The Cybercrime Newsletter is a publication of the National Attorneys General Training and Research Institute (NAGTRI). It is written and edited by Hedda Litwin, NAAG Cyberspace Law Chief Counsel (hlitwin@naag.org; 202-326-6022).

The views and opinions of authors expressed in this newsletter do not necessarily state or reflect those of the National Association of Attorneys General (NAAG). This newsletter does not provide any legal advice and is not a substitute for the procurement of such services from a legal professional. NAAG does not endorse or recommend any commercial products, processes, or services. Any use and/or copies of the publication in whole or part must include the customary bibliographic citation. NAAG retains copyright and all other intellectual property rights in the material presented in the publications.

In the interest of making this newsletter as useful a tool as possible for you, we ask that you keep us informed of your efforts. Additionally, we would like to feature articles written by you. Please contact us with information, proposed articles and comments about this newsletter. Thank you.

WE CAN DO MORE TO PROTECT STUDENT PRIVACY

By Rob McKenna

Effective use of high-quality data is making a difference in education by helping educators make informed decisions to improve student achievement. For example, early warning systems at Miami’s Carol City Senior High School combine attendance, performance and behavioral information to identify students who are struggling, allowing educators and parents to craft effective strategies for improvement when there is still time to get them on track to academic success and an on-time graduation.

The Family Educational Rights and Privacy Act (FERPA) of 1974 protects the privacy of student education records, allowing parents or students over 18 years of age the right to review and consent to the sharing of these records. There has been some ambiguity about how FERPA applies to statewide longitudinal data systems, and it is important for the federal government to provide greater clarity here.
States have prioritized the protection of education data in the past year, a positive step towards growing the public conversation around the critical role of data in education. We’ve seen 107 bills introduced in 35 states during this year’s legislative sessions. Some take a governance approach, seeking to amend or establish the procedures, roles, responsibilities and supports needed to ensure education data are used appropriately. Others take a prohibitive approach, seeking to reduce privacy risks by forbidding or halting the collection of certain types or uses of this data.

Beyond legislation, there are many actions state leaders such as Governors, Attorneys General, and state education agencies can take to build trust in the protection of student data. In May 2014, Education Counsel outlined key principles for strengthening state policies and law protecting data privacy, including selecting a state leader and advisory board responsible for ensuring appropriate privacy protections and implementing policies and guidance, establishing a public data inventory and statewide policies for governing personally identifiable information.

We need to ensure our laws are updated to keep up with changes in technology and ensure those same laws are fairly implemented. At the same time, we must also build public and policymaker awareness and understanding of how education data can help children, even as we build trust these data will be kept safe and secure. As state policy leaders, state Attorneys General can lead both of these efforts by

1) Ensuring the public and policymakers understand how current and new federal and state laws apply to both protect student privacy and permit appropriate access to student data, and

2) Maintaining the right balance between ensuring privacy while permitting that access.

State leaders, especially state Attorneys General and their staff, are guardians of privacy rights and often are also advocates for effective public education. It is crucial for them to appreciate the transformative power of education data, appropriately used and applied, and understand student privacy need not be compromised in the process.

1Rob McKenna served two terms as Washington’s seventeenth Attorney General. He is the chairman of the board of the Data Quality Campaign.

GOOGLE GLASS AND ITS PRIVACY IMPLICATIONS

By D’Juan Jones

A Primer on Google Glass

Google Glass, commonly known as “Glass,” is a wearable computer resembling a traditional pair of glasses. Glass is currently in the “Explorer” stage, meaning owners are using Glass in real-life situations and suggesting hardware and software improvements for the final version. The Explorer program was first launched in June 2013, and only individuals who attended Google’s Annual Technology Conference were invited to purchase Glass and join the Explorer program. In April 2014, the Explorer program was temporarily extended to the public for a 24-hour period. In response to the high volume of orders occurring within that period, Google permanently opened the Explorer program to the public in May 2014. Today, Glass can be purchased by any individual residing in the United States who has a United States mailing address and is over the age of 18 for approximately $1,500. Although Glass is available to the public, the quantity of Glass is limited, and current Explorer editions of Glass are not the final versions to be produced for widespread consumer purchase.

Unlike smartphones, Glass does not have a “cellular radio”—the technology enabling smartphones to browse the web and download applications without being connected to an outside Internet source. Glass must connect to an Internet source (such as WIFI) or to a smartphone through Bluetooth to func-
tion properly. Glass can perform many of the same tasks as a newly purchased smartphone—including the capture of photo and video, directions, text messaging, emailing, voice calling and performing Google searches. After a Glass owner has successfully connected the device to an Internet source, he or she can verbally ask Glass to perform a number of functions, including reading an email aloud, asking a question to prompt a web search and finding and navigating to the nearest coffee shop. Additionally, a Glass owner can lightly tap the navigation bar located on the frame of Glass and scroll to the desired function. Google supports very few applications on the Explorer edition of Glass. Those currently supported applications allow the owner to stream music, plan and track exercise regimes, browse social networks and access news sources. Applications under development by non-Google personnel will become available once Glass is released for widespread consumer purchase. Similar to the application stores for smartphones, the availability of additional applications will greatly expand the list of Glass capabilities.

Privacy Concerns for Glass Owners and Non-Users

There are several privacy concerns for Glass owners and for non-users. A non-user can include a person who is interacting directly with an owner of Glass or a stranger who inadvertently crosses path with a Glass owner. Privacy concerns include (a) the possibility of video and sound surveillance without consent; (b) the expansion of Glass capabilities through application development; (c) the storage of personal information on the Cloud and insecure Internet connections; and (d) the discoverability of private data.

In most circumstances, a smartphone user must physically raise their phone in order to capture photos or video, thereby alerting non-users about a photo or video being captured. However, Glass does not require such a “blatant” physical act—an owner can capture a photo, video or audio with a discreet finger tap, a whispered voice command or even an eye wink. In the current Explorer edition of Glass, there are no outward indicators alerting a non-user about an owner capturing photos or videos; non-users are exposed to a state of “always on” surveillance. Non-users are unable to discern when their private actions and conversations are being recorded, and consequently they must modify their behavior in the presence of a Glass owner. Moreover, the possibility of stealth photography allows a Glass owner to discreetly capture photos of vulnerable populations, such as children. Within a professional setting, an employee wearing Glass risks the inadvertent disclosure of trade secrets or confidential information. Additionally, Glass owners could record their conversations with other individuals without their knowledge, thereby violating the wiretapping statutes in jurisdictions requiring two-party consent.

The capabilities of Glass—and privacy concerns—will increase exponentially with the development of applications. Perhaps the most dangerous application is facial recognition software. Although Google has stated it would not support such applications, an individual can easily bypass this restriction, as is often done on Apple smartphones through a process known as “jail breaking.” Facial recognition capabilities would allow a Glass owner to capture the faces of a stranger and analyze the photo through online or application databases. This process could populate the name, occupation, social networking accounts and other private information of non-users without their knowledge or consent.

Google Glass is not equipped with built-in Internet capabilities and must connect to an outside Internet source. Additionally, much of the information gathered by Glass is stored on Google servers. These characteristics of Glass pose several privacy risks for Glass owners and non-users. Essentially, Glass is gathering data about everything the owner views. This data includes the clothing preferences, workplace, speech patterns, clothing and food preferences and travel patterns of the Glass owner and those with whom the owner interacts. This sensitive data could be accessed by hackers when Glass is
connected to an unsecure Internet source or viewed by anyone on a shared network when the data is automatically uploaded to a cloud.

Glass also presents privacy issues in the context of law enforcement and discovery. As discussed above, Glass has the ability to capture the bulk of the owner’s life and that of anyone with whom they interact. Issues concerning the discoverability of such data will need to be addressed in order to protect privacy of Glass owners and non-users while also balancing the needs of law enforcement.

Remedies and Legislation

Informal steps have been taken to address the privacy concerns presented by Glass, and many states have pending legislation to address the safety risks posed by Glass. Casinos, restaurants and movie theaters have proactively banned Glass. These establishments seek to combat the possibility of patrons having to modify their behavior in response to the presence of Glass and the possibility of Glass being used as a piracy tool. Viewed from a safety standpoint, lawmakers fear Glass is similar to smartphones and will distract motorists. Approximately eight states—Illinois, Delaware, Missouri, New York, Maryland, West Virginia, New Jersey and Wyoming—are considering legislation to ban the use of Glass while driving. Google has actively deployed lobbyists in an attempt to dissuade such legislation. Google proposes Glass will help ensure the safety of drivers through applications to keep drivers awake and alert drivers to upcoming hazards.

NITA SEEKS PUBLIC COMMENT ON BIG DATA, CONSUMER PRIVACY

The U.S. Commerce Department’s National Telecommunications and Information Administration (NTIA) issued a Request for Comments on how issues raised by big data impact the Consumer Privacy Bill of Rights, the Administration’s framework for privacy protections released in February 2012. Specifically, NTIA is seeking comment on 1) how the principles in the Consumer Privacy Bill of Rights support innovations related to big data while also responding to potential privacy risks; 2) whether the Consumer Privacy Bill of Rights should be clarified or modified to better accommodate the benefits or risks of big data; 3) whether a responsible use framework should be used to address the challenges posed by big data; and 4) mechanisms to best address the “notice and consent” model for privacy protection noted in the big data report. The comment notice was also posted in the Federal Register, Volume 79, No. 109, on June 6, 2014 and can be accessed at http://www.ntia.doc.gov/files/ntia/publications/big_data_rfc.pdf.

Comments are due on or before August 5, 2014 and may be submitted by email to privacyrfc2014@ntia.doc.gov. They may also be submitted by mail to the National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Ave., NW, Room 4725, Attn: Privacy RFC 2014, Washington, DC 20230.

ATTORNEYS GENERAL FIGHTING CYBERCRIME

ARKANSAS

Attorney General Dustin McDaniel filed a lawsuit against three online payday lending companies and their owners, accusing them of illegally providing loans with interest rates as high as 782 percent. The defendants are brothers Chris and John Kamberis of Kansas and companies King Marketing, LLC; Prestige Marketing, LLC; and SLR Ridge LLC. According to the lawsuit, the Kamberis brothers market illegal loans from entities purported to be

1D’Juan Jones is a summer intern at NAAG and a law student at Howard University School of Law.
based in the Caribbean island of Nevis in a deliberate attempt to avoid U.S. enforcement, as Nevis-based entities have no role in the loans and all business is conducted by employees in the Kansas City area. Attorney General McDaniel argues all loans issued by defendants had interest rates significantly higher than the 17 percent limit set by state law. According to the suit, defendants have taken more than $264,585 in illegal fees and loans to date. Attorney General McDaniel is seeking an injunction to prohibit the defendants from issuing payday loans to state consumers, a court order cancelling all outstanding loans and obligations and a court order requiring defendants to pay restitution, civil penalties, attorneys’ fees and costs.

**CALIFORNIA**

Attorney General Kamala Harris issued a guide on privacy policies and do not track disclosures for state businesses addressing recent changes in the state privacy law. The guide, “Making Your Privacy Practices Public,” was developed from consultations between Attorney General Harris’ Privacy and Enforcement Unit and stakeholders from the business sector, academia and privacy advocates.

**DELAWARE**

Attorney General Beau Biden announced the arrest of Eric Aldrich, a registered sex offender, on 25 counts of Dealing in Child Pornography. An investigation into the distribution of child pornography by the State Child Predator Task Force led them to execute a search warrant at Aldrich’s residence, where detectives seized three computers and other digital media. A forensic preview of the evidence revealed multiple videos of child pornography. Aldrich is prohibited from having Internet access as a condition of his supervised probation.

**FLORIDA**

Attorney General Pam Bondi’s Office obtained $426,000 in restitution pursuant to a settlement with Arrow Outlet, LLC, a penny auction website, resolving allegations Arrow used programming code to deceive consumers. ArrowOutlet.com allowed users to purchase and place bids on consumer goods, but according to the complaint, Arrow used an “auto-bid script” to artificially inflate the number of bids required to win a given auction. The suit alleges the script was designed to place bids at intervals, thereby prolonging the auction, increasing the number of bids purchased and preventing actual users from winning the auction. The settlement agreement prohibits Arrow from creating, administering, operating or in any way using a penny auction website to generate income.

**HAWAII**

Attorney General David Louie’s Criminal Justice Division indicted Jonathan Silva on one count of Electronic Enticement of a Child in the First Degree, a class B felony. Silva is accused of soliciting an underage girl through her Facebook account for sexual purposes, and was arrested when he arrived to meet her. The indictment resulted from an investigation by the Internet Crimes Against Children Task Force of Attorney General Louie’s Investigations Division, assisted by U.S. Immigration and Customs Enforcement. If convicted, Silva faces 10 years imprisonment and required registration as a sex offender.

**ILLINOIS**

Attorney General Lisa Madigan’s investigators, with assistance from the Lindenhurst Police Department, arrested Mark Galer on a charge of reproduction of child pornography, a Class X felony punishable by six to 30 years in prison, and four counts of possession of child pornography, a Class 2 felony punishable to three to seven years in prison. Galer was arrested after investigators and police executed a search warrant at his home. The arrest was part of Attorney General Madigan’s “Operation Glass House,” an initiative against the downloading and trading of child pornography.

**KENTUCKY**

Attorney General Jack Conway joined Kerry Harvey, U.S. Attorney for the Eastern District of Kentucky,
and Gary Hartwig, Special Agent in Charge, U.S. Immigration and Customs Enforcement’s Homeland Security Investigations (HSI), in announcing Erik Hentzen’s conviction for receiving and possessing child pornography images. The investigation was conducted by Attorney General Conway’s Cybercrimes Unit and HIS and began when authorities discovered numerous child pornography videos had been made available for download over the Internet. Investigators traced the source of the videos to the computer in Hentzen’s apartment. Unit investigators executed a search warrant and seized multiple computers belonging to Hentzen containing more than 4,000 videos of child pornography. The U.S. Attorney’s Office prosecuted the case.

LOUISIANA

Attorney General Buddy Caldwell announced the arrest of 19 individuals as a result of Operation Broken Heart, a coordinated law enforcement effort to apprehend child sexual exploitation offenders. The undercover initiative was led by Attorney General Caldwell’s Office and included local, state and federal Internet Crimes Against Children task force affiliates.

MASSACHUSETTS

Attorney General Martha Coakley announced Robert Kelley and Brian Symmes, owners of an Internet café, and their corporation pleaded guilty to charges related to operating an illegal slot parlor. The men operated B&B Cyber Café through their corporation, Lucky Day Cyber Café, LLC, and each defendant pleaded guilty to one count each of unlawful operation of a game or gaming device, organizing or promoting a lottery, operating an illegal lottery, allowing lotteries in a building and the sale of lottery tickets. Kelley and Symmes were each sentenced to serve two years of probation, and they were ordered to forfeit $23,000 in cash seized during the investigation, as well as forfeit an additional $100,000 to the Commonwealth. The case was prosecuted by Assistant Attorneys General Thomas Ralph and Timothy Wyse of the Cyber Crime Division and Assistant Attorney General Pat Hanley, Chief of the Gaming Enforcement Division. The investigation was conducted by State Police assigned to Attorney General Coakley’s Office, Senior Investigator Mark Pulli, Financial Investigator Anthony Taylor, the Attorney General’s Computer Forensic Laboratory and State Department of Revenue investigator Thomas Nowicki.

MISSISSIPPI

Attorney General Jim Hood announced the sentencing of Michael Ishee to 20 years in prison after pleading guilty to one count of possession of child pornography. Attorney General Hood’s Cyber Crime Division/Internet Crimes Against Children Task Force, with assistance from the Harrison County Sheriff’s Office, uncovered multiple images and videos of child pornography in Ishee’s possession. The case was investigated by Richard Johnson and prosecuted by Special Assistant Attorney General Brandon Ogburn of the Division.

NEW JERSEY

Acting Attorney General John Hoffman’s Division of Criminal Justice Financial & Computer Crimes Bureau obtained state grand jury indictments against Frank Fiorelli, James Engle and Robert Rowe II for allegedly distributing child pornography over the Internet through online file sharing. The indictments were presented to the grant jury by Deputy Attorney General Anand Shah of the Bureau. The three men were arrested in two separate child pornography sweeps, Operation Ever Vigilant and Operation Watchdog, conducted by the Division, the State Police, the State Internet Crimes Against Children Task Force and federal partners. The Digital Technology Investigation Unit of the State Police coordinated both operations, in concert with the Division and the ICAC Task Force. The U.S. Postal Service and the Morris County Prosecutor’s Office assisted with Operation Ever Vigilant, and ICE Homeland Security Investigations and the FBI assisted with Operation
Watchdog.

NEW YORK

Attorney General Eric Schneiderman joined San Francisco District Attorney George Gascon in announcing Google and Microsoft will incorporate a kill switch into the next version of their respective mobile phone operating systems. The announcement was part of a new report issued by the Secure Our Smartphone (“S.O.S.”) Initiative, an international partnership of law enforcement agencies, elected officials and consumer advocates.

NORTH CAROLINA

Attorney General Roy Cooper announced his request for a temporary restraining order barring Raleigh Geeks and its principals, Steven Leo, Garret Foster and Timothy Staie, from doing business in the State has been granted. Attorney General Cooper filed a lawsuit naming them as defendants after his Consumer Protection Division received 24 consumer complaints of misrepresentations about repairs or failure to return repaired computers. According to the complaint, Raleigh Geeks, a/k/a Caveman Computers, ProTech Computers and Fuquay Computer Center, with several locations in the State, regularly accepted payment for computer repairs upfront, but did not complete the work in the agreed timeframe. When consumers complained, they received repeated promises the work would be completed soon or no responses at all. The complaint also alleges Raleigh Geeks sometimes returned computers in worse repair or not at all, or in other cases would substitute a completely different machine and claim it as the original. Attorney General Cooper is also seeking a permanent ban against the owners’ and managers’ deceptive practices, refunds for consumers, civil penalties and the return of consumers’ computers.

OHIO

Attorney General Mike DeWine filed a lawsuit against Giviton, LLC, the now-defunct operator of a website selling deal vouchers, for failure to deliver the deals purchased. Giviton.com sold vouchers for deals such as paying $10 for $20 worth of services at a local business. The website shut down in July 2013, and consumers who had paid in full complained they could no longer access their vouchers or found their vouchers were not honored because of alleged disputes between the local businesses and Giviton. At least 32 consumers filed complaints with Attorney General DeWine’s Office or the Better Business Bureau disputing more than $4,000 in losses. The lawsuit charges Giviton with violating the Consumer Sales Practices Act and seeks restitution for consumers, an injunction to stop further violations and civil penalties.

PENNSYLVANIA

Attorney General Kathleen Kane’s Child Predator Section agents arrested Frank Clement on charges of four counts each of distribution and of possession of child pornography and one count of criminal use of a communication facility. According to the criminal complaint, Clement used a peer-to-peer network to make child pornography files available to download. Section agents, conducting an undercover operation, downloaded those files and identified Clement as the source through his computer’s IP address. The agents joined the Erie Police Department to execute a search warrant at Clement’s residence and, using a test string of common child pornographic terms, found more than 500 child pornography files in deleted space on Clement’s computer.

RHODE ISLAND

Attorney General Peter Kilmartin partnered with Cox Communications on “TakeCharge! of Online Bullying,” a new public service campaign against cyberbullying. Attorney General Kilmartin kicked off the campaign by speaking to middle school students, where he was joined by Cox Communications Senior Vice President and General Manager John Wolfe and Sarah Murray, a recent high school graduate who shared her story of being bullied. Attorney General Kilmartin also filmed a public service announcement
reminding parents of the importance of talking to children about online activity and directing them to the TakeCharge! website for helpful tips.

SOUTH CAROLINA

Attorney General Alan Wilson’s Office arrested Xavier Fulwood on 20 counts of Sexual Exploitation of a Minor second degree, a felony offense punishable by up to 10 years imprisonment on each count. The Internet Crimes Against Children (ICAC) Task Force received referrals from the Berkeley County Sheriff’s Office and the Columbia Police Department, both Task Force members, about child pornography images being disseminated from an account traced to Fulwood’s residence. Clarendon County Sheriff’s Office officers and ICAC special investigators executed a search warrant and seized computer and media equipment for further investigation, and Fulwood later admitted to downloading child pornography. The case will be prosecuted by Attorney General Wilson’s Office.

TEXAS

Attorney General Greg Abbott’s Internet Crimes Against Children Task Force and other task force affiliates arrested five suspects for possession of child pornography as part of Operation Broken Heart, an undercover initiative targeting online child predators. The suspects arrested were Christopher Lara, who allegedly had saved child pornography on his mobile phone; Matthew Weidner, who allegedly shared child pornography videos; and Avery Rodriguez, Perre Jones and Michael Martinez, all of whom allegedly shared child pornography on social networking sites.

VERMONT

Attorney General William Sorrell announced Joel Martin has been charged with four felony counts of Promoting Child Pornography, each count carrying a potential prison term of up to 10 years. According to court documents, Martin obtained and distributed child pornography over the Internet using peer-to-peer file sharing programs. The charges resulted from a shared investigation between Attorney General Sorrell’s Office, the State Internet Crimes Against Children Task Force, the Barre City, UVM and South Burlington Police Departments and the State Police.

VIRGINIA

Attorney General Mark Herring announced Greg Clabaugh and his son, Mark Clabaugh, were sentenced after each defendant pled guilty to two counts of reproduction of child pornography. Greg Clabaugh received a sentence of three years in prison and three years of probation, with an additional seven years in prison suspended. Mark Clabaugh was sentenced to two years in prison and three years of probation, with an additional eight years in prison suspended. Both defendants must register as sex offenders upon release. The investigation began after Christiansburg police discovered child pornography images being shared over a peer-to-peer network by Greg Clabaugh. They executed a search warrant, finding a laptop containing child pornography and file sharing software. Agents also discovered Mark Clabaugh had downloaded and burned CDs of child pornography for his father, and a subsequent forensic exam of the computer revealed more than 600 child pornography images and videos. The State Police assisted in the investigation. Attorney General Herring’s Office secured the convictions.

WASHINGTON

Attorney General Bob Ferguson’s Office resolved a lawsuit against Western by Design, LLC, operating as 1880 Western Wear, a recently closed online retailer of western apparel, for violating the Consumer Protection Act. There are 117 known complaints against the company through Attorney General Ferguson’s Office, the Better Business Bureau and Ripoff Reports for failure to deliver merchandise in a timely fashion as promised. In many cases, consumers waited over one year to receive ordered merchandise. The company also had a policy of no
refunds five days after an order was placed. In the Consent Decree, Western by Design agreed to provide refunds to consumers for items paid for but not received and pay $25,000 in civil penalties if all Consent Decree provisions are not met. If the company reopens or starts a new business, it agreed it will ship purchased goods within a specified number of days, respond to customer complaints within 72 hours and restrain from any misrepresentations of their business operations. Assistant Attorney General Brooks Clemmons was the lead on the case.

_________________________________________

**CYBER NEWS BRIEFS**

**OPEN FOR PUBLIC COMMENT: TWO-SPEED INTERNET**

The Federal Communication Commission (FCC) voted 3-2 to open public comment on proposed new rules, including allowing Internet content providers to provide faster transmission to a company willing to pay for such service. According to the FCC, paid prioritization will only be allowed where it does not adversely affect competition or harm consumers. Opponents argue the plan is tantamount to discrimination against other content. The proposal also requests public comments on whether and by how much the FCC should tighten regulation of Internet service providers, such as reclassifying high-speed Internet service as a utility-like application, subject to stricter regulatory controls than now apply. The FCC also asks if it should ban certain practices with potential to impede consumers from receiving equal access to all legal online content through their chosen Internet service provider. Public comment on the proposal should be sent to openinternet@fcc.gov.

**COST OF DATA BREACH RISES: $201 PER BREACHED RECORD**

The average two-year cost of a data breach at a U.S. company in 2013 rose to $5.85 million, an eight percent increase from $5.4 million in 2012, according to an analysis by the Ponemon Institute, a privacy and data security think tank. Their analysis, “2014 Cost of Data Breach Study: Global Analysis,” found businesses spent an average of $201 for each breached record, although the cost per compromised record is significantly higher at U.S. companies than like countries in the United Kingdom, Germany and the seven other countries included in the 314 companies Ponemon reviewed. The study notes incident response planning, hiring a chief information security officer and a strong security posture are steps companies can take to reduce data breach expenses. The study may be accessed at http://pdfserver.amlaw.com/cc/ponemoninstitutedatabreachstudy/2014.pdf.

**WHITE HOUSE ISSUES BIG REPORT ON BIG DATA**

The White House released a report on big data outlining policy recommendations for the use of personal data in the commercial, education and health care sectors. The 79-page report discusses ways in which both public and private entities can make use of big data and minimize its risks. It also addresses key questions for the development of a policy framework, such as how big data alters the consumer environment and how to protect people from discrimination enabled by the new technology. The report acknowledges the opportunities big data provides for innovative approaches to education, but warns schools must ensure against misuse of information collected. There is criticism of data brokers in the report, finding their information, although unregulated, is used in the same way as data in regulated industries. Lastly, but not least, the report calls for a uniform national data breach notification law. The study team was composed of John Podesta, White House counsel; John Holdren, director of the White House Office of Science and Technology Policy; Jeffrey Zients, director of the National Economic Coun-
FCC CALLS FOR DATA BROKER LEGISLATION

The Federal Trade Commission (FTC) issued a report on data brokers, urging Congress to pass legislation affording improved consumer protections for personal information gathered and shared by the data services industry. The report, “Data Brokers: A Call for Transparency and Accountability,” studied nine companies: Acxiom Corp., Corelogic Inc., Datalogix Inc., eBureau LLC, ID Analytics Inc., Inome Inc. d/b/a Intelius Inc., PeekYou LLC, Rapleaf Inc. and Recorded Future Inc. The FTC found data brokers obtain, store and share consumer information from almost every U.S. citizen and classify consumers by race, socioeconomic status and other characteristics potentially leading to discrimination. The FTC seeks legislation establishing the creation of an online portal identifying data brokers, explaining their practices and giving consumers the ability to suppress the use of their information. The FTC also wants the legislation to require retailers and other businesses interacting with consumers to reveal when they share customer information and explain how customers can opt out. The report can be accessed at https://lexmachina.com/2014/05/patent-litigation-review/.

FREE ABA LEGAL TECHNOLOGY BUYERS GUIDE AVAILABLE

The American Bar Association (ABA) Legal Technology Resource Center launched its Legal Technology Buyer’s Guide, an online directory of products and services organized by technology type, such as practice management and cloud computing. It includes a search feature for more specific product or service results. Each listing contains a brief overview of the company, key contact information, direct social media profiles, videos, white papers, guides and checklists. The Guide is free and new products and services will be added on a regular basis. It can be accessed at http://buyersguide.americanbar.org/.

LAW LIBRARIES TO INCREASE ONLINE RESOURCES

Law libraries spent a mean of $320,931 for online databases in 2013 and expect to increase online resources by an average of three percent in 2014, according to a survey by Primacy Research Group based in New York City. The company surveyed 60 Canadian and U.S. law libraries of various sizes and types, including libraries in law firms, university law
The survey found library budgets were divided evenly between print and electronic resources, with courthouse libraries spending two-thirds of their budget on print materials and law firms spending almost 60 percent on electronic materials. The survey also looked at social media, finding almost one-third of the libraries had a Facebook presence. University libraries were found to be the most active Facebook users, with two-thirds of those surveyed having a Facebook presence. University libraries were also the most active on Twitter, with almost one-half of those surveyed tweeting, compared with one-quarter of all libraries. Other topics in the survey include online directories, ebooks and other information resources, and the report classifies the data both by library type and institution size. The report may be accessed at http://www.primaryresearch.com/view_product.php?report_id=466

IN THE COURTS

CDA § 230: INTENTIONAL TORT CLAIMS

GoDaddy.com, LLC v. Toups, 2014 Tex. App. LEXIS 3891 (April 10, 2014). The Texas Court of Appeals, Ninth District, ruled appellees could not circumvent the Communications Decency Act, 47 U.S.C.S. § 230, by couching their claims as state law intentional torts. Hollie Toups filed an action against GoDaddy, an interactive computer service provider, on behalf of a class of women alleging two revenge porn websites hosted by GoDaddy had published sexually explicit photographs of the women without their consent. While admitting GoDaddy did not create the material at issue, Toups argued GoDaddy knew of the content, failed to remove it and profited from the websites, thereby making GoDaddy jointly responsible for damages. Toups asserted intentional infliction of emotional distress and gross negligence as causes of action. GoDaddy filed a motion to dismiss, asserting immunity under § 230 as a provider of interactive services and not a publisher of content. Toups responded the revenge porn websites were not protected by the First Amendment due to their content, and therefore were not entitled to CDA immunity. The trial court denied GoDaddy’s motion, and GoDaddy then filed a petition for interlocutory appeal, which the appeals court granted. The appeals court reversed, finding the trial court erred in denying the motion to dismiss, as GoDaddy acted only as an interactive computer service provider and not an information content provider. The court found Toups could not circumvent § 230, as the CDA did not provide for an intentional violation of criminal law to be an exception to the immunity given to ISPs. The judgment was reversed and remanded.

P2P FILES: EXPECTATION OF PRIVACY

U.S. v. Hill, 2014 U.S. App. LEXIS 8557 (8th Cir. May 7, 2014). The Eighth Circuit Court of Appeals ruled defendant had no reasonable expectation of privacy in the publicly shared files. A cyber crimes task force police officer used LimeWire, the P2P file-sharing program, to access Jason Hill’s computer, downloading 10 images of what appeared to be child pornography from Hill’s shared folder. A search warrant was served on Hill’s residence, and Hill eventually admitted he had viewed child pornography images, but did not save them. The officers seized Hill’s computers, and a forensic examiner found child pornography had been downloaded and stored on Hill’s hard drive. Hill was charged with knowingly possessing, receiving and distributing child pornography. Before trial, he moved to suppress the evidence from his computer, alleging the initial access of his computer was an unreasonable search, and anything derived from it was tainted; the U.S. District Court for the Western District of Missouri denied the motion. Hill was convicted and sentenced to concurrent terms of 144 months and 120 months. He appealed, arguing the district court erred in denying his motion to suppress because the police officer
violated his Fourth Amendment rights by accessing his computer and downloading files. The appeals court disagreed, finding Hill had downloaded and actively used file-sharing software, making the pornography files in his shared folder accessible to any LimeWire user, and thus Hill had no reasonable expectation of privacy in the publicly shared files and could not invoke Fourth Amendment protection.

PARTICULARITY: SEARCH WARRANT

State v. Letoile, 2013 N.H. LEXIS 50 (May 16, 2014). The New Hampshire Supreme Court found the information given by the ex-wife provided a sufficient basis to establish probable cause. Robert Letoile, Jr.’s ex-wife, while using his computer, clicked on the browsing history and found links to websites potentially containing child pornography. She told this to police, describing the images in language taken from the websites as depicting “nude young undeveloped girls.” Based on this information, police obtained a search warrant and seized Letoile’s computer, finding images and movies containing child pornography. Letoile was charged with 29 counts each of possession and attempted possession of child pornography. Letoile moved to suppress all evidence and statements obtained as a result of the search, arguing the affidavit and search warrant failed to establish probable cause because it did not provide a sufficient description of the alleged child pornography. The trial court denied the motion, concluding the ex-wife’s descriptions would lead a reasonable person to believe there was a substantial likelihood child pornography would be found on the computer. Letoile was convicted of 26 counts of possession of child pornography. Letoile appealed, arguing the trial court erred in denying his motion to suppress because the affidavit failed to set forth sufficient facts linking child pornography to his computer. The State high court disagreed, finding probable cause for the issuance of the search warrant. The court noted that, although the ex-wife described images found on websites rather than on Letoile’s hard drive, the trial court made the common sense inference of a fair probability the images from the websites listed in Letoile’s browser history would be found on his computer and hard drive. The decision was affirmed.

PRISONER POSSESSION OF CELL PHONE: DANGEROUS CONTRABAND

People v. Green, 2014 NY Slip Op 3303 (May 8, 2014). The New York Supreme Court, Appellate Division, found the cell phone seized from defendant constituted dangerous contraband. Correction officers discovered a cell phone hidden on prisoner Barry Green’s body, and Green subsequently admitted he purchased the phone to speak with his wife. Green was then indicted and charged with one count of promoting prison contraband in the first degree. He was convicted and sentenced to a prison term of three to six years, to be served consecutively to the sentence he was currently serving. Green appealed, arguing the People failed to establish the cell phone constituted dangerous contraband. The appellate court noted Penal Law § 205.00 (4) defined dangerous contraband as “contraband which is capable of such use as may endanger the safety or security of a detention facility or any person therein.” The court also relied on People v. Finley, 10 NY 3d at 647, 657 (2008), in which the state Court of Appeals identified the test for determining whether an item is dangerous contraband is whether its particular characteristics result in a substantial probability the item will be used in a manner likely to cause death or other serious injury, facilitate an escape or bring about other major threats to a detention facility’s institutional safety or security. The court further noted the testimony at trial indicating an inmate in possession of a cell phone has potential to develop an
escape plan, orchestrate an injury to another or carry out criminal activity and thus presents a significant risk to the facility. The court found the People had met their burden of establishing the cell phone seized from Green constituted dangerous contraband under the Finley test, and the jury could reasonably have found Green’s use of a cell phone would likely have created a dangerous situation inside the facility. The judgment was affirmed.

FOURTH AMENDMENT: RETENTION OF LAPTOP

*U.S. v. Sullivan*, 2014 U.S. App. LEXIS 9800 (9th Cir. May 28, 2014). The Ninth Circuit Court of Appeals found the government’s retention of the laptop was not unreasonable. Edward Sullivan, a parolee, was arrested based on a mother’s report he had kidnapped and pimped her minor daughter. During a parole search of Sullivan’s car, agents seized a laptop computer, digital camera, a book about pimping and a cell phone. Sullivan was charged with eight parole violations, including keeping pornographic images on his phone. Officers also obtained a warrant to search Sullivan’s laptop, finding a video of child pornography featuring the daughter. Sullivan was charged with one count of production and one count of possession of child pornography. He moved to suppress the evidence obtained from his laptop, arguing the 21-day delay between the date the officers seized the laptop and the date they obtained a warrant was unreasonable and violated his Fourth Amendment rights. The U.S. District Court for the Northern District of California denied the motion. Sullivan was found guilty on both counts and was sentenced to the mandatory minimums of 25 years in prison for the production count and 10 years for the possession count, to be served concurrently, followed by a lifetime of supervised release. He appealed, raising the same argument, and the government cross-appealed the district court’s denial of an obstruction of justice enhancement in sentencing. The appeals court found the government’s seizure and retention of the laptop for 21 days before obtaining a search warrant was, under the totality of the circumstances, not unreasonable under the Fourth Amendment. The court affirmed the judgment but reversed the district court’s exclusion of an obstruction of justice application from the sentencing calculation and remanded for sentencing.

FOURTH AMENDMENT: RETENTION OF PERSONAL FILES

*U.S. v. Ganias*, 2014 U.S. App. LEXIS 11222 (2nd Cir. June 17, 2014). The Second Circuit Court of Appeals ruled the defendant’s Fourth Amendment rights were violated by the unauthorized retention of his personal files. Stavros Ganias provided tax and accounting services to small businesses. Two of his clients, American Boiler and Industrial Property Management (IPM), came under investigation by the Army (and later the IRS) for theft and improper billing practices, and government agents obtained a warrant to search Ganias’s accounting offices and seize all data relating to the operations of those two companies. Pursuant to that warrant, agents made forensic mirror images of the hard drives of all three of Ganias’s computers, including files beyond the scope of the warrant such as Ganias’s personal financial records, but assured Ganias the non-responsive files would be purged after the search for American Boiler and IPM files was complete. Thirteen months after the seizure, Army and IRS agents isolated and extracted all relevant files, but did not purge the non-responsive files, viewing that data as the government’s, not Ganias’s, property. Agents also began suspecting Ganias was underreporting his own income, and they obtained another warrant to search Ganias’s personal financial records which they had seized and retained 30 months ago. Ganias was indicted for tax evasion, and moved to suppress his personal computer records. The U.S. District Court for the District of Connecticut denied the
motion, and Ganias was convicted and sentenced to 24 months imprisonment. He appealed, contending his Fourth Amendment rights were violated when the government seized his personal computer records and retained them for 30 months. The appeals court ruled the Fourth Amendment did not permit agents executing a search warrant for the seizure of particular data to seize and indefinitely retain every file on that computer for use in future investigations. The court found the appeals court erred in denying Ganias’s motion to suppress, as Ganias’s Fourth Amendment rights had been violated by the unauthorized retention of his personal files. The judgment was vacated and the case remanded for further proceedings.

WIRETAP ACT: LISTENING THROUGH CELL PHONE SPEAKER

*Commonwealth v. Spence, 2014 Pa. LEXIS 1067* (April 28, 2014). The Pennsylvania Supreme Court ruled a state trooper did not violate the state Wiretapping and Electronic Surveillance Act, 18 Pa. C.S. § 5702, when he listened through an informant’s cell phone speaker. A high school student involved in a traffic stop was subsequently arrested for illegal possession of prescription drugs. Pursuant to a request by a state trooper, the arrestee agreed to become a confidential informant and engage in a controlled buy to inculpate his drug supplier, a dealer named “Wes.” The arrestee contacted Wes by cell phone, and at the trooper’s direction, activated the speaker function on his cell phone and engaged in two calls with Wes to arrange a drug transaction at a convenience store. Troopers arrested Wesley Spence at the convenience store and recovered prescription drugs on his person. The Commonwealth charged Spence with three counts each of possession of a controlled substance, possession with intent to deliver a controlled substance and possession of drug paraphernalia. Spence moved to suppress all of the evidence, alleging the trooper’s listening in on the conversation constituted an unlawful interception of the conversation in violation of the Act. The Commonwealth argued a cell phone does not constitute a “device” within the meaning of the Act, which specifically excludes a telephone furnished by a service provider from the definition. The trial court granted the motion, and the Superior Court affirmed. The Commonwealth again appealed, and the state Supreme Court granted review and reversed, agreeing with the Commonwealth as to telephones being exempt under the Act from the definition of “device,” irrespective of the use to which the telephone was put. The court thus found the trooper did not violate the Act when he listed to the conversation through the cell phone speaker.

FOURTH AMENDMENT: CELL SITE INFORMATION

*U.S. v. Davis, 2014 U.S. App. LEXIS 10854* (11th Cir. June 11, 2014). The Eleventh Circuit Court of Appeals affirmed the district court’s denial of defendant’s motion to exclude location evidence based on stored cell site information. Quartarius Davis was charged with two counts of conspiracy to engage in robbery and seven counts each of robbery and possession of a firearm in furtherance of a crime of violence. During pretrial proceedings, he moved to suppress electronic location evidence the government had obtained without a warrant as a violation of his Fourth Amendment rights. The U.S. District Court for the Southern District of Florida denied the motion; Davis renewed the motion during trial, and it was again denied. Davis was convicted on all 16 counts, and the court imposed a prison term of 1841 months, or approximately 162 years. Davis raised the denial of his motion to suppress on appeal, among other issues. The government argued they had relied on a §2703(d) order to support the obtaining of evidence. The appeals court found although the government’s warrantless gathering of Davis’s cell site location information violated his
reasonable expectation of privacy under the Fourth Amendment, the district court did not commit reversible error in denying his motion to suppress the fruits of that search under the good faith exception to the exclusionary rule. The court also vacated the sentencing enhancement regarding brandishing a firearm imposed by the district court.

FIFTH AMENDMENT: COMPPELLING PASSWORD

Commonwealth v. Gelfgatt, 2014 Mass. LEXIS 416 (June 25, 2014). The Massachusetts Supreme Court ruled defendant could be compelled to provide his key to seized encrypted evidence. A grand jury returned indictments charging attorney Leon Gelfgatt with 17 counts of forgery, 17 counts of uttering a forged instrument and three counts of attempting to commit larceny by false pretenses of the property of another. The charges arose from allegations Gelfgatt, through his use of computers, conducted a sophisticated scheme of diverting funds intended to be used to pay off large mortgage loans on residential properties to himself. The Commonwealth filed a motion to compel Gelfgatt to enter his password into encrypted software he placed on digital media storage devices seized by the Commonwealth. The trial court denied the motion as a potential violation of Gelfgatt’s Fifth Amendment rights, and the Commonwealth appealed. They also filed a motion to report the following related question of law: “Can the defendant be compelled pursuant to the Commonwealth’s proposed protocol to provide his key to seized encrypted digital evidence despite the rights and protections provided by the Fifth Amendment to the United States Constitution and Article Twelve of the Massachusetts Declaration of Rights?” The State high court concluded any factual statements conveyed by Gelfgatt’s act of entering an encryption key in the computers are “factual conclusions,” since the evidence clearly showed Gelfgatt’s involvement in the mortgages, so Gelfgatt would only be telling the Commonwealth what it already knows. Therefore, the court concluded the Commonwealth’s motion to compel decryption did not violate Gelfgatt’s Fifth Amendment rights nor his rights under Article 12 of the State Declaration of Rights. The court reversed the lower court’s denial of the motion and remanded for further proceedings.

Ed. note: Assistant Attorney Generals Randall Ravitz and Thomas Ralph represented the Commonwealth. The following submitted briefs for amici curiae: the Florida Department of Law Enforcement, the National White Collar Crime Center, the American Civil Liberties Union Foundation of Massachusetts, the Massachusetts Association of Criminal Defense Lawyers, Daniel Gelb and David Opderbeck.

________________________

LEGISLATIVE ROUNDUP

LOCATION TRACKING

TENNESSEE. On May 22, Governor Bill Haslam signed SB 2087 into law, a bill prohibiting government entities from obtaining the location information of an electronic device without a search warrant except under exigent circumstances. A violation of the law is a Class C misdemeanor. It has been chaptered as Pub. Ch. 991.

SMARTPHONE REMOTE DISABLING

MINNESOTA. On May 14, Governor Mark Dayton signed SF 1740 into law, a bill requiring any new smartphone sold or purchased in the State on or after July 1, 2015 to be equipped with preloaded antitheft functionality (i.e., “kill switch”) or be capable of downloading such functionality at no cost. The bill also allows law enforcement to confiscate any smartphone identified as stolen or as evidence in a criminal case, and allows a wireless device dealer to seek restitution for any resultant out-of-pocket expenses and lost profits in any criminal case arising from the investigation. Further, the bill requires
every wireless communications device dealer to install and maintain video surveillance or similar devices to photograph a frontal view of each seller of a wireless device and retain all images for a minimum of 30 days. A violation of that requirement results in a misdemeanor. The bill has been chaptered as Ch. 241.

**DISSEMINATION OF INDECENT MATERIAL TO MINORS**

RHODE ISLAND. On June 18, the House of Representatives passed HR 7766, a bill making it a felony to electronically disseminate sexually explicit images to minors. If enacted, a violation of the legislation would be punishable by up to five years in prison and/or a fine of up to $5,000. The bill was filed on behalf of Attorney General Peter Kilmartin. It has been place on the Senate calendar.

**DATA BREACH NOTIFICATION**

FLORIDA. On June 20, Governor Rick Scott signed SB 1524 into law, requiring notice be given within 30 days to affected customers and the Department of Legal Affairs if a breach of security of personal information occurs. Violations would be subject to civil penalties. The legislation also requires customer records to be disposed of in a manner protecting personal information. The bill has been chaptered as Ch. 2014-189 and is effective on July 1, 2014.

**SUPREME COURT WATCH**


In *Riley*, petitioner David Riley was stopped for a traffic violation, eventually leading to his arrest on weapons charges. An officer searching Riley incident to the arrest seized a cell phone from Riley's pocket, accessed information on the phone and noticed the repeated use of a term associated with a street gang. At the police station two hours later, a detective specializing in gangs further examined the phone's digital contents, and based in part on photographs and videos the detective found, the State charged Riley in connection with a shooting a few weeks ago and sought an enhanced sentence based on Riley's gang membership. Riley moved to suppress all evidence the police had obtained from his cell phone. The trial court denied the motion, and Riley was convicted. The California Court of Appeal affirmed.

In *Wurie*, respondent Brima Wurie was arrested after police observed him participating in an apparent drug sale. At the police station, the officers seized a cell phone from Wurie's person, noticing the phone received multiple calls from a source identified as "my house" on its external screen. The officers opened the phone, accessed its call log, determined the number associated with the "my house" label and traced that number to what they suspected was Wurie's apartment. They secured a search warrant and found drugs, a firearm and ammunition and cash in the ensuing search. Wurie was then charged with drug and firearm offenses. He moved to suppress the evidence obtained from the search of the apartment. The District Court denied the motion, and Wurie was convicted. The First Circuit Court of Appeals reversed the denial of the motion to suppress and vacated the relevant convictions.

The Court unanimously held that the police may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested. The Court held that the search-incident-to-arrest exception to the warrant requirement does not apply “with respect to digital content on cell phones” because the governmental interests that support the doctrine — harm to officers and destruction of evidence — are rarely implicated “when the
search is of digital data,” while the privacy interests at stake are high given the immense amount of personal information contained on cell phones. The Court rejected various “fallback arguments” proposed by California and the United States as “flawed” and instead noted that the exigent circumstances exception could justify the warrantless search of a particular cell phone.

Previously, the Court granted certiorari in the following cases for the next term. The summaries below were provided by Dan Schweitzer, NAAG Supreme Court Counsel.

**T-Mobile South, LLC v. City of Roswell, 13-975.** The Communications Act of 1934, as amended by the Telecommunications Act of 1996, provides that state and local decisions denying a request to place, construct, or modify a personal wireless facility “shall be in writing and supported by substantial evidence contained in the written record.” 47 U.S.C. §332(c)(7)(B)(iii). At issue is whether a state or local government document stating that an application has been denied, but providing no reasons for the denial, can satisfy that “in writing” requirement. Petitioner T-Mobile applied to the City of Roswell, Georgia for a permit to construct a cell tower. The city council held a public hearing, during which council members expressed their individual reasons for opposing the proposal. At the end of the hearing, the council members voted to deny the application. Two days later, the city sent a three-sentence letter to T-Mobile confirming the denial and informing T-Mobile how it could obtain a copy of the hearing transcript. The letter did not express any reason for the denial. Petitioner T-Mobile applied to the City of Roswell, Georgia for a permit to construct a cell tower. The city council held a public hearing, during which council members expressed their individual reasons for opposing the proposal. At the end of the hearing, the council members voted to deny the application. Two days later, the city sent a three-sentence letter to T-Mobile confirming the denial and informing T-Mobile how it could obtain a copy of the hearing transcript. The letter did not express any reason for the denial. T-Mobile responded by filing suit in federal district court challenging the denial. The district court held that the letter did not satisfy the Communications Act’s “in writing” requirement because, although individual council members had stated their concerns during the hearing, it was impossible for the court to determine which reasons motivated the council as a whole or garnered the support of a majority of the council’s members. The Eleventh Circuit reversed, concluding that the letter and hearing transcript can be considered collectively, and that as such they satisfy the “in writing” requirement. 731 F.3d 1213.

Relying on an earlier decision addressing the same question, the Eleventh Circuit held that under the plain words of the statute, there may be multiple documents setting forth the decision and the reasons for the decision. “All of the written documents should be considered collectively in deciding if the decision, whatever it must include, is in writing.” The court concluded that the letter to T-Mobile, in conjunction with minutes summarizing the hearing and reasons for the denial and a verbatim transcript of the hearing, provided the evidence supporting the decision and satisfied the requirement that a decision be “in writing.” In its petition, T-Mobile argues that the statute requires that a denial must be both “in writing and supported by substantial evidence.” Courts cannot perform judicial review, T-Mobile contends, unless they can ascertain the basis of the decision by reading it in the document transmitting the denial of the application. T-Mobile maintains that the object of the Communications Act is to prevent local governments from imposing undue impediments to wireless communication, and denying applications without providing the reasoning for the decision is a “costly and burdensome, if not downright impossible” impediment.

**Elonis v. United States, 13-983.** At issue is whether, as a constitutional or statutory construction matter, a person can be convicted of the federal crime of threatening to injure another person “only if he subjectively intended to threaten another person” or whether instead he can be convicted if a “reasonable person” would construe his words as a threat. Based on Facebook posts in which he threatened his ex-wife, former co-workers, and others, petitioner Anthony Elonis was charged with the federal crime of “transmit[ting] in interstate or foreign commerce any communication containing . . . any threat to injure the person of another.” 18 U.S.C. §875(c).
Elonis moved to dismiss the indictment, claiming that his speech was protected under the First Amendment. Although the First Amendment does not protect “true threats,” the Court had not defined the scope of that exception until *Virginia v. Black*, 538 U.S. 343 (2003), where it held that the term applies to “those statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals.” Elonis argued that his statements could be punished under that definition only if he had a subjective intent to threaten, i.e., to place the victim in fear of bodily harm or death. The district court denied the motion and later instructed the jury that a “true threat” is made when a “reasonable person would foresee that the statement would be interpreted . . . as a serious expression of an intention to inflict bodily injury or take the life of an individual.” The jury convicted Elonis on four of the charges. The Third Circuit affirmed, rejecting Elonis’ First Amendment argument. 730 F.3d 321.

The Third Circuit held that circuit precedent long ago established that prosecutions under §875(c) require only proof that “a reasonable person would foresee that the statement would be interpreted” as a threat. The court read *Black* as requiring only “that the speaker must intend to make the communication” at issue, and not that the speaker intends to carry out the threat. The court noted that most of the circuits to address this issue have held the same; only the Ninth Circuit has held to the contrary. In his petition, Elonis contends that the objective standard employed by the Third Circuit is “fundamentally inconsistent” with the principle that the First Amendment protects “even speech that is offensive, impulsive, or negligent.” Instead, Elonis argues, the speaker’s subjective intent must be taken into account when considering whether his statements were “true threats.” In essence, Elonis argues, the “reasonable listener” standard is a negligence standard — which means a person can “commit a ‘speech crime’ by accident.” Elonis points to other contexts where the First Amendment imposes mens rea requirements and insists that one ought to be imposed here as well. In granting certiorari, the Court added a question to the one Elonis presented (which dealt only with the constitutional issue): “Whether, as a matter of statutory interpretation, conviction of threatening another person under 18 U.S.C. §875(c) requires proof of the defendant’s subjective intent to threaten.”

**PUBLICATIONS CORNER**

**LAW ENFORCEMENT GUIDE TO VIDEO EVIDENCE**

“Video Evidence: A Law Enforcement Guide to Resources and Best Practices” is designed to provide information on tools and resources available to assist law enforcement with video processes and procedures. It is designed in a FAQ format and includes such topics as video retrieval tools, guidance on storing video files, tools for sharing videos and training resources. It can be accessed at https://it.ojp.gov/gist/164/Video-Evidence-A-Law-Enforcement-Guide-to-Resources-and-Best-Practices.

**THIS ISSUE’S LAW REVIEW ARTICLE:**

**CELL PHONE AND LAPTOP BORDER SEARCHES**