businesslaw

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

Mc Graw Hill Education

Contents

Dear Professor,

I trust your spring semester is progressing nicely! Welcome to McGraw-Hill's February 2014 issue of Proceedings, a newsletter designed specifically with you, the Business Law educator, in mind. Volume 5, Issue 7 of Proceedings incorporates "hot topics" in business law, video suggestions, an ethical dilemma, teaching tips, and a "chapter key" cross-referencing the February 2014 newsletter topics with the various McGraw-Hill business law textbooks.

You will find a wide range of topics/issues in this publication, including:

1. The Target data security breach;

2. Tom Cruise's defamation lawsuit against a tabloid publisher;

3. A Louisiana teen's sentence for the wrestling-style killing of his sister;

4. Videos related to a) a communications director's firing for a controversial "tweet" and b) judicial action regarding gay marriage in Utah;

5. An "ethical dilemma" related to the National Security Administration's (NSA's) data collection practices; and

6. "Teaching tips" related to Article 1 ("Target Data Breach Spurring Lawsuits, Investigations") and Video 2 ("Utah Same-Sex Couples Getting Marriage Licenses").

Let us all hope for spring, with the promise that it brings!

Jeffrey D. Penley, J.D.
Catawba Valley Community College
Hickory, North Carolina

businesslaw

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

Mc Graw Hill Education

Of Special Interest

This section of the newsletter covers three (3) topics:

1) The Target data security breach;

2) Tom Cruise's defamation lawsuit against a tabloid publisher; and

3) A Louisiana teen's sentence for the wrestling-style killing of his sister.

Hot Topics in Business Law

Article 1: "Target Data Breach Spurring Lawsuits, Investigations"

http://www.usatoday.com/story/money/business/2013/12/22/target-breach-suits-and-investigations/4167977/

According to the article, consumer frustration and outrage over the Target credit card breach is moving from Facebook and Twitter to the courts and state governments even as the stolen accounts are flooding the black market.

Three class-action lawsuits have been filed in the wake of the theft of data on about 40 million credit and debit card accounts of shoppers at Target from November 27 to December 15. More than $5 million in damages is being sought in the cases, two of which were filed in California and one in Oregon.

The Attorneys General in at least four states -- Connecticut, Massachusetts, New York and South Dakota – have asked Target for information about the breach. That is the first step to a possible multi-state investigation into the breach.

Meanwhile, millions of the card accounts stolen have begun showing up for sale on the black market, says the security reporter who initially broke the news about the breach. "Credit and debit card accounts stolen in (the Target breach) ... have been flooding underground black markets in recent weeks, selling in batches of one million cards and going for anywhere from $20 to more than $100 per card," writes Brian Krebs on his KrebsOnSecurity.com site.

Recently, Target offered customers a 10% discount in its United States stores, after CEO Gregg Steinhafel said that the company would provide free credit monitoring to at-risk customers.

The company may need to do a lot more in the future. "With these data security breaches, there's usually the question of consumer confidence and trust," says Daren M. Orzechowski, a New York-based intellectual property attorney with White & Case LLP. "They have to balance if they feel they need to do more to try to preserve consumer confidence."

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

The speed of class-action suits and state officials getting involved "is not surprising," says Orzechowski, who deals in data privacy issues. Many states have strong breach notification laws that require the attorney general be notified, he said.

Both the state and civilian queries will be interested in "when did Target know there was an issue and how long did they wait, in terms of responding, because there's a lot of obligations on promptly notifying people and there is going to be a lot of focus on that in the days to come."

As of yet, there is no idea of how much consumers were harmed, says Columbia Law School professor John Coffee. "We do not yet know if Target was negligent or whether these were very skillful hackers who could have penetrated any system--but those critical factual issues seldom slow the race to the courthouse," he said.

Also investigating the Target breach -- the second-largest in United States history being a 2005 case involving retailer TJX -- is the Secret Service. Target is based in Minneapolis and has almost 1,800 stores in the United States and 124 in Canada, according to its website.

Target is directing customers to its website and a toll-free phone number for more information about the breach.

The breach could also lead to smarter, more hacker-resistant smart cards. "We are using 20th century cards against 21st century hackers," says Mallory Duncan, general counsel at the National Retail Federation. In the United States, most account info is contained on the magnetic strip on the card's back and is easily replicated. In the rest of the world, most cards contain digital chips that create a unique code, not easily copied, every time the card is used.

Discussion Questions

1. What is the legal basis for Target's potential liability to its customers for the data breach?

The legal basis for Target's potential liability to its customers for the data breach is negligence. In order to establish a viable claim for negligence, the plaintiff must establish, by the greater weight of the evidence, the following four elements:

a. The defendant owed a reasonable duty of care to the plaintiff;
b. The defendant violated the duty of care owed to the plaintiff;
c. The defendant proximately caused the plaintiff harm; and
d. The plaintiff experienced damages as a result of the defendant's breach of the reasonable duty of care owed to the plaintiff.

2. In your reasoned opinion, should Target be legally responsible to its customers for the criminal actions of the hacker(s)? Why or why not?

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

This question may ultimately be for the judicial system to decide. As the article indicates, the outcomes for both the government and the civilian cases depend on when Target knew there was a data security breach, and upon discovering the data security breach, how long the company waited before notifying customers. These are fact-specific issues that will be addressed during the discovery phase of litigation.

3. As the article indicates, three (3) class action lawsuits have already been filed in this case. In your reasoned opinion, should courts certify (in other words, acknowledge and allow) class actions against Target for the data breach, or should customers be required to file individual lawsuits on their own behalf?

This is an opinion question, so student responses will likely vary. In order to "certify" a class action case (in other words, in order to permit a class action case to proceed in the judicial system), the court must be convinced that those participating in the case have sufficient "commonality of interest" in their litigation against the defendant. A class action lawsuit can be advantageous to the plaintiffs who participate as members of the class, since they can "pool" their resources and enjoy certain "economies of scale" in proceeding against the defendant. If the class action lawsuits are not certified, customers will be required to find their own individual attorneys and file their own individual lawsuits if they choose to proceed against Target.

Article 2: "Tom Cruise Settles Defamation Lawsuit against Tabloid Publisher"

http://www.cnn.com/2013/12/21/showbiz/tom-cruise-suri-defamation/

According to the article, actor Tom Cruise has settled a $50 million defamation suit he filed last year against a tabloid publisher after it ran stories accusing him of having "abandoned" his daughter Suri during his divorce from her mother, actress Katie Holmes.

The lawsuit against Bauer Publishing, InTouch and Life & Style magazines "has been settled," said Lindsay Ferraro, public relations director for both magazines, in an e-mail. "The terms of the settlement were not disclosed and remain confidential."

Neither Bauer Publishing nor the magazines "intended to communicate that Tom Cruise had cut off all ties and abandoned his daughter, Suri, and regret if anyone drew that inference from anything they published," she added.

A court document noted that the suit was dismissed recently "with prejudice," meaning that it cannot be re-filed.

The one-paragraph settlement says the dismissal was agreed to by Cruise and the tabloid publisher and that each side was responsible for their own legal fees.

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

In a sworn affidavit filed last month in federal court, Cruise rejected as "patently false" the assertion that he had abandoned his daughter, now 7. "I have in no way cut Suri out of my life -- whether physically, emotionally, financially or otherwise," he said.

The publisher said then in a statement that both magazines "stand behind the reporting and articles at issue in Mr. Cruise's action."

The July 18, 2012 Life & Style cover carried the headline "SURI IN TEARS, ABANDONED BY HER DAD" along with a photo of the child. There was no accompanying text to explain the headline.

The complaint also pointed to an InTouch cover story from September 2012 headlined "44 DAYS WITHOUT TOM ... ABANDONED BY DADDY ... Suri is left heartbroken as Tom suddenly shuts her out and even misses her first day of school... HAS HE CHOSEN SCIENTOLOGY OVER SURI FOR GOOD?"

Cruise said his daughter often accompanied him during his travels around the world to make movies, which "allowed me to see my daughter while still fulfilling my obligations to my work, my colleagues, and the studios that hire me."

Discussion Questions

1. Define defamation.

Defamation, an intentional tort, is either a false statement or a bad faith opinion made about a person that damages his or her reputation in the community. Oral defamation is known as slander, while written defamation is known as libel. There are two (2) defenses to a defamation action: a) truth; and b) good faith opinion. If the defendant successfully argues that he or she asserted either a truthful statement or a good faith opinion about the plaintiff, the defendant prevails in the defamation action.

2. As the article indicates, Bauer Publishing, InTouch and Life & Style magazine have settled the defamation lawsuit involving Tom Cruise. Does the settlement constitute a legal admission of liability by the defendants? Why or why not?

A settlement does not constitute a legal admission of liability by the defendants Bauer Publishing, InTouch and Life & Style magazine. Instead, a settlement indicates an implicit acknowledgement by both parties that it is in their mutual best interests to resolve the dispute rather than have the judicial system make a final determination of liability.

3. In your reasoned opinion, did the defendants defame Tom Cruise? Explain your response.

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

This is an opinion question, so student responses will likely vary. A determination of defamation liability depends on the unique facts of a particular case. If jury is called upon to render a verdict regarding defamation, it will have to determine whether the facts of the case demonstrate that the defendant asserted either a false statement or a bad faith opinion about the plaintiff resulting in damage to the plaintiff's reputation in the community. The instant case appears to center on the word "abandon." Whether Mr. Cruise "abandoned" his daughter is a problematic question, since abandonment can be physical and/or psychological in nature. The settlement in this case is a clear indication that both the plaintiff Cruise and the defendants Bauer Publishing, InTouch and Life & Style magazine did not want to leave that question for the jury to answer by way of a verdict.

Article 3: "Louisiana Teen Sentenced for Wrestling-Style Killing of Sister"

http://www.cnn.com/2013/12/11/justice/louisiana-boy-sentenced/?iref=obnetwork

According to the article, a 13-year-old Louisiana boy has been sentenced to three years in a secure juvenile facility for killing his 5-year-old half-sister by performing pro-style wrestling moves on her.

The boy was left unsupervised with Viloude Louis at their home in the New Orleans suburb of Terrytown on June 16. Jefferson Parish authorities said the teen imitated "WWE-style" wrestling moves on the girl.

The children's mother left them at home when she went to the store, according to authorities.
The teen will get credit for the time he has already served. The facility where the boy will serve his sentence has not been identified.

In June, authorities said that the boy had described punching and jumping on the young girl and slamming her into her bed.

The teen was charged with second-degree murder.

WWE released a statement, offering its condolences.

"WWE supports Judge (Andrea Price) Janzen's summation that the 13-year-old boy absolutely knew that he was hurting his 5-year-old little sister. Therefore, it is illogical to conclude that the brutal and ultimately fatal beating of a 5-year-old little girl by a teenager could be confused with imitation of WWE moves seen on TV," it read.

The boy pleaded guilty to negligent homicide.

As part of the sentence, the state ordered that he be provided educational programming and therapy to help him tackle what Palermo described as anger management, grief and trauma. The teen's parents have been ordered to participate in his therapy.

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

In June, the Jefferson Parish Sheriff's Office said that the children's mother will not be charged.

Discussion Questions

1. As the article indicates, the thirteen-year-old juvenile defendant was charged with second-degree murder in the death of his five-year-old half-sister, and pled guilty to negligent homicide. Describe the difference between second-degree murder and negligent homicide.

Second-degree murder is defined as the intentional taking of the life of another human being without premeditation and deliberation. Negligent homicide, a lesser offense, is defined as the death of another human being that results from the criminally negligent actions of the defendant.

2. Should juvenile court or "adult" (in other words, ordinary) criminal court have jurisdiction over a case like this? Explain your response.

This is an opinion question, so student responses may vary. Although there has been a pronounced trend in the United States to try juveniles as an adult, the fact that the defendant is 13 years old makes a case like this particularly problematic. If the defendant was 17 years old (one year below the age of majority of 18) when the crime was committed, it would be easier to rationalize trying him as an adult. There is a remarkable difference between juvenile and regular criminal court when it comes to matters of crime and punishment; the juvenile system focuses on rehabilitation, while the regular criminal court system focuses on retribution and punishment. In the instant case, the state of Louisiana has considered this a matter for the juvenile court to address.

3. As the article indicates, the thirteen-year-old juvenile defendant was left unsupervised with his five-year-old half-sister while his mother went to the store. In your reasoned opinion, should the defendant's mother have any criminal responsibility for the young girl's death? Why or why not?

As a general rule, a parent is not responsible for the criminal actions of his or her child. This is based on the assumption that a parent cannot control the actions of his or her child "around-the-clock." As an exception to the general rule, if a parent knows or has reason to know the child will commit a crime, the parent must take reasonable precautions to see to it that the crime does not occur. In the instant case, the Jefferson Parish Sheriff's Office declared that the children's mother would not be charged. Most likely, this decision was based on the sheriff's determination that the children's mother did not know or have reason to know that her son would commit such a horrible, tragic act.

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

Video Suggestions

Video 1: "Justine Sacco, Fired After Tweet on AIDS in Africa, Issues Apology"

http://abcnews.go.com/International/justine-sacco-fired-tweet-aids-africa-issues-apology/story?id=21301833

Note: In addition to the video, please see the following article, also included at the above-referenced web site address:

"Justine Sacco, Fired After Tweet on AIDS in Africa, Issues Apology"

According to the article, the communications director fired over a tweet evoking AIDS and race that was sent as she was headed to Africa apologized recently, saying she is "ashamed" for her insensitivity to the millions of people living with the virus.

Justine Sacco, formerly a public relations executive for the Internet giant InterActive Corp., which owns popular websites like Match.com, Dictionary.com, and Vimeo, was fired over a tweet that came from her account on Friday that read: "Going to Africa. Hope I don't get AIDS. Just kidding. I'm white!"

Controversy erupted while Sacco was reportedly mid-flight with no Internet access. Recently, Sacco said, "My greatest concern was this statement reach South Africa first." After sending her statement to South African newspaper The Star, Sacco shared the following apology:

"Words cannot express how sorry I am, and how necessary it is for me to apologize to the people of South Africa, who I have offended due to a needless and careless tweet," Sacco said.

"There is an AIDS crisis taking place in this country, that we read about in America, but do not live with or face on a continuous basis. Unfortunately, it is terribly easy to be cavalier about an epidemic that one has never witnessed firsthand.

"For being insensitive to this crisis -- which does not discriminate by race, gender or sexual orientation, but which terrifies us all uniformly -- and to the millions of people living with the virus, I am ashamed.

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

"This is my father's country, and I was born here. I cherish my ties to South Africa and my frequent visits, but I am in anguish knowing that my remarks have caused pain to so many people here; my family, friends and fellow South Africans. I am very sorry for the pain I caused."

A trending hashtag #HasJustineLandedYet and parody account @LOLJustineSacco quickly appeared on Twitter after Sacco sent the tweet. A fake Facebook account under her name was also created, where a post links to www.justinesacco.com, which brings up a donation page for Aid for Africa.

InterActive Corp. issued a statement distancing itself from the tweet and saying the employee was fired.

"There is no excuse for the hateful statements that have been made and we condemn them unequivocally," the InterActive Corp statement said. "We hope, however, that time and action, and the forgiving human spirit, will not result in the wholesale condemnation of an individual who we have otherwise known to be a decent person at core."

Discussion Questions

1. As the article indicates, Justine Sacco was fired by her employer, InterActive Corp., for her comments regarding AIDS in Africa. Does Ms. Sacco have any employment law-related arguments to assert in her favor regarding her termination of employment?

Ms. Sacco does not have any substantial employment law-related arguments to assert in her favor regarding her termination of employment. InterActive Corp. has its corporate headquarters in New York City, so legal standards regarding the employer-employee relationship in New York and the United States apply to this case. In most situations, the employment-at-will doctrine applies to the employer-employee relationship and decisions regarding termination of employment. Under the employment-at-will doctrine, an employer can terminate an employee for any reason or no reason at all, assuming the employer does not terminate the employee for discriminatory reasons prohibited by state and/or federal law. Even if the employee had an employment contract for a guaranteed term, an employer can still justify early termination for cause, including unprofessional statements made by an employee that shed negative light on the employer. For obvious reasons, InterActive Corp. would like to distance itself from the unfortunate statements Justine Sacco made about AIDS and Africa. Distancing itself from such statements can include terminating the employee.

2. Should an employee have any legal protection if it could be determined that such statements were made in jest? Why or why not?

This is an opinion question, so student responses may vary. In your author's opinion, any attempt at jest did not ameliorate the inappropriateness of the statements Ms. Sacco made about AIDS and Africa. It is highly ironic that Ms. Sacco made such statements while serving as a communications director. What is most unfortunate for her is that the controversy surrounding her statements, and

her violation of the most basic duty a communications director owes to her company, will likely follow her in any attempt to pursue a similar position with another company.

3. Make InterActive Corp.'s best legal and ethical arguments as to why Justine Sacco's termination of employment was justified.

As indicated in response to Video 1 Discussion Question Number 1 above, Justine Sacco's statements shed negative light on InterActive Corp., since she was the company's employee when she made the inappropriate statements. Adding "insult to injury" in terms of negative public perception of the company is that Ms. Sacco was InterActive Corp.'s communications director. The fact that Ms. Sacco did not promote a positive public perception of the company is justification alone, both legally and ethically, for InterActive Corp. to terminate her employment.

Video 2: "Utah Same-Sex Couples Getting Marriage Licenses"

http://www.huffingtonpost.com/2013/12/20/utah-same-sex-marriage_n_4482703.html

Note: In addition to the short video, please see the following article, also included at the above-referenced web site address:

"Utah Same-Sex Couples Getting Marriage Licenses"

According to the article, a federal judge struck down Utah's same-sex marriage ban recently in a decision that marks a drastic shift toward gay marriage in a conservative state where the Mormon church has long been against it.

The decision set off an immediate frenzy as the clerk in the state's most populous county began issuing marriage licenses to dozens of gay couples while state officials took steps to appeal the ruling and halt the process.

Cheers erupted as the mayor of Salt Lake City led one of the state's first gay wedding ceremonies in an office building about three miles from the headquarters of the Mormon church.

Deputy Salt Lake County Clerk Dahnelle Burton-Lee said the district attorney authorized her office to begin issuing licenses to same-sex couples but she couldn't immediately say how many had been issued.

Just hours earlier, U.S. District Judge Robert J. Shelby issued a 53-page ruling saying the constitutional amendment Utah voters approved in 2004 violates gay and lesbian couples' rights to due process and equal protection under the 14th Amendment. Shelby said the state failed to show that allowing same-sex marriages would affect opposite-sex marriages in any way.

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

"In the absence of such evidence, the State's unsupported fears and speculations are insufficient to justify the State's refusal to dignify the family relationships of its gay and lesbian citizens," Shelby wrote.

The decision drew a swift and angry reaction from Utah leaders, including Republican Governor Gary Herbert.

"I am very disappointed an activist federal judge is attempting to override the will of the people of Utah. I am working with my legal counsel and the acting attorney general to determine the best course to defend traditional marriage within the borders of Utah," Herbert said.

The state immediately filed both a notice of appeal of the ruling and a request for an emergency stay that would stop marriage licenses from being issued to same-sex couples. It is unknown when the judge will make a decision on whether to grant the stay.

"It will probably take a little bit of time to get everything in place," said Ryan Bruckman, a spokesman for the attorney general's office. He said the judge told the attorney general's office it would be a couple of days before any request for an emergency stay would be reviewed.

The ruling has thrust Shelby into the national spotlight less than two years after Congress approved his nomination to the federal bench. He was appointed by President Barack Obama after Republican Sen. Orrin Hatch recommended him in November 2011.

In his ruling, Shelby wrote that the right to marry is a fundamental right protected by the United States Constitution.

"These rights would be meaningless if the Constitution did not also prevent the government from interfering with the intensely personal choices an individual makes when that person decides to make a solemn commitment to another human being," Shelby wrote.

Many similar challenges to same-sex marriage bans are pending in other states, but the Utah case has been closely watched because of the state's history of staunch opposition to gay marriage as the home of The Church of Jesus Christ of Latter-day Saints.

The church said in a statement that it stands by its support for "traditional marriage."

"We continue to believe that voters in Utah did the right thing by providing clear direction in the state constitution that marriage should be between a man and a woman, and we are hopeful that this view will be validated by a higher court," the church said.

Not all Mormons were disappointed. A group called Mormons for Equality applauded the ruling, saying it was particularly sweet coming in "the heartland of our faith."

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

The group has been among the leaders of growing movement among Mormons to push the church to teach that homosexuality is not a sin.

The Mormon church's stance has softened considerably since it was one of the leading forces behind California's short-lived same-sex-marriage ban, Proposition 8, in 2008. A church website launched this year encourages more compassion toward gays, and church leaders backed the Boy Scouts' recent policy allowing gay youth.

The Utah ruling comes the same week New Mexico's highest court legalized gay marriage after declaring it unconstitutional to deny marriage licenses to same-sex couples. A new law passed in Hawaii last month now allows gay couples to marry there.

If the ruling stands, Utah would become the 18th state to allow gay marriages, said Jon Davidson, director of Lambda Legal, which pursues litigation on LGBT issues nationwide.

That's up from six before the United States Supreme Court last summer struck down part of the Defense of Marriage Act that defined marriage as between a man and a woman. The District of Columbia also allows same-sex marriage.

Discussion Questions

1. On what legal basis did United States District Court Judge Robert J. Shelby overturn Utah's constitutional ban on same-sex marriage?

Judge Robert J. Shelby's decision to overturn Utah's constitutional ban on same-sex marriage is based on the Fourteenth Amendment to the United States Constitution, which states, in pertinent part, that "(n)o state shall make or enforce any law which shall...deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws." By his decision, Judge Shelby is concluding that Utah's constitutional ban on same-sex marriage is a denial of both due process and equal protection for those in the gay community who seek to enjoy the bonds of matrimony.

2. In your reasoned opinion, is this case an example of an activist judge "legislating from the bench?" Explain your response.

The term "legislating from the bench" is a politically-charged term suggesting that a member of the judiciary is exceeding the constitutional authority of his or her position (interpreting the law) by, in essence, assuming a legislative role (making the law). Those opposing Judge Shelby would likely argue that in allowing gay marriage, he is making law, while Judge Shelby would likely contend that he is merely interpreting the law—specifically, in terms of whether the Fourteenth Amendment's Due Process and Equal Protection Clauses apply to those in the gay community who would like to wed.

3. In your reasoned opinion, should the United States Supreme Court address the issue of same-sex marriage? If so, on what legal basis? If not, why not?

Regardless of student opinion on the issue of gay marriage, in your author's opinion, this is an issue that "screams out" for the United States Supreme Court to address. The federal constitutional question is clearly presented in this case—namely, whether the Fourteenth Amendment to the United States Constitution's Due Process and Equal Protection Clauses forbid Utah and other states from denying homosexual couples the right to wed. This case involves a fundamental federal constitutional question—Such cases have filled the dockets of the United States Supreme Court since it was first established by our Founding Fathers.

businesslaw

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

Mc Graw Hill Education

Of Special Interest

This section of the newsletter addresses the National Security Administration's (NSA's) data collection practices.

Ethical Dilemma

"We Need Real Protection from the NSA"

http://www.usatoday.com/story/opinion/2014/01/15/nsa-protection-snowden-spying-column/4499793/

Note: This is an "opinion editorial" written by Ed Loomis, Kirk Wiebe, Thomas Drake, William Binney and Diane Roark. Loomis, Wiebe, Drake and Binney were career professionals at the National Security Administration (NSA), while Roark served on the House Intelligence Committee. The FBI raided each of their homes in 2007, falsely accusing them of leaking part of the NSA program to The New York Times in 2005.

Wake up, America. While we've been paying attention to other things, our intelligence agencies have been tearing holes into the Bill of Rights.

President Obama is expected to issue new guidelines that purport to rein in these abuses, but leaked details leave little reason for hope that his proposals will go far enough. What America needs is a U-turn before we lose our freedom and our country.

In the years since 9/11, administrations of both parties, along with United States intelligence agencies, have secretly built up enormous powers that they do not intend to relinquish. They were aided in this endeavor by the very institution that was supposed to be a safeguard, a Foreign Intelligence Surveillance Act (FISA) court whose secret rulings essentially set aside the Constitution. Ill-considered legislation from Congress has only enabled the collapse of checks and balances.

In late 2005 and early 2006, *The New York Times*, then Mark Klein and USA TODAY received fragmentary information on a program that collected private information on Americans. Last June, publication of documents taken from the National Security Agency by Edward Snowden revealed a far more intrusive program of domestic spying.

These programs were supposed to protect us, but the president's NSA review panel found that spying on Americans has not prevented any terrorist attacks. Even if it had, the power the government has aggregated is a more dangerous threat to our freedom than is terrorism itself.

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

The executive branch has vast troves of electronic data on most Americans, even those who have never been suspected of a crime.

America's Founders knew better than to give a government powers with such enormous potential for abuse. Yet under both the Bush and Obama administrations, unconstitutional powers have been abused.

Excessive power corrupts human nature, without regard to geography or partisan affiliation, as we have seen repeatedly through history and again in the past 12 years. Despite this history, the strongest reforms proposed in Congress or by the recent presidential panel, with its 46 recommendations, are insufficient to restore our freedom.

The many areas requiring rollback illustrate just how far things have gone. Real change would start with a confession to the voters by the NSA and the intelligence committees:

- They should release the true extent of their data collection before the Snowden reporters do. Tell us how many Americans are in your files. Reveal the other categories of government agency and private business records that you have amassed.

- Identify any other agencies that copy NSA databases and/or collect their own.

- Reveal the secret "black" budget that funds this intrusion into every nook and cranny of our lives.

- Give citizens the right to see any information collected about them. Want to improve your success against terrorists?

And obey the Constitution? The obvious answers are:

- Return NSA to "targeted" collection focusing on suspects and their associates. NSA has demonstrated its inability to find a few terrorist "needles" buried in a continually expanding "haystack" of communications between innocent people both domestic and foreign.

- Establish protections that encrypt data about Americans found in these targeted investigations until a court has found probable cause to suspect them, and add systems that automatically track people using the databases so we catch abuses — and improve security.

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

- Cease allowing NSA-derived information to be used for domestic criminal investigations.

- Don't co-opt tech companies and telecommunications firms under the ruse of national security and threats. Seek their help only in exceptional, supervised instances.

- Stop weakening Internet encryption then claiming that the insecurity you helped create justifies still more "cyber-security" databases, dollars and power.

As for Congress, how about some real oversight for a change?

- Revoke the legislation that has undermined the Constitution, including the 2001 Authorization for Use of Military Force and the USA Patriot Act.

- Destroy the mass databases on Americans collected without probable cause.

- Outlaw the FBI's National Security Letters.

- Remove power over ordinary Americans from the FISA court and abolish the court's "secret law" by returning to the original 1978 version of FISA. It works.

- Never again rely completely on NSA's word. Establish a permanent independent Signals Investigatory Body of technical experts tasked with auditing NSA data collection and access to NSA databases that reports to Congress and the FISA Court.

- Legally protect whistle-blowers and journalists, the public's best sources for information on intelligence and law enforcement community conduct.

These measures would deflate the unconstitutional power of our national security state.

Discussion Questions

1. As indicated in the preface to this article, this is an “opinion editorial” written by Ed Loomis, Kirk Wiebe, Thomas Drake, William Binney and Diane Roark. Loomis, Wiebe, Drake and Binney were

career professionals at the National Security Administration (NSA), while Roark served on the House Intelligence Committee. The FBI raided each of their homes in 2007, falsely accusing them of leaking part of the NSA program to The New York Times in 2005. In your opinion, do the authors' past experiences bolster or hinder their credibility regarding reaction to NSA "data mining?" Explain your response.

To any critical thinker researching an issue and using the results of such research to formulate a reasoned opinion, evaluating credibility of source is a vital function. Admittedly, the authors of the article may have an "axe to grind" in terms of the FBI's raiding of their homes, but in your author's opinion, their argument that the National Security Administration's (NSA's) data mining practices constitute a violation of the Fourth Amendment to the United States Constitution's right to privacy should be evaluated on its own merits.

2. What is the constitutional basis for your authors' concerns about the National Security Agency's (NSA's) data mining practices?

As mentioned in response to Ethical Dilemma Discussion Question Number 1 above, the constitutional issue at hand is whether the National Security Agency's (NSA's) data mining practices constitute a violation of the Fourth Amendment to the United States Constitution's right to privacy.

The Fourth Amendment to the United States Constitutions states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The particular issue here is whether the NSA's data mining occurs without any real judicial oversight (i.e. the warrant requirement of the Fourth Amendment) and if so, whether such practices constitute a valid exception to the Fourth Amendment right to privacy.

3. In your reasoned opinion, how likely will the United States Congress exercise greater oversight of the National Security Agency and its data mining practices?

This is an opinion question, so student responses will likely vary. Your author does not believe the United States Congress will exercise greater oversight of the National Security Agency and its data mining practices, since the issue is so politically divisive, and since Congress is, at least for the foreseeable future, legislatively ineffectual due to political polarization.

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

Of Special Interest

This section of the newsletter will assist you in covering Article 1 ("Target Data Breach Spurring Lawsuits, Investigations") and Video 2 ("Utah Same-Sex Couples Getting Marriage Licenses") of the newsletter.

Teaching Tips

Teaching Tip 1 (Related to Article 1—"Target Data Breach Spurring Lawsuits, Investigations"): "Weak US Card Security Made Target a Juicy Target"

Note: Have students review the following article for further information regarding the Target debit/credit card security breach:

"Weak US Card Security Made Target a Juicy Target"

http://www.foxnews.com/tech/2013/12/23/weak-us-card-security-made-target-juicy-target/

According to the article, the United States is the juiciest target for hackers hunting credit card information. And experts say incidents like the recent data theft at Target's stores will get worse before they get better.

That is in part because U.S. credit and debit cards rely on an easy-to-copy magnetic strip on the back of the card, which stores account information using the same technology as cassette tapes.

"We are using 20th century cards against 21st century hackers," says Mallory Duncan, general counsel at the National Retail Federation. "The thieves have moved on but the cards have not."

In most countries outside the U.S., people carry cards that use digital chips to hold account information. The chip generates a unique code every time it's used. That makes the cards more difficult for criminals to replicate. So difficult that they generally do not bother.

"The United States is the top victim location for card counterfeit attacks like this," says Jason Oxman, chief executive of the Electronic Transactions Association.

The breach that exposed the credit card and debit card information of as many as 40 million Target customers who swiped their cards between November 27 and December 15 is still under investigation. It is unclear how the breach occurred and what data, exactly, criminals have.

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

Although security experts say no security system is fail-safe, there are several measures stores, banks and credit card companies can take to protect against these attacks.

Companies have not further enhanced security because it can be expensive. And while global credit and debit card fraud hit a record $11.27 billion last year, those costs accounted for just 5.2 cents of every $100 in transactions, according to the Nilson Report, which tracks global payments.

Another problem: retailers, banks and credit card companies each want someone else to foot most of the bill. Card companies want stores to pay to better protect their internal systems. Stores want card companies to issue more sophisticated cards. Banks want to preserve the profits they get from older processing systems.

Card payment systems work much the way they have for decades. The magnetic strip on the back of a credit or debit card contains the cardholder's name, account number, the card's expiration date and a security code different from the three or four-digit security code printed on the back of most cards.

When the card is swiped at a store, an electronic conversation is begun between two banks. The store's bank, which pays the store right away for the item the customer bought, needs to make sure the customer's bank approves the transaction and will pay the store's bank. On average, the conversation takes 1.4 seconds.

During that time the customer's information flows through the network and is recorded, sometimes only briefly, on computers within the system controlled by payment processing companies. Retailers can store card numbers and expiration dates, but they are prohibited from storing more sensitive data such as the security code printed on the backs of cards or other personal identification numbers.

Hackers have been known to snag account information as it passes through the network or pilfer it from databases where it's stored. Target says there is no indication that security codes on the back of customer credit cards were stolen. That would make it hard to use stolen account information to buy from most Internet retail sites. But the security code on the back of a card is not needed for in-person purchases. And because the magnetic strips on cards in the U.S. are so easy to make, thieves can simply reproduce them and issue fraudulent cards that look and feel like the real thing.

"That's where the real value to the fraudsters is," says Chris Bucolo, senior manager of security consulting at ControlScan, which helps merchants comply with card processing security standards.

Once thieves capture the card information, they check the type of account, balances and credit limits, and sell replicas on the Internet. A simple card with a low balance and limited customer information can go for $3. A no-limit "black" card can go for $1,000, according to Al Pascual, a senior analyst at Javelin Strategy and Research, a security risk and fraud consulting firm.

To be sure, thieves can nab and sell card data from networks processing cards with digital chips, too, but they wouldn't be able to create fraudulent cards.

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

Credit card companies in the U.S. have a plan to replace magnetic strips with digital chips by the fall of 2015. But retailers worry the card companies won't go far enough. They want cards to have a chip, but they also want each transaction to require a personal identification number, or PIN, instead of a signature.

"Everyone knows that the signature is a useless authentication device," Duncan says.

Duncan, who represents retailers, says stores have to pay more — and banks make more — on transactions that require signatures because there are only a few of the older networks that process them, and therefore less price competition. There are several companies that process PIN transactions for debit cards, and they tend to charge lower fees to stores.

"Compared to the tens of millions of transactions that are taking place every day, even the fraud that they have to pay for is small compared to the profit they are making from using less secure cards," Duncan says.

Even so, there are a few things retailers can do, too, to better protect customer data. The most vulnerable point in the transaction network, security experts say, is usually the merchant. "Financial institutions are more used to having high levels of protection," says Pascual. "Retailers are still getting up to speed."

The simple, square, card-swiping machines that consumers are used to seeing at most checkout counters are hard to infiltrate because they are completely separate from the Internet. But as retailers switch to faster, Internet-based payment systems they may expose customer data to hackers.

Retailers need to build robust firewalls around those systems to guard against attack, security experts say. They could also take further steps to protect customer data by using encryption, technology which scrambles the data so it looks like gibberish to anyone who accesses it unlawfully. These technologies can be expensive to install and maintain, however.

Thankfully, individual customers are not on the hook for fraudulent charges that result from security breaches. But these kinds of attacks do raise costs —and, likely, fees for all customers. "Part of the cost in the system is for fraud protection," Oxman says. "It costs money, and someone's going to pay for it eventually."

Teaching Tip 2 (Related to Video 2—"Utah Same-Sex Couples Getting Marriage Licenses"): The Fourteenth Amendment to the United States Constitution

Note: In discussing Video 2, please have students refer to the following language of the Fourteenth Amendment to the United States Constitution, also known as the "Due Process" and "Equal Protection" clauses of the Constitution:

businesslaw

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

Mc Graw Hill Education

"No state shall...deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."

businesslaw

Proceedings

A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

Mc Graw Hill Education

Chapter Key for McGraw-Hill/Irwin Business Law Texts:

	Hot Topics	Video Suggestions	Ethical Dilemma	Teaching Tips
Kubasek et al., Dynamic Business Law	Chapters 7 and 8	Chapters 5 and 42	Chapters 2 and 5	Chapters 5 and 8
Kubasek et al., Dynamic Business Law: Summarized Cases	Chapters 7 and 8	Chapters 5 and 42	Chapters 2 and 5	Chapters 5 and 8
Kubasek et al., Dynamic Business Law: The Essentials	Chapters 5 and 6	Chapters 4 and 24	Chapters 1 and 4	Chapters 4 and 6
Mallor et al., Business Law: The Ethical, Global, and E-Commerce Environment	Chapters 5 and 6	Chapters 3 and 51	Chapters 3 and 4	Chapters 3 and 6
Barnes et al., Law for Business	Chapters 5 and 6	Chapters 4 and 25	Chapters 3 and 4	Chapters 4 and 6
Brown et al., Business Law with UCC Applications	Chapters 5 and 6	Chapters 2 and 23	Chapters 1 and 2	Chapters 2 and 6
Reed et al., The Legal and Regulatory Environment of Business	Chapters 10 and 13	Chapters 6 and 21	Chapters 2 and 6	Chapters 6 and 10
McAdams et al., Law, Business & Society	Chapters 4 and 7	Chapters 5 and 12	Chapters 2 and 5	Chapters 5 and 7
Melvin, The Legal Environment of Business: A Managerial Approach	Chapters 9 and 22	Chapters 2 and 11	Chapters 2 and 5	Chapters 2 and 9
Bennett-Alexander & Harrison, The Legal, Ethical, and Regulatory Environment of Business in a Diverse Society	Chapters 6 and 8	Chapters 1 and 11	Chapter 1	Chapters 1 and 6

businesslaw

Proceedings

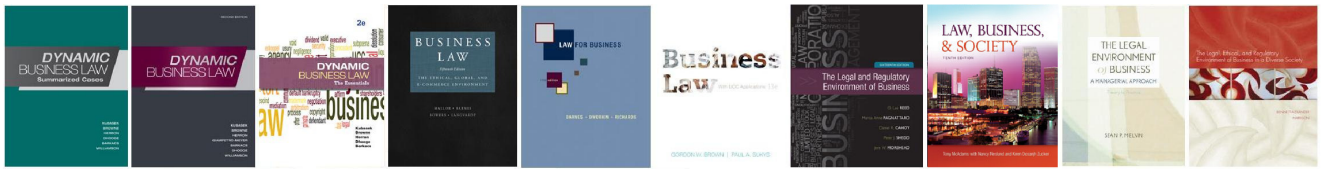
A monthly newsletter from McGraw-Hill

February 2014 Volume 5, Issue 7

Mc Graw Hill Education

This Newsletter Supports the Following Business Law Texts:

Barnes et al., Law for Business, 11th Edition 2012© (0073377716)
Bennett-Alexander et al., The Legal Environment of Business in A Diverse Society, 1st Edition 2012© (0073524921)
Brown et al., Business Law with UCC Applications Student Edition, 13th Edition 2013© (0073524956)
Kubasek et al., Dynamic Business Law, 2nd Edition 2012© (0073377678)
Kubasek et al., Dynamic Business Law: The Essentials, 2nd Edition 2013© (0073524972)
Kubasek et al., Dynamic Business Law: Summarized Cases, 1st Edition 2013© (0078023777)
Mallor et al., Business Law: The Ethical, Global, and E-Commerce Environment, 15th Edition 2013© (0073377643)
McAdams et al., Law, Business & Society, 10th Edition 2012© (0073525006)
Reed et al., The Legal and Regulatory Environment of Business, 16th Edition 2013© (0073524999)
Melvin, The Legal Environment of Business: A Managerial Approach 2011© (0073377694)



Mc Graw Hill Connect Learn Succeed™