



## TECHGEAR



The Asus Transformer Prime (starting at \$500) is an Android tablet with a quad-core processor and 10.1-inch screen.

An optional docking station adds a keyboard and extends the tablet's battery life to 18 hours.

## WEBLINKS



**PAUL STANFIELD** is an attorney with a background in pharmacy, general business practice, and technology-related issues. He practices with Stanfield Hiserodt, P.L.L.C., which concentrates its practice in technology areas.

### TechCrunch ([techcrunch.com](http://techcrunch.com))

Contains good, topical information on current tech issues, some of which even I can understand.

### TechDirt ([techdirt.com](http://techdirt.com))

Has a slight edge to its reporting on technology and associated legal issues.

### SlashDot ([slashdot.org](http://slashdot.org))

Contains a good compilation of articles and items for the nerdy side of me.

### Deadspin ([deadspin.com](http://deadspin.com))

Has a totally irreverent, scandalous, and often profane take on sports that I like.

### Crooks and Liars ([crooksandliars.com](http://crooksandliars.com))

Gives me my daily dose of left-leaning information.

# Your Law Firm's Duty to Protect Sensitive Personal Information

BY PAULA S. deWITTE, J.D., PH.D., P.E.

In the "old days" of hacking in the early 2000s, hacking was done for the thrill of taking over a system's resources. Hacking required extensive knowledge and skill. Today, hacking is done for profit. Hackers can download tools from the web and within 30 minutes create mayhem anywhere in the world. Most identity theft occurs in China and the former Soviet republics where criminals are not extradited to the United States.<sup>1</sup>

Identity theft is the crime that keeps on giving. Identities can be stolen and sold repeatedly. Victims spend their lives cleaning up their financial histories, responding to non-valid arrest warrants, and wondering what's next.

As identity theft increases, states are passing more aggressive laws targeted at the source — the businesses that maintain personal information. Texas enacted its own Identity Theft Enforcement and Protection Act (ITEPA)<sup>2</sup> in 2005 as a tie-in statute to its Deceptive Trade Practices Act.<sup>3</sup> Actual identity theft does not have to occur to trigger statutory fines or other remedies.

Identity theft steals sensitive personal information (SPI). SPI is an individual's first and last name in combination with the individual's social security number, driver's license number, or financial account number with access information. Just the name and social security number (found in any firm's employment records) triggers the statute's business duties.

What does this have to do with a law practice? Most law firms have adequate computer or network security (e.g., firewalls, virus detectors), but lack adequate physical security and personnel, which

account for many of the data breaches. Law firms tend to rely on their information technology (IT) staff for their information assurance (IA) functions. Just as one would not hire a family law attorney for a criminal matter, IT and IA require different training, skills, and certifications. IT personnel keep a law firm's systems running while IA keeps these systems secure.

Examples of bad security practices include:

- Client documents sent to personal or unencrypted email accounts to facilitate work from home;
- Stolen or unattended laptops;
- Weak passwords (e.g., a pet's name); and
- Discarded CDs or USB thumb drives containing SPI.

Computer or network security would detect none of these breaches. Physical and personnel-oriented security is required. Let's look at each of the three duties.

### Duty 1: Use reasonable procedures to safeguard SPI.

Who determines what's reasonable? The potential victim or the business maintaining SPI? Procedures must be documented and in writing so they can be communicated effectively and rigorously practiced. Procedures must be periodically reviewed with changes in technology or the security environment. Tomorrow's next big technology brings its own security vulnerabilities. Procedures must encompass all security — computer and networks, physical premises, and people.



*Identity theft is the crime that keeps on giving. Identities can be stolen and sold repeatedly. Victims spend their lives cleaning up their financial histories, responding to non-valid arrest warrants, and wondering what's next.*

**Duty 2: Destroy or arrange for the destruction of SPI.**

The law firm must identify and locate all SPI to destroy it. SPI in discovery documents or on forgotten USB drives, misplaced CDs, and back-up systems is easily overlooked. Once located, it must be destroyed. Many people mistakenly believe reformatting a hard drive, running a magnet over a hard drive, or discarding broken hard drives safely will destroy SPI. The most effective way to destroy SPI is to use certified software to overwrite drives or to shred drives, including broken drives. Most broken drives can still have their data accessed. Law firms cannot delegate the responsibility to a vendor. They must validate that vendors effectively destroy the data.

**Duty 3: Immediately notify individuals if the business reasonably believes a data breach has occurred or is notified that a data breach has occurred.**

Many firms first realize a data breach has occurred when they are notified by law enforcement or the victims. ITEP requires that potential victims be notified “immediately” and establishes different methods of notification depending on the number of records compromised. Changes in Texas law, which go into effect on Sept. 1, 2012, will increase the financial penalties for untimely notification as well as require, in some cases, notification to citizens of other states. Texas is keeping up with the most progressive states in protecting privacy.

**The Encryption Exception**

ITEP does make an exception for encrypted data. The statute does not define

what encrypted data is. Encryption is not a yes/no question, but rather a continuum from weak (and easily broken) to strong. Claiming data is encrypted is meaningless without knowing the level and extent of encryption.

More important, it is nearly impossible to encrypt an entire system — the hardware, software, remote devices, USB sticks, CDs, etc. If any part of the system is unencrypted, SPI is at risk. Some states’ laws make no exception for encrypted data, so the best bet is to put in place those reasonable SPI protection procedures and not rely on the encryption exception.

**Final Thoughts**

Consider Sony’s predicament. A Sony security breach affected 100 million people worldwide.<sup>4</sup> With a market capitalization of \$17 billion,<sup>5</sup> Sony will spend an estimated \$2 billion, more than 10 percent of its value, to remediate this breach under myriad countries’ and states’ laws. That’s a non-value added expense that contributes nothing to the bottom line.

So think, could your law firm afford 10 percent of its value for a security breach? ☹

**Notes**

1. For more information on this topic, see “*Loose Lips Sink Attorney-Client Ships: Unintended Technological Disclosure of Confidential Communications*,” St. Mary’s Law Journal, Vol. 39, No. 4, 781-818.
2. Bus. & Com. Code Ann. §521 (Vernon Supp. 2007) available at <http://www.statutes.legis.state.tx.us/Docs/BC/pdf/BC.521.pdf>.
3. Bus. & Com. Code Ann. §521.152 (Vernon Supp. 2007) available at <http://www.statutes.legis.state.tx.us/Docs/BC/pdf/BC.521.pdf>.
4. See [http://www.businessweek.com/news/2011-05-03/sony-data-breach-exposes-users-to-years-](http://www.businessweek.com/news/2011-05-03/sony-data-breach-exposes-users-to-years)

[of-identity-theft-risk.html](http://www.businessweek.com/news/2011-05-03/sony-data-breach-exposes-users-to-years-of-identity-theft-risk.html).

5. See <http://finapps.forbes.com/finapps/jsp/finance/compinfo/CIAAtAGlance.jsp?tkr=SNE>.



**PAULA S. deWITTE** divides her work between her professional engineering consulting practice and her law practice. She is one of fewer than 60 licensed Texas Professional Engineers in the area of software engineering. Contact her at [Paula.deWitte@PauladeWitte.com](mailto:Paula.deWitte@PauladeWitte.com).

**MARCELLUS?**

**We're here to help!**

- Oil & gas title examination & certification
- Leasing matters
- All real estate issues
- Agent of First American Title Insurance



**DAVIS & DAVIS**  
ATTORNEYS AT LAW

107 East Main St. • Uniontown, PA 15401  
**724-437-2799**





