, the more use it will be. Elements of an IRP usually include the following (among many, many others):

- Instructions to call counsel at once (with names and contact numbers), to preserve privilege while determining if the Incident is a "Breach" requiring widespread notification;
- Names and contact information of a team of relevant people;
- Diagnostic steps to determine what has happened, how widely it has spread, what business data has been compromised, what personal data has been accessed or disclosed, and what systems are affected;
- Isolation and Containment steps;
- Business Continuity, typically through back-ups which are maintained offline and are therefore separate from the affected systems;
- Information flow and control; and
- Post-Mortem: learning from and improving systems.\

F. "Tabletop Exercises."

The best way to test an IPR is to practice it, in a conference room. This is called "running a Tabletop Exercise," and is best conducted by an experienced outside cybersecurity firm. After consulting with the client and learning about the business, the firm will assemble the client's team in a room and start introducing a series of "facts" in a scenario. Much as in real life, it will only introduce a few facts at first, and the team will have to decide what to do next. Then there will be more, and more, and faster, with some that are wholly extraneous and some very important ones hidden deep in the pile. It is always surprising how much the team learns – about what to anticipate, whom to call, where surprises are likely to come from, and above all, what else they must prepare to face.

G. Fill in the Blank: "My Vendor's Friend is My…..?"

In contracting for digital products or services, it is common enough to consider the vendor's warranties, disclaimers, indemnification, insurance, and data protection policies – not just its cybersecurity defenses, but also its policies regarding data collection, transfer, storage, use, disclosure, and disposal. What is much less common – but no less important – is consideration of the same policies of the vendor's *subcontractors*, and even of its *subcontractors' subcontractors*. Ironically, the more trusted the vendor, the more likely it is that the vendor trusts its subcontractors, and the higher the risk of error. Today, the same techniques that have been developed for use in clothing and shoe-manufacture supply chains mostly with respect to fair-labor practices, and for use in the food industry to ensure quality and safety, should be adapted to use in the data-protection

industry to ensure data protection all the way up and down the line.

H. "Who will Guard the Guards Themselves?"

Keep a close eye always on "administrative controls," or logins and passwords that are used for access at an administrative level. Surprisingly often, administrative access is intended to be for a limited time or limited scope, but somewhere between "I thought that was taken down after the project was over," and "nobody told me to do that," the admin authority is left up. Security checks frequently find whole pages of administrative logins and passwords which should have been taken down long before, but somehow weren't, leaving the company vulnerable to easy intrusion.

IV. THE EVIL DAY: MANAGING A "BREACH"

No single federal law governs the security of all personal data. Determining which federal law applies largely depends, in part, on the regulations applicable to the entity that collected the data and the type of data that was collected and regulated. Further, data breach notification requirements have largely been determined by state legislatures.

As of March 2018, all fifty states currently have data breach notification statutes on their books. It is important to be aware, however, that not all fifty statutes are alike. They have similarities, but their reach (computerized data only? Or paper products as well?), definitions (does it apply only to encrypted data? Is a "breach" only unauthorized "use" and/or "disclosure," or also unauthorized "access?"), and obligations (report breaches to the Attorney General as well as affected individuals? Report when – as soon as practical? within 30 days? 45?), vary widely.

The Texas breach notification statute is found at Tex. Bus. & Com. Code § 521.053. It requires that a person who conducts business in Texas and "owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Tex. Bus. & Com. Code § 521.053(b). (If a person merely "maintains" it and does not own or license it, that person must notify the person who does own or license it.) *Id.* at (c).

A. Definition of a "Breach."

Not every security "incident" is a breach. The definition of "breach" is very specific and the consequences of suffering a true breach may be severe, and so as soon as an incident comes to light, it is wise to consider carefully whether it rises to the level of a "breach" as defined by the Texas statute or other controlling authority(ies).

Under the general Texas statute, a "breach of system security" means "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data." *Id.* at (a). This leaves at least five (5) openings to argue that an incident is not a "breach," and thus to preclude the requirement of notifying data subjects and others.

- Has the data been "acquired?" or has it been merely "accessed," which is not necessarily the same thing? (Or is it merely "unaccounted for," as old files in warehouses sometimes are, and which may be a third thing entirely?)
- Is the affected data "computerized," or merely on paper in boxes in a warehouse?
- Does it "compromise the security, confidentiality, or integrity" of sensitive personal information? (Perhaps there are historical or other facts to indicate that the acquisition does not.)
- Is the affected information "sensitive," or merely "personal identifying" as described above?
- Was it encrypted? If so, then apparently it would not be subject to the notification requirements, unless the invader also has the key.

It is important to remember that while all states now have some kind of data-breach notification requirements, those requirements differ markedly from state to state; so what may not be required in one may be certainly required in one or more others. Also, federal and state requirements in specific industries, such as healthcare (HIPAA, H.B. 300) and finance (Gramm-Leach-Bliley) have separate notification requirements.

B. *Whom* to Notify.

In Texas, the general requirement is to notify the data subject, namely, the individuals whose sensitive personal information is affected. Tex. Bus. & Com. Code § 521.053(b). Unlike other states, Texas does not require that the Attorney General be notified also. If however more than 10,000 persons must be notified, the business must also report to each consumer reporting agency that maintains files on consumers on a nationwide basis (such as TransUnion, Experian, and Equifax) of the timing, distribution, and content of the notices. *Id.* at (h).

In addition, there may be any number of (i) data subjects in other states, (ii) industry regulators, (iii) insurance carriers, (iv) contractual counterparties, and others who must be notified. To repeat, for emphasis: each state has different requirements. Almost all apply to breaches of data security with respect to its residents, so a company doing business in more than one state (or

in only one state but serving customers from many states) may have to comply with a myriad of different requirements at once.

C. *When* to Notify.

In Texas, the general requirement is to notify "as quickly as possible, except as [law enforcement may request or as] necessary to determine the scope of the breach and restore the reasonable integrity of the data system." *Id.* at (b). Various other statutes may have other specific timeframes, such as HIPAA (within 45 days) or the new European General Data Regulation (72 hours or without undue delay, depending on whether your organization respectively qualifies as 'controller" or "processor" of "personal data").

V. TEXAS DEPARTMENT OF INFORMATION RESOURCES (GOVERNMENT INFORMATION AND COMMUNICATIONS TECHNOLOGY)

The Texas Department of Information Resources ("DIR"), www.dir.texas.gov, describes its mission as "to provide technology leadership, solutions, and value to Texas state government, education, and local government entities to enable and facilitate the fulfillment of their core missions." It provides a wide variety of contracts, "shared" services that allow state agencies to access managed IT as a service, information services, reference materials, programs, data coordination and project management services, suggestions of approved suppliers, educational events and materials, and much more.

A. Texas Cybersecurity Strategic Plan

Earlier in 2018, the Office of the Chief Information Security Officer of Texas worked with the Statewide Information Security Advisory Committee to create a five-year, statewide strategic plan. http://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=163

The Strategic Plan focuses on five initiatives, all generally focused on assisting Texas state agencies and entities to improve their cybersecurity:

- ***Engagement***: Foster state and agency leadership engagement for cybersecurity initiatives;
- ***Tooling***: Provide proactive cybersecurity defense through insight and technology;
- ***Staffing***: Ensure adequate knowledge, skills, and experience of the cybersecurity workforce;
- ***Response***: Minimize the detection and response time for security events; and
- ***Outreach***: Establish a cybersecurity outreach program to increase awareness of cybersecurity best practices.

B. Texas Cybersecurity Act (H.B. 8)

Effective September 1, 2017, various sections of the Government Code were amended to include House Bill 8, known as the "Texas Cybersecurity Act." https://capitol.texas.gov/tlodocs/85R/billtext/html/HB00008F.htm . The Act will affect how state institutions (and universities) implement cybersecurity. Its particulars include (among numerous others):

- Including in an agency's sunset review an assessment of its cybersecurity practices;
- Establishing an Information Sharing and Analysis Center for agencies to share information regarding cybersecurity threats, best practices, and remediation strategies, as well as a Cybersecurity Council;
- Providing mandatory guidelines for requiring continuing education in cybersecurity for IT employees;
- Providing for breach notifications by state agencies to the same extent as required of persons who do business in Texas;
- Requiring an information security assessment at least every two years;
- Requiring data security plans for online and mobile applications;
- Requiring a state agency to "identify information security issues and develop a plan to prioritize the remediation and mitigation of these issues," with detailed instructions of what is to be included in the plan; and
- Requiring various studies to be conducted, including of the adequacy of election security, digital data storage and records management practices, and associated costs.

C. Texas Administrative Code, Sec. 202 (Infosec Standards)

Section 202 of the Texas Administrative Code sets forth detailed requirements for information security standards and practices. The Department of Information Resources is largely responsible for establishing the control standards, and for the agencies and their information security officers to follow. (An agency may establish a higher standard, of course.) http://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202