

{ bytes in brief }

LAW AND TECHNOLOGY NEWS MONTHLY

EDITORS: Sharon D. Nelson, Esq. and John W. Simek
ASSOCIATE EDITOR: Jason R. Foltin EDITOR EMERITUS: G. V. Nelson



© 2010 SENSEI ENTERPRISES, INC.

www.senseient.com

COMPUTER FORENSICS | INFORMATION TECHNOLOGY

ISSUE 160 - SEPTEMBER 2010

PLEASE NOTE: The URLs referenced in bytes frequently link to newspapers and other current news sources. These links may fail over time. [Click here to visit Sensei home page at www.senseient.com](http://www.senseient.com)

BLACK HAT: ANDROID, IPHONE APP DATA RISKS OVERLOOKED

On July 29th, Information Week reported on a recent survey titled "The App Genome Project" released by mobile security company Lookout. The survey looked at how Android and iPhone apps handled security and the results weren't so hot - smartphones present more of a risk of data leakage than most users realize. The issue, in Lookout's opinion, isn't so much that Android devices or the iPhone may have vulnerabilities. It's that developers fail to appreciate the risks presented by third-party code and device users fail to consider the implications of granting permission to an app to access their data. For instance, a recent story revealed that one particular wallpaper app for Android devices that had been downloaded several million times was found to be sending user data - phone number, subscriber identifier, and currently programmed voicemail phone number - to a server in China. While it is unclear whether this data gathering was done with malicious intent, it definitely underscores the extent to which mobile devices present an information disclosure risk. According to Lookout, approximately 29% of free Android applications and 33% of free iPhone applications have the ability to access user location data. In addition, 14% of all iPhone apps and 8% of all Android apps can access user contact data. Finally, almost half (47%) of Android apps and just about one quarter (23%) of iPhone apps include third-party code - typically related to ad serving and tracking. Third-party code is particularly troubling. In fact, just last week, Citibank notified U.S. banking customers that its Citi Mobile app for the iPhone contained a programming flaw that left their bank account information stored insecurely. To combat the problem, Lookout stressed that developers need to follow good security practices and urged developers not to allow any sensitive information to be written to log files. A copy of the story may be found at http://news.cnet.com/8301-27080_3-20011780-245.html.

WHITE HOUSE PROPOSAL WOULD EASE FBI ACCESS TO RECORDS OF INTERNET ACTIVITY

On July 29th, The Washington Post reported that the Obama administration is seeking to add "electronic communication transactional records" to the list of items that the law says the FBI may demand without a court order in an attempt to make it easier for the agency to compel companies to turn over records of an individual's Internet activity. According to attorneys for the Federal government, this category of information includes the addresses to which an Internet user sent e-mail; the times and dates e-mail was sent and received; and possibly a user's browser history. It does not include, the lawyers hasten to point out, the "content" of e-mail or other Internet communication. Moreover, proponents of the proposed change have argued that the transactional information at issue is the functional equivalent of telephone toll billing records, which the FBI can obtain without court authorization. Learning the e-mail addresses to which an Internet user sends messages, they have said, is no different than obtaining a list of numbers called by a telephone user. However, to industry lawyers and privacy advocates, this so-called technical clarification is, in reality, an expansion of the power the government wields through so-called national security letters. Moreover, critics have called the proposed change another example of an administration retreating from campaign pledges to enhance civil liberties in relation to national security. Michelle Richardson, legislative counsel for the American Civil Liberties Union, stated that the proposal is incredibly bold, given the fact that most Internet or e-mail providers do cooperate with the government and provide the requested data. Another issue critics have jumped on is that the phrase "electronic communication transactional records" is not defined anywhere by statute. Kevin Bankston, a senior staff attorney with the Electronic Frontier Foundation, stated that this poses a huge problem because the expanded power could then possibly be used to

obtain Internet search queries and Web histories detailing every website visited and every file downloaded. It is clear that both sides are prepping for a long, drawn-out fight. A copy of the story may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2010/07/28/AR2010072806141.html>.

GOOGLE, CIA INVEST IN 'FUTURE' OF WEB MONITORING

On July 29th, Wired.com reported that both the CIA and the Internet search giant Google have expressly backed Recorded Future, a company that monitors the web in real time and says it uses that information to predict the future. To do so, the company scours tens of thousands of websites, blogs and Twitter accounts, stripping from web pages the people, places and activities they mention. The company examines when and where these events happened ("spatial and temporal analysis") and the tone of the document ("sentiment analysis"). Then it applies some artificial-intelligence algorithms to tease out connections between the players. Recorded Future maintains an index with more than 100 million events, hosted on Amazon.com servers. The analysis, however, is on the living Web. The overarching idea is to figure out for each incident who was involved, where it happened and when it might go down. Recorded Future then plots that chatter, showing online "momentum" for any given event. Company CEO Christopher Ahlberg noted that "the cool thing is, you can actually predict the curve, in many cases." As this recent investment demonstrates, America's spy services have become increasingly interested in mining "open source intelligence" - information that's publicly available, but often hidden in the daily avalanche of TV shows, newspaper articles, blog posts, online videos and radio reports. As former CIA-director General Michael Hayden once explained, "there's a real satisfaction in solving a problem or answering a tough question with information that someone was dumb enough to leave out in the open." A Recorded Future blog posting on the technology may be found at <http://blog.recordedfuture.com/2010/03/13/recorded-future---a-white-paper-on-temporal-analytics/>.

SYMANTEC FINDS 92% OF ALL E-MAIL IS SPAM

On August 12th, Information Week reported that a recent study by Symantec has found that spam is on the rise, and as of July 2010 spam comprises 92% of all e-mail messages, up from 89% just one year ago. On a brighter note, the report stated that phishing is down; albeit, the rise of a new Live-Chat based attack is of considerable concern. More specifically, this particular type of attack spoofs an e-commerce website's "live chat" feature that targets a person's login ID and password for the legitimate e-commerce site. Overall, news on the phishing front remains fairly positive. For instance, the amount of spam containing a phishing attack declined from June to July of this year by 5%. Likewise, the number of different kinds of phishing attacks has been declining. In particular, the number of unique phishing websites - created by automatic attack toolkits - decreased by 60% from June to July, though the number of unique URLs used in phishing attacks increased by 10%. Importantly, the report also pointed out that spammers, ever topical, have continued to shift their tactics. In fact, just one year ago, Barack Obama and Michael Jackson led the spam subject-line charts, while this past June the World Cup dominated. In July 2010, however, the most-seen spam subject line was "claim your part of the \$20 billion BP oil fund." And, as always, regional variations are in full effect. For instance, Russian spammers have blanketed their country - in the grip of a combined heat wave and wildfires of unknown magnitude - with false advertisements for air conditioners. A copy of the story may be found at <http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=226700151>.

MCAFFEE SAYS SECURITY INDUSTRY FAILING ON CYBERCRIME

On August 10th, Information Week reported that antivirus vendor McAfee has called on security researchers and the security industry at large to go on the offensive against criminals and pursue a more proactive strategy for fighting cybercrime. As senior VP of McAfee Labs Jeff Green explained in a statement, in the arms race against online criminals, and their increasingly sophisticated yet inexpensive crimeware, malware, and spam-generating capabilities, arguably the good guys are losing. Every time we release a new statistic about the rise in malware, it points to our failure as an industry. So what can be done? In its report, McAfee recommended that the security industry make it riskier for criminals to operate online, noting that like any enterprise business model, the psychology of organized cybercrime follows the three major factors: risk, effort, and reward. Along these lines, McAfee suggested publicly disclosing the names of cyber criminals, increasing the fines against cyber criminals, increasing the shutdowns of affected domains, more effective spam filtering, closing dropped e-mail accounts, and freezing payment accounts that are suspected of fraud. Another recommendation was to pursue more "shuns and stuns," meaning routing traffic around known-bad networks, as well as actively disabling botnets. McAfee also

suggested that countries should engage in (or at least foster) more cross-border collaboration as well as coordination with private industry. Notably, as McAfee pointed out, that combination recently helped get alleged Estonian hacker Sergei Tsurikov extradited to the United States. Finally, the report called on the Internet Corporation for Assigned Names and Numbers (ICANN) to take a stronger stance against cyber crime, especially since it's the body that controls the registrants that sell the domains, which cyber criminals use to host malicious sites. However, don't expect things to change drastically anytime soon. This is a long-term effort and one that will require great political bartering and global treaties. But if handled correctly, it could make online crime a significantly more risky endeavor. The report may be downloaded at http://www.mcafee.com/us/research/mcafee_security_journal/index.html.

DEFENSE DEPT. DEMANDS THAT WIKILEAKS RETURN FILES

On August 5th, the U.S. Department of Defense demanded that Wikileaks return all military records that it possesses, saying that the records are the property of the U.S. government. In addition, the department's press secretary, Geoff Morrell, said that the Wikileaks.org website constitutes a brazen solicitation to U.S. government officials, including our military, to break the law by claiming that leaking confidential or classified information is legal. Wikileaks tweeted its response, calling Morrell obnoxious and the request a threat. The website then posted another message, saying "now is a good time to send Wikileaks all your money!" For those not privy to recent events, Wikileaks posted about 100 megabytes of confidential dispatches from U.S. troops in Afghanistan, which appears to have caused more Americans to view the war as a mistake. This led to an unusually heated outcry in political circles, with the White House condemning the leak, a Republican congressman suggesting that whoever gave the documents to Wikileaks be executed for treason, and conservative commentators arguing that Wikileaks.org should be shut down by any means necessary. One problem with censoring Wikileaks, however, is that the organization's main server is located in Sweden. Thus, it would likely be difficult for the U.S. government to convince an Internet service provider in Sweden - or the Swedish government, for that matter - that material that irks the Pentagon is necessarily also illegal under Swedish law. Further, even if Wikileaks.org is taken offline, the group has long planned for mirror sites in other nations. While the U.S. military contemplates what action to take against Wikileaks, it has taken quick action on the home front, banning the Web site from its computers. The Twitter posts may be found at <http://twitter.com/wikileaks/status/20411933104> and at <http://twitter.com/wikileaks/status/20412001224>.

CYBERCROOKS USE WEB APPS TO INFILTRATE SMARTPHONES

On August 2nd, USA Today reported that hackers are adapting tried-and-true computer infections to work on Internet-enabled smartphones that are all the rage with consumers. In fact, just recently, Mobile security firm Lookout discovered 80 Android wallpaper apps that had been harvesting the phone and voicemail numbers and data that can be used to ascertain a user's location from unsuspecting Android users. According to the company, this information was then being transmitted to a website based in China. Similarly, in a more pernicious attack, a scammer has pioneered a way to trigger premium-rate phone calls from infected Windows smartphones. The attack, discovered by Mikko Hypponen, senior researcher at Finnish anti-virus firm F-Secure, begins by spreading infections via a popular 3D game delivered as a Web app. Infected smartphones then initiated expensive calls to far-off locales, such as Somalia. But the calls are cut off before they're answered. The crook uses a system that allows him or her to collect most of the charge for the call. Many security experts have stated that such hacks underscore the potential for spreading malicious Web apps on Android handsets, iPhones, BlackBerrys and Windows Mobile phones. Yet, it is important to note that smartphone Web app infections are still rare. Right now, there are some 40 million known malicious programs for Internet-connected computers vs. less than 600 for smartphones. As always, the richest target remains consumer and commercial banking and other accounts that run on Windows XP computers, still the most widely used devices to access the Internet. However, as much more secure Windows 7 PCs begin to replace older XP machines, cyber criminals inevitably will turn to smartphones and mobile devices such as the iPad. A copy of the story may be found at http://www.usatoday.com/tech/wireless/phones/2010-08-02-cybercrime-smartphones_N.htm.

MOST IT PROS CIRCUMVENT FILE TRANSFER SECURITY POLICIES

On August 5th, Information Week reported that a recent Ipswitch study has found that nearly half of all employees admit to sending highly sensitive or regulated information - the kind which, if lost or stolen, could trigger a data breach notification under many states' laws - at least once per week. VP of global strategy for Ipswitch, L. Frank

Kenney, explained that this problem is likely due to the fact that employees will almost always take the path of least resistance, even if that unintentionally means violating company policies and breaking security protocols. Speaking of protocols, Ipswitch found that 62% of surveyed organizations do have security policies that specify how files may be shared or must be secured for transit. However, 72% of the respondents said that their firm doesn't have any visibility into how files get moved internally or externally, meaning that those file-related security policies are not actually being monitored, enforced, or audited. It might not come as a surprise then that 69% of those surveyed stated that they use plain, unencrypted e-mails and attachments to send highly sensitive or regulated information at least once per month, and 34% say they do it daily. Not surprisingly, Mr. Kenney stated that with all of this file sharing going on at so many firms, it is far too easy for information to get into the wrong hands. For instance, Kenney noted that numerous data breaches result not from attackers hacking into corporate systems, but because a courier loses an unencrypted backup tape en route to a storage facility. In addition, the survey noted that these same risks are prevalent in mobile or portable devices with big storage capacities, such as a USB drive, BlackBerry, or iPhone, which can be easily lost or stolen. 70% of interviewees said they access and store company files and data using their mobile devices, Web mail, and remote connections. In addition, 41% of respondents said they use their own storage devices, such as a USB drive, to back up important work files. More information may be found at http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=226600060&cid=RSSfeed_IWK_Security.

SYMANTEC REPORT CHRONICLES SLOPPY DATA RETENTION PRACTICES

On August 3rd, NetworkComputing.com reported that a recent study by Symantec shows that while most businesses believe in the value of a data retention plan, fewer than half follow one, resulting in increased expense and reduced efficiency as they basically follow a "save everything" policy in practice. More specifically, the study found that while 87 % of respondents believe in the value of a formal information retention plan, only 46 % actually have one. Moreover, the survey reported that 75 % of backup data storage plans consist only of "infinite retention" of materials or legal holds, which are orders not to destroy certain data that may be material in a lawsuit or regulatory investigation. As Symantec explained, these results demonstrate that many organizations are saving data on backup software indefinitely when that data really should be archived. Symantec noted that data does not need to be saved in backup for more than 90 days and could safely be deleted or archived beyond that. As the company explained, this "when in doubt, save everything approach" means companies spend needlessly for extra storage capacity, increase the time it takes to recover data and complicates e-discovery. Further, the survey revealed obstacles to companies adopting a sensible data retention plan. 41 % of IT administrators don't see a need for a plan, 30% said no one in their organization has been given that responsibility and 29 % cited cost as the reason. Symantec also found that backup software is being used for indefinite data storage or legal holds, neither or which is an appropriate or practical use of such software. Illustrative of this fact, the survey found that 70% of respondents use backup storage for legal holds, but that 40 % of the data saved is not relevant to the litigation or investigation. Further compounding the problem, the survey found lax enforcement of data retention policies that are in place. For instance, while 51 % of companies surveyed prohibit employees from creating their own archives on their own computers, 65 % admit that some employees do it anyway. Finally, the report also noted "stunning" differences between the data retention policies and practices of large enterprises versus smaller companies. According to the survey, which grouped the 1,680 respondents into five tiers based on size, 71 % of top-tier enterprises had a formal data retention plan while only 27 % of bottom tier enterprises did. And only 26 % of top tier enterprises used their backup storage for archiving versus 49 % of the bottom tier. To combat these glaring problems, Symantec recommended a five-step plan for developing and adhering to a reasonable data retention system. First, develop a plan. Second, stop using backup storage for legal holds and infinite retention. Third, deploy deduplication, which finds multiple copies of documents and other data and deletes them so only one version is saved. Fourth, delete unneeded data according to your plan. Fifth, use the archive system, not backup, for discovery purposes. A copy of the story may be found at <http://www.networkcomputing.com/deduplication/symantec-report-chronicles-sloppy-data-retention-practices.php>.

CHECK POINT ANNOUNCES NEW SOFTWARE TO CONTROL FACEBOOK, OTHER WEB APPS

On August 2nd, NetworkComputing.com reported that software designer Check Point has announced that it has created new software which is intended to help companies implement flexible policies over 4,500 applications and 50,000 social network widgets. More specifically, this program is designed to give enterprises the ability to restrict access to certain applications at certain times of day or even certain groups of individuals. Many have hailed the

potential of this software, noting that organizations can now give employees free rein to use Web 2.0 apps for business, while curbing unproductive use and minimizing associated security threats. For example, companies can allow chat and selected applications on the Facebook platform, but ban games and other unproductive or risky apps. Additionally, this new software also incorporates a training/employee awareness tool that allows companies to create custom pop-up messages that either advise users of corporate policy or ask how they intend to use the app. In any case, all activities are logged for follow-up reporting, forensics and acceptable use and/or security policy enforcement. Check Point assigns a risk rating of 1 to 5 for each application it controls. For example, P2P file-sharing software BitComet is ranked 5, while Adobe Acrobat Reader is a 1. So when creating policy, rather than go through each of the 4,500-plus applications, enterprises might start by prohibiting all apps carrying a high-risk rating. A copy of the story may be found at <http://www.networkcomputing.com/next-gen-network/check-point-announces-new-software-to-control-facebook-other-web-apps.php>.

NEW THREAT: HACKERS LOOK TO TAKE OVER POWER PLANTS

On August 3rd, The Associated Press reported that computer hackers have started to target power plants and other critical operations around the world in bold new efforts to seize control of them, setting off a scramble to shore up aging, vulnerable systems. These environments are collectively called Supervisory Control and Data Acquisition (SCADA) systems and provide the real-time control needed for industrial operations. While cyber criminals have long tried to break into vital networks and power systems, experts for the first time discovered malicious computer code specifically designed to take over systems that control the inner workings of industrial plants. Luckily, the Department of Homeland Security has responded to this growing threat by establishing specialized teams that can respond quickly to cyber emergencies at industrial facilities across the country. However reassuring this may be, this new malicious code shows that attacks on industrial systems are evolving at warp speed. In the past, it was not unusual to see hackers infiltrate corporate networks, breaking in through gaps and stealing or manipulating data. The intrusions, at times, could trigger plant shutdowns. The threat began to escalate last year, with cyber criminals exploiting weaknesses in systems that control what the industries do. The latest computer worm, dubbed Stuxnet, was an even more alarming progression. Now hackers are creating codes to actually take over the critical systems. Making matters worse, operating systems at power plants and other critical infrastructure are decades old. Sometimes they are not completely separated from other computer networks used by companies to run administrative systems or even access the Internet. Those links between the administrative networks and the control systems provide gateways for hackers to insert malicious code, viruses or worms into the programs that operate the plants. And it's not like critical infrastructure hasn't been warned. Annual reports issued by Homeland Security and the Department of Energy have detailed weaknesses in the industrial computer systems, and have repeatedly pressed companies to improve security practices. Reports as recently as this May urged companies to routinely download patches to update software, change and improve passwords, carefully restrict access to critical systems and use firewalls to separate commonly used networks from those that control key systems. More information may be found at <http://www.google.com/hostednews/ap/article/ALeqM5h7IX0JoE1AGngQoEfWWmCM6THizQD9HC86L80>.

JUDGE GIVES ONLINE NEWSPAPER OPINION POSTERS PROTECTION UNDER CONSTITUTION

On July 27th, Superior Court Judge Calvin Murphy ruled in a pre-trial motion involving a Gaston County murder case that First Amendment protection extends to those who make anonymous comments about stories on news websites. Attorneys for Michael Mead had sought to gain information that could have been used to help reveal the identity of an anonymous commenter on the news organization's website. More specifically, attorneys for Mead were interested in the identity of one anonymous commenter who revealed information about a court date related to a bond revocation prosecutors sought in regard to a polygraph test. What made this comment so interesting was that the information had not been made public yet. In addition, the same commenter also stated that Judge Eric Levinson was "itching" to return Mead to jail to await trial. Hoping to get information about the commenter, one of Mead's attorneys argued that the speech of an anonymous commenter does not meet the definition of a journalist and therefore does not deserve protection. Another of Mead's attorneys, Jason White, argued the commenting section of The Gazette's website was more of a social network than a news gathering operation. In response, John Bussian, attorney for The Gaston Gazette argued that forcing the newspaper to reveal information leading to the identity of a commenter would have a "chilling effect" on anonymous online speech. Further, Bussian noted that, typically, news organizations have a valid argument to protect themselves under the state's shield laws as they attempt to generate public commentary about government officials, the trial and other events. However,

Judge Murphy nullified the request, siding with the The Gaston Gazette and finding that such information remains protected by the First Amendment and state's journalism shield laws. Obviously happy with the decision, Bussain stated that the ruling recognized the principle in North Carolina law that, absent unusual circumstances, the media can't be forced to disclose information about how they manage comments on news reports posted to their websites. He went on to say that courts in other states have protected free press rights this way for a while, but this is the first time a judge in North Carolina has done it. A copy of the story may be found at <http://www.raleightelegram.com/2010072908.html>.

FACEBOOK LAUNCHES "PLACES," GEO-LOCATION SERVICE THAT'S BOTH COOL AND CREEPY

On August 18th, Facebook announced its newest feature, called Places, which allows users to share their locations with friends - and allows their friends to be updated in real-time. The goal of this new app is to bring virtual relationships into the physical world. Additionally, many have hailed this particular feature as a business tool, with local businesses getting free advertising as users post updates about their most recent stops. Yet, with all the benefits, there is a creepier side. For instance, guests at a party can turn the host's home address into a public "place" on Facebook - the only recourse available would be for the host to flag his or her address for removal. Additionally, the idea that an individual's friend can tag him or her at particular locations is nerve-racking. True, the individual still has to give the friend permission to tag you and the individual can then untag him or herself, but one can only wonder how long it takes for the API to be used for a "who's not home?" app for burglars. Initially, the service will only be available as an iPhone app or through a special touch.facebook.com web site - which the company has stated works very well on Android and other smartphones. Apps for other devices are said to be coming soon. A copy of the announcement may be found at <http://blog.facebook.com/blog.php?post=418175202130>.

SCHOOL AVOIDS CHARGES IN WEB CAM SPY CASE

On August 18th, Information Week reported that U.S. Attorney Zane David Memeger has decided not to press formal charges against Lower Merion School District, a Pennsylvania school district that took thousands of pictures of students using the web cams on school-issued laptops; albeit, the district will still have to contend with two invasion-of-privacy lawsuits filed by students in federal court. The case started back in February when the parents of Blake Robbins sued the district after the couple found out that the district was monitoring their son. This shocking revelation came after Lindy Matsko, assistant principal of Harriton High School, told Blake Robbins that the district believed he "was engaged in improper behavior in his home, and cited as evidence a photograph from the Web cam embedded in [his] personal laptop issued by the school district." A subsequent investigation found nearly 58,000 web cam photos and screen shots in the district's databases - some of the images included photos of Blake Robbins sleeping and partially undressed. The school district investigated the incident, but found no evidence that employees were spying on students. But, then again, the investigation still hasn't explained why the district, despite knowing that Blake Robbins had the laptop in his possession, activated the tracking software and left it running for two weeks. That notwithstanding, the school board has since tightened the use of this technology in light of the scandal. In fact, the board this week prohibited school employees from remotely accessing students' computers without the permission of students or parents. More information may be found at <http://www.informationweek.com/news/security/management/showArticle.jhtml?articleID=226700494>.

FBI OUTSOURCES CYBERSECURITY TO MANTECH

On August 18th, Information Week reported that the FBI has awarded Washington-area ManTech International a five-year contract worth nearly \$100 million for round-the-clock intrusion-detection monitoring; security engineering; incident identification and response; vulnerability assessment and penetration testing; cyberthreat analysis; and specialized cybertraining services. ManTech will use ISO 9001 - compliant security processes to provide its services, as well as introduce new technology aimed at reducing cyberthreat risks. ISO 9001 is a global quality standard from the International Organization for Standardization (ISO) for good management practices. If nothing else, the deal shows willingness of the federal government to place IT services in the hands of third parties in an attempt to beef up its cyber security, as many agencies don't have enough staff on hand to do the job and often handle sensitive and highly classified intelligence information. In fact, a recently released Forrester Research report found that while businesses and the public sector used to be hesitant to outsource security, the market for managed security services has been growing steadily over the last few years. Moreover, according to Forrester,

government customers are one of the primary markets for managed security services providers (MSSPs). The story may be found at <http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=226700486>.

RESEARCHERS USE SMUDGE ATTACK, IDENTIFY ANDROID PASSCODES 68% OF THE TIME

On August 16th, ZDNet.com reported that Penn State researchers have managed to identify the pass code patterns on two Android smartphones (the HTC G1 and the HTC Nexus One), 68% of the time, using photographs taken under different lighting conditions, and camera positions. According to the researchers, who have described their findings in a paper titled "Smudge Attacks on Smartphone Touch Screens," they began by evaluating the conditions by which smudges can be photographically extracted from smartphone touch screen surfaces. The researchers considered a variety of lighting angles and light sources as well as various camera angles with respect to the orientation of the phone. For the researchers, the results were very encouraging; for the everyday user, they are downright scary. In one scenario, the pattern was partially identifiable in 92% and fully in 68% of the tested lighting and camera setups. Even in the worst performing experiment, under less than ideal pattern entry conditions, the pattern was partially extracted in 37% of the setups and fully in 14% of them. Armed with these results, the researchers recommended that Google strengthen Android's password pattern. In fact, they went so far as to say that entrusting the confidentiality of your data to a highly marketable, user-friendly touch screen password pattern, is a bad decision in the first place, if the user is not considering the use of third-party data encrypting applications in case the device gets stolen/lost. A copy of the story, along with a link to download the researcher's paper may be found at <http://www.zdnet.com/blog/security/researchers-use-smudge-attack-identify-android-passcodes-68-percent-of-the-time/7165>.

FEDS: ONLINE 'SEXTORTION' OF TEENS ON THE RISE

On August 14th, ABC News reported that both federal prosecutors and child safety advocates have said that they are seeing an upswing in such cases of online sexual extortion ("sextortion"). For those not privy to this new type of extortion, it typically occurs after a teen texts nude cell phone photos or shows off his or her body. Then, after pornographers come across the racy pictures, they threaten to expose the teen's behavior to friends and family unless he or she poses for more explicit porn, creating a vicious cycle of exploitation. While no one currently tracks the number of cases involving sextortion in either state or federal courts, prosecutors and others have pointed to several recent high-profile examples as evidence that the problem is growing. For instance, in Alabama, Jonathan Vance, 24, of Auburn was sentenced to 18 years in prison in April after he admitted sending threatening e-mails on Facebook and MySpace extorting nude photos from more than 50 young women in Alabama, Pennsylvania and Missouri. Then there is the case of Antony Stancl, an 18 year-old Wisconsin man who received 15 years in prison in February after prosecutors said he posed as a girl on Facebook to trick male high school classmates into sending him nude cell phone photos, which he then used to extort them for sex. Finally, a 31-year-old California man was arrested in June on extortion charges after authorities said he hacked into more than 200 computers and threatened to expose nude photos he found unless their owners posed for more sexually explicit videos. Authorities said that 44 of the victims were juveniles. Federal prosecutors said he was even able to remotely activate some victims' webcams without their knowledge and record them undressing or having sex. These examples have prompted many to caution teens about their online activities. What many teens fail to realize is that privacy is nonexistent on the Internet, and once indiscretions appear online, they are virtually impossible to take back. One nude photo sent to a boyfriend's cell phone could easily be circulated through cell phone contacts and wind up on websites that post sexting photos. Once there, it's available for anyone who wants to trace it back to the person in the photo. Further compounding the issue, teens can be quite vulnerable to blackmail because they're easy to intimidate and embarrassed to seek help. And the extortionists are often willing to make good on their threats. A copy of the story may be found at <http://abcnews.go.com/US/wireStory?id=11401876>.

Bytes in Brief[™] is a FREE monthly digest of Internet law and technology news delivered to you by e-mail. For members of the legal and business community interested in Internet law and technology developments, *Bytes in Brief* provides a synopsis of related news and links to sources with more expanded coverage. In the time it takes to drink a cup of coffee, *Bytes in Brief* is designed to make sure you are tracking major developments in this fast moving area.

If staying current in this field is important to you and you find yourself buried under unread magazines, newspapers and journals, *Bytes in Brief* can help you stay in touch without a major outlay of time or expense.

To subscribe, enter your e-mail address into the sign-up box below. It will take you offsite to the *Constant Contact* website, where our opt-in only list is maintained and updated. After you confirm your e-mail address, you will receive an e-mail asking for confirmation that you do wish to become a *Bytes In Brief* subscriber. Once you reply to that e-mail, you will be added to the subscription list.

Subscribe to <i>Bytes in Brief!</i>	
Email: <input type="text"/>	<input type="button" value="Go"/>

Privacy by  **SafeSubscribeSM**
For Email Marketing you can trust

Copyright © 2010 Sensei Enterprises, Inc. All rights reserved.