



Straight Talk:
IP and Technology Developments
October 2011

ANDREWS
ATTORNEYS **KURTH** LLP

STRAIGHT TALK IS GOOD BUSINESS.®

andrewskurth.com

Articles

What's in a Tweet?

Michele P. Schwartz and Prisca LeCroy

IP and Technology Developments - October 2011

October 25, 2011

What does it mean to “tweet”? In 1972, the year of Michael Jackson's debut solo album and his chart-topping hit cover of *Rockin' Robin*, the answer was easy—tweeting is what a robin does. But a networked person in 2011 would give a different answer. To “tweet” is to use the internet service Twitter® to broadcast a pithy message to your entire social network—a system useful for anything from organizing the overthrow of an oppressive regime, to informing the world that you are eating a sandwich ... a really good sandwich. But when Twitter sought to register the term, which has become one of the most internationally recognized marks of our day, the application was denied.

The denial was due to a prior service mark registration owned by Twittad, a company that provides advertising services on Twitter, for the tagline “Let Your Ad Meet Tweets.” Because the word “Tweets” in this phrase is a direct reference to Twitter's services, Twitter was understandably displeased with this result. On September 8th, Twitter filed suit against Twittad in the Northern District of California requesting cancellation of Twittad's registration for the tagline.

What is interesting about this lawsuit is not that Twitter would object to another company's derivative use of the term “Tweet” to the exclusion of Twitter itself. What's interesting is that Twitter didn't ask for more. Indeed, Twitter is not seeking to keep Twittad from using the phrase “Let Your Ad Meet Tweets.” Twitter just doesn't want the phrase to be a registered service mark.

Twitter's restraint is no doubt in part because third-party use of “tweet” actually helps Twitter. When other companies encourage their users to “tweet” or when they design services that make use of Twitter's platform, Twitter profits through the expanded use and advertising of its brand. But Twitter's restraint may also be due to the law that allows third parties to use other companies' trademarks as long as the use is in direct reference to the trademark holder's goods or services. This type of use is called “nominative fair use.”

Trademark infringement occurs when an infringer uses another company's mark—or something similar to the mark—to confuse the public into thinking that infringer's product is created or endorsed by the mark holder. Nominative fair use occurs when you use the mark to refer to the mark holder's product—perhaps to compare it to your own product or to explain how your product works with the mark holder's product. Thus, Chevrolet is permitted to use the mark Ford® in truthful advertising that compares Ford® trucks to Chevy® trucks, and the producer of a generic toner refill can say on its packaging that its product is compatible with Canon® printers if this is accurate.

Different courts have applied different factors for finding nominative fair use and have differed over whether it is an affirmative defense or merely an alternate means for determining whether the public is likely to be confused. But the analysis basically comes down to two questions: Has the user employed the mark more than is necessary to identify the mark holder's product and has the user done anything, other than use the mark itself, to imply sponsorship or endorsement by the mark holder? If the answer to these questions is “no,” the use is probably not infringing. In the seminal case on nominative fair use, the 1990's boy band “New Kids on the Block” sued a newspaper for running a poll asking teenyboppers to call a “900” number to vote for their favorite “New Kid.” The court ruled in favor of the newspaper, finding that the newspaper had not used the trademark beyond what was necessary to identify the band and that the newspaper had not implied that “New Kids” actually sponsored or endorsed the poll.

But perhaps the greatest takeaway from Twitter's lawsuit is that even the most successful companies can forget to register their trademarks. (Click here to see our previous article on the importance of registering trademarks at the start of a new venture.) A trademark can be more than merely the name of your business. Twitter is, in fact, the owner of the trademark “Twitter.” But Twitter did not think of registering “Tweet,” an important term associated with Twitter's service, until several years after Twitter began doing business. At that point, numerous other companies, including Twittad, had filed applications to register Tweet-based marks, causing Twitter's current dilemma. Other companies should learn from Twitter's mistake and

Articles

seek registration for any terms or phrases that are integral to their products or advertising efforts as soon as possible. As they say, “The early bird catches the worm and lives to *tweet* about it.”

For more information, please email IPandTech@andrewskurth.com.

Click the links below to contact the authors of this article.

Michele Schwartz or Prisca LeCroy

Other articles from this issue of *IP and Technology Developments*.

- [The U.S. Has a New Patent Law](#)
 - [The Federal Circuit’s Recent Reexamination Rulings](#)
 - [Is an Isolated DNA Patentable?](#)
 - [Three Large States Revise Their Security Breach Notification Laws and Texas Applies Its Law to Residents of Some Other States to Boot](#)
-

[Download a PDF of the entire issue.](#)

Articles

The U.S. Has a New Patent Law

Taylor P. Evans

IP and Technology Developments - October 2011

October 25, 2011

President Obama signed the Patent Reform Act of 2011 into law on September 16, 2011. Below is a summary of selected provisions of the Act.

First to File

Effective March 2013, the U.S. patent system will change from a first-to-invent to a first-to-file system. This means that if two people make the same invention and there has been no public disclosure of the invention, and both describe and claim that invention in separate patent applications, the inventor that filed his patent application first gets the patent. Thus, filing early will be more critical than ever before. Companies should consider filing a provisional application for an invention as early as possible, possibly followed by additional provisional applications as the technology of an invention develops, with a non-provisional application within a year of the first provisional application. The first-to-file provision will have no effect on existing patents or applications filed before March 2013.

Post-Grant Challenges

Effective September 2012, third parties will be able to challenge the validity of patents within nine months of issuance in the Patent Office in a Post-Grant Opposition Review proceeding. Any basis for a validity challenge will be entertained, including questions of novelty and obviousness, as well as challenges based on non-patentable subject matter or an improper written description or other formalities. After nine months, third parties may challenge patents through Inter Partes Review, which will replace existing Inter Partes Reexamination proceedings. In an Inter Partes Review, invalidity challenges must be based only on prior patents and printed publications.

In view of these changes, companies planning to initiate Inter Partes Reexamination proceedings should do so prior to September 2012. In addition, companies should arrange a monitoring program to identify patents that relate to the company's product line for possible challenge in a Post-Grant Opposition Review proceeding upon issuance. Similarly, patentees should be aware that a significant challenge against their patents in the patent office may develop, and they should be prepared to defend against challenges from competitors when their own patents issue.

False Marking

The new Act severely limits false marking lawsuits. Only the federal government and direct competitors that have been damaged can sue for false marking. Furthermore, non-government litigants will no longer be able to collect five hundred dollars in damages per item. In addition, it is no longer actionable not to remove expired patent numbers from products. The new law also provides for "virtual marking," by which a company marks its product with "Patent" or "Pat.," followed by a web address. The corresponding website displays the patent marking information and must be available to the public at no charge. These changes apply retroactively to existing cases.

Disjoinder

The new law bars plaintiffs from suing multiple defendants in the same suit if the only thing that the defendants have in common is that they are alleged to infringe the same patent(s). Courts will also be barred from consolidating cases involving different defendants according to the same criteria, except that unrelated parties may still be joined for purposes of discovery. This provision applies to all suits filed on or after September 16, 2011.

Articles

Supplemental Examination

Supplemental examination is a new post-grant procedure that will allow a patentee to cure possible inequitable conduct by presenting previously withheld information to the Patent Office after issuance of a patent. After the previously withheld information is presented, and if the claims are allowed again, that information cannot be used in later court proceedings. Supplemental examination proceedings cannot be commenced or continue once an infringement action has been brought.

Assignee Filing

Under the new Act, a company can file a patent application on behalf of an inventor where the inventor is under obligation to assign its rights to the company and refuses to sign the oath or declaration. This provision will become effective in September 2012.

Fees

Effective September 26, 2011, all Patent Office fees will be subject to a 15% surcharge.

Other Changes

There are numerous other changes to the patent system under the Patent Reform Act of 2011, including, for example, elimination of the "best mode" requirement, and changes unique to specific types of inventions, such as business methods or computers. For additional information or to discuss all the new changes in more detail, please call us.

For more information, please email IPandTech@andrewskurth.com.

Click the link below to contact the author of this article.

Taylor P. Evans

Other articles from this issue of *IP and Technology Developments*.

- What's in a Tweet?
 - The Federal Circuit's Recent Reexamination Rulings
 - Is an Isolated DNA Patentable?
 - Three Large States Revise Their Security Breach Notification Laws and Texas Applies Its Law to Residents of Some Other States to Boot
-

Download a PDF of the entire issue.

Articles

The Federal Circuit's Recent Reexamination Rulings

Gregory L. Porter

IP and Technology Developments - October 2011

October 25, 2011

Last month I wrote about how the Federal Circuit overturned a patentee's \$29.4 million infringement verdict and held that canceling dependent claims in a reexamination without changing the language of the independent claims narrowed the claim scope due to intervening rights. *Marine Polymer v. Hemcom*. Since then the Federal Circuit has issued an additional opinion pertaining to concurrent district court and PTO proceedings.

The recent case of *Bettcher Industries, Inc. v. Bunzl USA* pertained to a concurrent *inter partes* reexamination and district court case and the effect of 35 U.S.C. § 315(c). 35 U.S.C. § 315(c) states in pertinent part:

[a] third-party requester whose request for an *inter partes* reexamination results in [reexamination]...is estopped from asserting at a later time, in any civil action...the invalidity of any claim finally determined to be valid and patentable on any ground which the third-party requester raised or could have raised during the *inter partes* reexamination proceedings.

In *Bettcher* the accused infringer instituted *inter partes* reexamination proceedings and the validity of the claims was upheld by the Examiner and Board of Appeals. The patentee argued to the district court that the accused infringer should now be precluded from relying on the same prior art that was considered in the reexamination. In a case of first impression, the Federal Circuit held on October 3rd that the estoppel provisions in 35 U.S.C. § 315(c) do not take effect until the conclusion of all appeals, including any Federal Circuit appeals. Thus, the *Bettcher* case differs from last month's *Marine Polymer* case. In *Marine Polymer* the patentee's arguments in a pending, non-final reexamination adversely impacted the patentee's co-pending district court case. Here the reexamination patentee's district court case will not be affected by the *inter partes* reexamination until the exhaustion of all appeals including a Federal Circuit appeal.

As a practical matter the *Bettcher* case means that it may take roughly six years from the inception of an *inter partes* reexamination before any estoppels provided for by the statute take effect. That is currently the average time it can take to navigate a PTO *inter partes* reexamination through to a final Federal Circuit decision. Fortunately, the new America Invents Act will lessen this time since estoppel is to take effect when a Board decision is delivered at the PTO as opposed to after final Federal Circuit review. However, the *inter partes* review provisions of the America Invents Act do not take effect until September 16, 2012. Therefore, practitioners involved in PTO reexaminations and district court litigations will have to continue to fully and carefully coordinate the PTO and litigation strategies and their respective timing to optimize the chances for success at both the PTO and district court.

For more information, please email IPandTech@andrewskurth.com.

Click the link below to contact the author of this article.

Gregory L. Porter

Other articles from this issue of *IP and Technology Developments*.

- The U.S. Has a New Patent Law
 - What's in a Tweet?
 - Is an Isolated DNA Patentable?
 - Three Large States Revise Their Security Breach Notification Laws and Texas Applies Its Law to Residents of Some Other States to Boot
-

Articles

Is an Isolated DNA Patentable?

Ping Wang, M.D., Peter Brunovskis, Ph.D. and Michael Ye, Ph.D

IP and Technology Developments - October 2011

October 25, 2011

Is DNA patentable? Are isolated genes representative of what the Supreme Court characterizes as patent-ineligible "products of nature"? In a much anticipated decision, the Federal Circuit recently reversed a District Court's decision that Myriad Genetics' composition claims to "isolated DNA" are unpatentable under 35 USC § 101.

The disputed patent claims were directed to DNA compositions associated with breast cancer and methods for using these isolated DNAs for diagnosing breast cancer and screening for potential cancer therapeutics targeting breast cancer. More than 20 plaintiffs, including researchers, professional societies, and women affected by cancer brought the lawsuit against Myriad Genetics and the United States Patent & Trademark Office. Myriad Genetics, which owns the patents, carries out commercial testing for mutations in the breast cancer susceptibility genes, BRCA1 and BRCA2. Much of the controversy and debate centered on whether gene patents incite or hinder innovation. Many believe that they drive up costs and squelch competition.

In a 2-1 ruling reflecting the controversy surrounding the validity of gene patents, Judges Lourie and Moore agreed that isolated DNAs are patentable, "human-made inventions" exhibiting "markedly different characteristics" from what is found in nature. Writing for the majority, Judge Lourie held that "isolated DNAs, not just cDNAs have a markedly different chemical structure compared to native DNAs" and constitute a "distinct chemical entity" distinguished from their corresponding DNAs in nature by cleavage from native DNAs through removal of covalent bonds. Judge Moore agreed that the DNAs in question are not products of nature, but emphasized that such products are not automatically patentable subject matter *per se*, except in this case they are, since "the isolated DNA sequences have markedly different properties which are directly responsible for their new and significant utility." In his dissenting opinion, Judge Bryson agreed that cDNAs are patent eligible, but held that the disputed intron-containing DNAs are patent-ineligible because they fail the Supreme Court's *Chakrabarty* standard insofar as the genetic coding material is the same, structurally and functionally, in both the native gene and the isolated form of the gene. Judge Bryson further opined that "a contrary ruling is likely to have substantial adverse effects on research and treatment in this important field."

The Court further affirmed the District Court's decision that Myriad's method claims for "analyzing" or "comparing" gene sequences were invalid, since "they claim only abstract mental processes (e.g., '...wherein a difference in sequence indicates an alteration in sequence.')" and reversed the District Court's decision that Myriad's cancer therapeutic screening claims were invalid, since the claims do not merely recite abstract method steps, but rather "transformative steps...present[ing] 'functional and palpable applications' in the field of biotechnology."

The decision was reassuring to many in the biotech industry whose 40,000+ DNA-related patents and 2,645 patents claiming "isolated DNA" issued over the past 29 years could have been rendered invalid. Nevertheless, the decision is unlikely to end the debate, given the strong sentiments surrounding the case and the unresolved issues under 35 USC §101 that remain open to debate. It is likely that requests for *en banc* rehearing or petitions to the Supreme Court will follow.

For more information, please email IPandTech@andrewskurth.com.

Click the link below to contact the author of this article.

Ping Wang, M.D.

Other articles from this issue of *IP and Technology Developments*.

- [What's in a Tweet?](#)

Articles

- The Federal Circuit's Recent Reexamination Rulings
- The U.S. Has a New Patent Law
- Three Large States Revise Their Security Breach Notification Laws and Texas Applies Its Law to Residents of Some Other States to Boot

[Download a PDF of the entire issue.](#)

Articles

Three Large States Revise Their Security Breach Notification Laws and Texas Applies Its Law to Residents of Some Other States to Boot

Jeff Dodd

IP and Technology Developments - October 2011

October 25, 2011

Over forty states have adopted laws requiring businesses to implement some form of security procedures with respect to specified data relating to individuals¹ and to provide notice when those data security measures have been breached. While the structures of these laws often share common elements, the requirements vary somewhat. So, the problem for businesses is navigating the thicket of state laws when responding to data breaches potentially affecting the residents of several states. Three states—Texas, California and Illinois—recently amended their statutes. For those companies doing business across the United States that have comprehensive data notification plans, the changes are not so earth-shattering that your plans will change significantly (though you will need to address the particular changes). For those who do not have comprehensive plans, you will need to be aware that if you are afflicted with a breach, you will have to move quickly to assess your notification obligations under state laws that are stubbornly non-uniform.

Let us start with Texas. Before recent amendments, the Texas Business and Commerce Code required a “person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information” who suffers “any breach of system security”² to notify each “resident of this state whose sensitive personal information³ was, or is reasonably believed to have been, acquired by an unauthorized person.”⁴ In essence, as with many states, the Texas notification statute required two ties to Texas for the statute to apply: the person with the notification duty had to conduct business in the state and the potentially affected persons had to be residents of Texas. Notice must be given as “quickly as possible” after “discovering or receiving notification of the breach,”⁵ and the statute also sets forth acceptable manner of giving notice of the data breach.⁶ Prior to recent amendments, the Texas statute imposed civil penalties for violations payable to the State of Texas of “at least \$2,000 but not more than \$50,000 for each violation.”⁷ In addition, a violation of the data notification statute is also “a deceptive trade practice actionable under Subchapter E, Chapter 17.”

In 2011 Texas amended these provisions.⁸ Most interestingly, Texas attempted to address one issue associated with a data breach potentially affecting residents of more than one state. Suppose, for example, a business does business in Texas and suffers a security breach affecting Texas residents and residents of another state that has no notification regime. The Texas legislature amended Texas law to make the notification obligation of a person conducting business in Texas run not only to any resident of Texas but also to any other resident in a state “that does not require” notification. If a state requires “a person described by Subsection (b)” to provide notice of a breach of system security, “the notice of the breach of system security provided under that state’s law satisfies the requirements of Subsection (b).”

Here is the twist, however: Texas’ statute may now reach, not only to the residents of states that have no notification statute, but also in one important set of circumstances to residents of those states that do. Bear with me here as I walk through the logic. A person “described by subsection (b)” is, presumably, a person “who conducts business in [Texas] and owns or licenses computerized data.” Many other states trigger notice obligations based when a person does business in their states, but the notice obligations run only to the residents of their states. Texas followed a similar approach before the amendments. Accordingly, before the amendments, if a company did business in Texas and suffered a security breach it had to notify residents of Texas, but the Texas statutes did not require notice to the residents of other states. That was left to other state law.

Now notice obligations run to all residents of all states as a threshold matter. Then in a new subsection (b-1), the amendments carve back on the scope of coverage: notice must be provided to residents of Texas and to residents of “another state that does not require a person described by Subsection (b)” —i.e. a person doing business in Texas owning or licensing computerized data—to provide notice of a security breach.⁹ Clearly, if a company does business in Texas and in another state with a security breach notice statute, that company will be required to provide notice to potentially affected Texas residents under Texas law and notice to residents of the other state under the other state’s law. Suppose, however, an

Articles

enterprise does business in Texas and does not do business in another state (let us get creative and call it State X), but the residents of State X are potentially affected by the breach. If State X has a notification statute, but its statute has a double trigger—i.e., imposing obligations on the enterprise doing business in State X to provide notice to residents of State X—then technically a person doing business in Texas but not in State X would not be required to provide notice to residents of State X under State X’s law. In that circumstance, as well as the situation where the other state has no breach notification law at all, the amendments to Texas law would require notice to potentially affected residents in the other states. We Texans are big-hearted enough to require notice to you even if your state does not.

The amendments also substantially increased the civil penalties for a failure to provide timely notice. *In addition to* the civil penalty payable to the State of Texas of “at least \$2,000 but not more than \$50,000 for each violation,”¹⁰ the amended statute provides that “a person who fails to take reasonable action to comply with Section 521.053(b) is liable to this state for a civil penalty of not more than \$100 for each individual to whom notification is due under that subsection *for each consecutive day that the person fails to take reasonable action* to comply with that subsection. Civil penalties under this section may *not exceed \$250,000 for all individuals to whom notification is due after a single breach.*”¹¹ Since this enhanced penalty is based on the number of individuals to which notice is not timely given, and since the statute now applies to at least some non-Texas residents, Texas may well collect for the alleged sins of Texas businesses affecting residents of other states.¹² We Texans are not only big-hearted, but we also know how to expand our revenue base. Bottom line: If you do business in Texas, it would pay to provide notice wherever you do business and to adopt policies that prescribe how notice will be given.¹³

California and Illinois also amended their data breach statutes to describe with some specificity what must go into the breach notices. California’s law, as with Texas’ law, applies to persons conducting business in its state but requires notice to be given only to California residents. In recent amendments to Section 1798.82 of its Civil Code, California tinkered with its notice requirements.¹⁴ The notices must be written in “plain language”—I will defy you to cite an instance where a business issuing a notice says that it has written it in “unplain language”—and must set out the following:

- “The name and contact information of the reporting person or business.”
- “A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.”
- If “possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.”
- “Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.”
- “A general description of the breach incident, if that information is possible to determine at the time the notice is provided.”
- The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver’s license or California identification card number.

The revised law also provides that at “the discretion of the person or business, the security breach notification may also include any of the following: (A) Information about what the person or business has done to protect individuals whose information has been breached and (B) Advice on steps that the person whose information has been breached may take to protect himself or herself.” The problem, of course, is exactly what duties a business undertakes by setting out the protective measures it has taken and by providing advice as to protective measures.¹⁵ Finally, the revised law requires that a sample copy of the notice be submitted to the California Attorney General if the notice is being required to be sent to more than “500 California residents as a result of a single breach of the security system.”

Illinois also amended its statute this year to be more specific as to the notice requirements.¹⁶ As amended, the law will require that notices to Illinois residents must “include, but need not be limited to, (i) the toll-free numbers and addresses for consumer reporting agencies, (ii) the toll-free number, address, and website address for the Federal Trade Commission, and (iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes.”¹⁷

Articles

Again, as I mentioned above, none of this is particularly earth-shattering and most data response plans would cover this type of information, but not all states require exactly the same type of information and so companies should take a look at their plans.

Also, prior to the amendments, data collectors maintaining data including personal information that they did not own or license had to notify owners or licensees of the data of a breach of its security measures. The amendments now require more of such service providers. "In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach."¹⁸ I note that the scope of the obligation to cooperate is not limited to the enumerated steps; rather the statute imposes a general, roving duty to cooperate.¹⁹

In the final analysis, the recent amendments to the Texas, California and Illinois security breach notification laws do not fundamentally change the way businesses that suffer a breach must approach giving notice of the breach, but the amendments underscore that each state may impose somewhat different obligations. Since the time to provide a notice is at a premium when a breach occurs (and since penalties can be quite heavy), we suggest that businesses operating in several states develop plans for compliance with the laws of those states before a breach occurs; for those with such plans in place, you should take a look at the new requirements to determine what, if anything, should be revised in your plans.

For more information, please email IPandTech@andrewskurth.com.

Click the link below to contact the author of this article.

Jeff Dodd

Other articles from this issue of *IP and Technology Developments*.

- [What's in a Tweet?](#)
- [The Federal Circuit's Recent Reexamination Rulings](#)
- [The U.S. Has a New Patent Law](#)
- [Is an Isolated DNA Patentable?](#)

[Download a PDF of the entire issue.](#)

1. For example, Section 521.052 of the Texas Business and Commerce Code requires a business to "implement and maintain reasonable procedures, including taking 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." Section 521.052(b) does not apply to "financial institutions" (as defined by 15 U.S.C. Section 6809) but, interestingly enough, it does apply to "a nonprofit athletic or sports association."

2. 521.053(a) of the Texas Business and Commerce Code provides that "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."

Articles

3. "Sensitive personal information" is defined as an unencrypted first name or first initial of the first name with a last name in combination with one or more of the following: (a) social security number, driver's license number or government-issued identification number; (b) "account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account"; or information identifying an individual and relating to "the physical or mental health or condition of the individual," "the provision of health care to the individual," or "payment for the provision of health care to the individual." Texas Business and Commerce Code Section 521.002(a).

4. 521.053(c) also provides that any "person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

5. Prompt notice is excused to the extent necessary "to determine the scope of the breach and restore the reasonable integrity of the data system" or to the extent requested by "a law enforcement agency that determines that the notification will impede a criminal investigation."

6. 521.053(e) sets forth methods for providing notice, but 521.053(g) provides businesses with discretion to set their own procedures: "Notwithstanding Subsection (e), a person who maintains the person's own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy."

7. Section 521.151 of the Texas Business and Commerce Code clearly vests the discretion in the Texas Attorney General as to whether to bring the action. It also allows the Texas Attorney General to see equitable relief and to recover reasonable expenses.

8. H.B.ANo.A300. The amendments take effect September 1, 2012.

<http://www.capitol.state.tx.us/tlodocs/82R/billtext/pdf/HB00300F.pdf#navpanes=0>

9. Here is the new exception in full:

(b-1) Notwithstanding Subsection (b), the requirements of Subsection (b) apply only if the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of this state or another state that does not require a person described by Subsection (b) to notify the individual of a breach of system security. If the individual is a resident of a state that requires a person described by Subsection (b) to provide notice of a breach of system security, the notice of the breach of system security provided under that state's law satisfies the requirements of Subsection (b).

Texas Business & Commerce Code 521.053(b-1)(effective September 1, 2012).

10. Section 521.151(a) of the Texas Business and Commerce Code.

11. Texas Business & Commerce Code 521.053(b-1) (effective September 1, 2012).

12. Texas also extensively revised its Health and Safety Code requirements as to data security and privacy to reach beyond the obligations of the Health Information Portability and Accountability Act.

13. As I mentioned above, Texas Business & Commerce Code 521.053(g) provides businesses with discretion to set their own procedures: "Notwithstanding Subsection (e), a person who maintains the person's own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy."

Articles

14. Senate Bill No. 24, Chapter 197, approved by the Governor of California on August 31, 2011.

http://www.infolawgroup.com/uploads/file/sb_24_bill_20110831_chaptered.pdf.

15. Consider the following question: By stating that a notice “may” include such other information, does the statute imply that the prescribed and identified permissive information is the only information that can be included in a notice?

16. HB 3025, Public Act 097-0483.

<http://www.ilga.gov/legislation/fulltext.asp?GAID=11&SessionID=84&GA=97&DocTypeID=HB&DocNum=3025&LegID=60509&SpecSess=&Se>

In addition to the amendments summarized above, the statute imposes specific obligations concerning the disposal of data containing personal information. Several states have that requirement.

17. HB 3025, Public Act 097-0483, Section 10(a). Interestingly, the statute adds that the “notification shall not, however, include information concerning the number of Illinois residents affected by the breach.”

18. HB 3025, Public Act 097-0483, Section 10(b).

19. The amendments do not speak to cost reimbursement.

AUSTIN

111 Congress Avenue
Suite 1700
Austin, Texas 78701
512.320.9200

BEIJING

Room 2007, Capital Mansion
No. 6 Xin Yuan Nan Lu,
Chao Yang District
Beijing, China 100004
86.10.8486.2699

DALLAS

1717 Main Street
Suite 3700
Dallas, Texas 75201
214.659.4400

HOUSTON

600 Travis Street
Suite 4200
Houston, Texas 77002
713.220.4200

LONDON

Level 16, City Tower
40 Basinghall Street
London EC2V 5DE
England
44.20.7382.0550

NEW YORK

450 Lexington Avenue
New York, New York 10017
212.850.2800

THE WOODLANDS

Waterway Plaza Two
10001 Woodloch Forest Drive
Suite 200
The Woodlands, Texas 77380
713.220.4800

WASHINGTON, DC

1350 I Street, NW
Suite 1100
Washington, DC 20005
202.662.2700

ANDREWS
ATTORNEYS **KURTH** LLP

STRAIGHT TALK IS GOOD BUSINESS.®

Copyright © 2011 by Andrews Kurth LLP. Andrews Kurth, the Andrews Kurth logo and Straight Talk Is Good Business are registered service marks of Andrews Kurth LLP. All Rights Reserved. This brochure has been prepared for informational purposes only and does not constitute legal advice. This information is not intended to create (and receipt of it does not constitute) an attorney-client relationship. Readers should not act on this information without seeking professional counsel. Prior results do not guarantee a similar outcome and depend on the facts of each matter. Attorney Advertising.