May-June 2015 Issue

The following is a compendium of news reports, case law and legislative actions over the latest bi-monthly period that may be of interest to our AG offices that are dealing with cyber-related issues. Neither the National Association of Attorneys General nor the National Attorneys General Training & Research Institute expresses a view as to the accuracy of news accounts, nor as to the position expounded by the authors of the hyperlinked articles.

This Issue’s Feature Article: “Understanding the ‘Nonce-Sense’ of Bitcoin: A Guide for Prosecutors”
By Johnette Jauron, Deputy Attorney General, California Department of Justice

Understanding cryptocurrency in general and Bitcoin in particular is crucial to investigating and prosecuting dark market transactions on the Internet. As in any illicit financial investigation, following the money is often the best way to catch the perpetrator and prove the case. Bitcoin transactions are not the anonymous transfers they are reputed to be; however, with some background knowledge, patience and a little creative investigation, Bitcoin transfers can yield admissible evidence in a criminal case. This article summarizes Bitcoin as a protocol, discusses bitcoins as currency, introduces the concept of the blockchain and offers investigative examples of where Bitcoin transactions can provide evidence of criminal conduct and identify Bitcoin users.¹

Article continues on page 16.

Attorneys General Fighting Cybercrimes

Thirty-eight Attorneys General, led by Texas Attorney General Ken Paxton, reached a settlement with Radio Shack Corp. limiting the sale of consumers’ personally identifiable information. Under the terms of the agreement, reached as a result of mediation in Radio Shack’s bankruptcy proceeding, the bulk of the company’s consumer data will be destroyed, and the purchaser of Radio Shack’s assets will only be able to access the email addresses provided by customers during the last two years.
Twenty-two Attorneys General entered into a settlement with Classmates Inc., as well as Florists’ Transworld Delivery Inc. and FTD.com Inc., in which the companies agreed to pay $11 million, including a $3 million consumer restitution fund, to resolve allegations of engaging in misleading advertising and billing practices. Specifically, the investigation focused on the companies' relationships with third parties who offered membership programs using negative option marketing tactics upon completion of a consumer's transaction with Classmates or FTD. Classmates and FTD also shared consumers' personal information so they could be billed for the offers. Among other provisions, the agreement prohibits the marketing partners from using the Classmates or FTD names or logos. Further, consumers must receive clear notice they are receiving a separate offer from the partners. Classmates, FTD and their partners are all prohibited from making a "free" or "risk free" offer if it will convert to a paid subscription.

Fifty-one Attorneys General, the Consumer Financial Protection Bureau and the Federal Communications Commission reached settlements with Sprint Corp. and Celico Partnership d/b/a/ Verizon Wireless, resolving allegations the companies placed unauthorized charges for third-party services, such as horoscopes, trivia or sports scores, on consumers' mobile phone bills, a practice known as “mobile cramming.” Under the terms of the settlements, the companies must obtain consumers' express consent before billing them for third party charges, and any such authorized charges must be listed separately on the consumers' bills. In addition, Sprint will pay $68 million, including $50 million in consumer restitution; Verizon will pay $90 million, including $70 million in consumer restitution.

Arkansas Attorney General Leslie Rutledge’s Cyber Crimes Unit arrested Lance Smith for possession of child pornography, a Class C felony. Unit agents seized a laptop, hard drive and flash drive from Smith’s residence which will undergo further forensic testing at the Unit’s forensic lab.

California Attorney General Kamala Harris announced that Casey Meyerling, operator of cyber-exploitation website WinByState.com, pleaded no contest to one count of extortion, three counts of attempted extortion and one count of conspiracy. The investigation by the Attorney General’s eCrime Unit found Meyerling solicited the anonymous, public posting of private explicit photographs of individuals without their permission and then required victims to pay $250 via a Google Wallet account to remove the posted photographs. Following Meyerling's
plea, the court found him guilty. The Rohnert Park Department of Public Safety and the Northern California Computer Crimes Task Force assisted with the case.

**Illinois Attorney General Lisa Madigan** filed suit against FileFax Inc., a document storage company, for allegedly exposing thousands of patient medical records containing social security numbers and other personal information. The records were those of patients of Suburban Lung Associates, which contracted with FileFax to maintain and destroy them. The suit alleges FileFax failed to provide safe and secure collection, retention, storage and destruction of the records, citing one instance where FileFax disposed of records in a publicly accessible unlocked garbage dumpster outside of its facility. Assistant Attorneys General Matthew Van Hise and Yangsu Kim of the Consumer Fraud Bureau are representing the State.

**Kentucky Attorney General Jack Conway’s** Cybercrimes Unit investigators arrested Brian Evans on 20 counts of possession of child pornography, a Class D felony punishable by one to five years in prison on each count. The investigators, along with State Police troopers, had executed a search warrant at Evans’ residence. The case is being prosecuted by the Casey County Attorney’s office.

**Louisiana Attorney General Buddy Caldwell’s** Cyber Crime Unit investigators arrested George Rogers on 100 counts of possession of child pornography. The arrest resulted from an investigation by the Unit, U.S. Department of Homeland Security Investigations, the State Police, the St. Tammany Parish Sheriff’s Office and the Slidell Police Department. Rogers faces up to 20 years in prison on each count.

**Massachusetts Attorney General Maura Healey** announced that State Police assigned to her office arrested Jeffrey Duncan for possession of child pornography. Based on information from the National Center for Missing and Exploited Children about an email account that was allegedly obtaining child pornography images, the State Police linked the account to Duncan and obtained and executed a search warrant for his residence. Initial investigation of devices seized from the residence revealed alleged child pornography images. The case is being prosecuted by Assistant Attorney General Benjamin Hoerner of the Cyber Crime Division. Investigators from Attorney General Healey’s Digital Evidence Lab and the Springfield Police Department assisted in the investigation.
Mississippi Attorney General Jim Hood announced that William Conley pled guilty to one count of child exploitation and was sentenced to 40 years in prison, with eight years to serve and five years of post-release supervision. The undercover investigation by Attorney General Hood’s Cyber Crime Unit/Internet Crimes Against Children Task Force found Conley was downloading child pornography videos using a file-sharing program. The case was prosecuted by Special Assistant Attorney General Brandon Ogburn.

New Hampshire Attorney General Joseph Foster’s Consumer Protection and Antitrust Bureau entered into a settlement with Court Ordered Classes, Inc., an online California company, resolving allegations the company solicited residents to enroll in its online classes on domestic violence, anger management and batterers’ issues under the false representation the classes were approved by the State to fulfill the court-ordered requirement for counseling. Under the terms of the Assurance, the company agrees not to enroll or accept payments for courses from residents for at least one year, after which it may apply for approval to do so from the Attorney General. The company will remove any reference to the State on its website and will pay $1,500 in lieu of a civil penalty and reimburse the State $1,350 for the cost of its investigation.

Acting New Jersey Attorney General John Hoffman and the Division of Consumer Affairs obtained a settlement with Jeremy Rubin, the developer of “Tidbit,” a software code offered to website developers as a way to generate revenue by taking over part of the processing power of computers visiting those websites in order to mine for Bitcoins, a virtual currency. The Division investigation found Rubin offered the software to website developers without reviewing their privacy policies and without any control, compliance or review mechanism in place. According to the Consent Order, Rubin is prohibited from accessing or attempting to access residents’ computers without clearly and conspicuously notifying the owners and obtaining their consent. The Order also contains a $25,000 settlement, to be suspended and automatically vacated within two years upon compliance. Deputy Attorney General Glenn Graham of the Consumer Fraud Prosecution Unit and Deputy Attorney General Elliott Siebers and former Deputy Attorney General Edward Mullins III of the Government and Healthcare Fraud Unit represented the State.

New York Attorney General Eric Schneiderman’s office filed suit and obtained a temporary restraining order against The College Network and its owner, Gary
Eyler, charging the Indiana-based company used false and deceptive advertising to induce prospective nursing students into buying ineffective study guides. The suit alleges the company’s online ads offered associate degrees in nursing that could be earned "in just 18 months," and created the false impression The College Network was affiliated with Excelsior College, an accredited online college in Albany. When prospective students responded to the online ads, the company sent representatives to their home who used high pressure sales tactics to enroll them in the company’s program, consisting of a series of ineffective study guides, and charging them $500 for each guide. The suit also names Tennessee-based Southeast Financial Credit Union, which partnered with the College Network to provide financing to students, and American Credit Exchange, a collection agency operated by Eyler to pursue students who defaulted on their loans. Assistant Attorneys General Amy Schallop and Emily Auletta of the Consumer Frauds and Protection Bureau are representing the State.

North Carolina Attorney General Roy Cooper announced that a default judgment has been entered against computer repair business Raleigh Geeks and its owners, Timothy Staie and Mark White. The company, also operating as Caveman Computers, ProTech Computers and Fuquay Computer Center, accepted upfront payment for computer repairs without making repairs on time, if at all. In some instances, Raleigh Geeks returned different computers to customers, claiming they were the computers originally brought in. The default judgment bans defendants from operating a computer repair business in the State and orders them to pay $10,425.53 in restitution and up to $445,000 in civil penalties. They are also ordered to return any still-missing computers.

Pennsylvania Attorney General Kathleen Kane’s Child Predator Section and the Mount Carmel Police Department, pursuant to an online investigation initiated by the Monroe County District Attorney’s Office, executed a search warrant at the residence of Jason Hile and seized multiple computers. A preliminary review of the seized evidence by Attorney General Kane’s Computer Forensics Unit revealed numerous files of suspected child pornography and will be further analyzed. Hile, who was not at home during the search, was later arrested on two counts of distributing child pornography, 15 counts of possessing child pornography and one count of criminal use of a communications facility. The case will be prosecuted by Senior Deputy Attorney General Christopher Jones of the Section.
Texas Attorney General Ken Paxton announced the results of “Operation Broken Heart,” a national undercover operation that included his Internet Crimes Against Children Task Force (ICAC). During the two-month period, Attorney General Paxton’s ICAC executed 12 search warrants statewide and arrested 17 suspects for possession or promotion of child pornography and/or engaging in online solicitation of a minor for sexual purposes.

Vermont Attorney General William Sorrell filed a settlement with Embassy Suites South San Francisco, resolving allegations the hotel failed to notify consumers of a security breach without unreasonable delay. The hotel had received notification from customers of unauthorized charges on their credit cards, but did not send notice of a breach to residents until six months later.

Virginia Attorney General Mark Herring joined Dana Boente, U.S. Attorney for the Eastern District of Virginia, and Douglas Mease, Special Agent in Charge of the Richmond Office of the U.S. Secret Service, to announce that Ofort Awuah and Dane Ellis were convicted by a federal jury of Access Device Fraud, Conspiracy to Commit Access Device Fraud and Aggravated Identity Theft. The men made online purchases using stolen credit card numbers and identities, often rubbing down the embossed numbers on “My Vanilla” commercial gift cards and using an embosser to place the stolen credit card numbers on them, along with the name of the person whose number they had stolen. Awuah faces maximum penalties of 10 years’ in prison on two access device fraud counts, 15 years on a third access device fraud count, seven years on the conspiracy count and a mandatory consecutive two years on the aggravated identity theft count. Ellis, of New York, faces maximum penalties of seven years’ incarceration on a conspiracy count and 15 years on an access device fraud count. The case was investigated by the Fredericksburg and Fairfax County Police Departments, the Stafford County Sheriff’s Office and the U.S. Secret Service as part of the Metro-Richmond Identity Theft Task Force. Special Assistant U.S. Attorney Ann Reardon and Assistant U.S. Attorney Michael Moore are prosecuting the case.

Wisconsin Attorney General Brad Schimel’s special agents coordinated “Operation New Hope,” a peer-to-peer operation conducted by the Wisconsin Internet Crimes Against Children Task Force that targeted individuals who possess and distribute child pornography. Personnel from 45 local, state and federal law enforcement agencies participated in the operation, which resulted in service of 17 search warrants, 18 arrests and six additional criminal referrals.
Legislative News

Sexual Cyberharassment
FLORIDA. On May 15, 2015, Governor Rick Scott signed SB 538 into law, a bill making it a crime to publish online a sexually explicit photograph of another without their consent and authorizing law enforcement to arrest, with probable cause and without a warrant, any person suspected of committing such a crime. A person who violates the statute commits a misdemeanor of the first degree, and a person with subsequent violations commits a felony of the third degree. In addition, a victim may bring a civil action for injunctive relief and up to $5,000 in monetary damages. The bill has been codified as Chapter 2015-24 and will become effective on October 1, 2015.

Employee Social Media Accounts
VIRGINIA. New Virginia Code § 40.1-28.7:5, providing that an employer cannot require an employee to turn over usernames or passwords for personal social media accounts, becomes effective on July 1, 2015. The law also prohibits requiring employees to add another employee, supervisor or administrator to the list of contacts for the account or taking action against the employee for exercising rights under the statute. It applies to current and prospective employees and includes state and local governments in the definition of private employers.

Data Breach Notification
CONNECTICUT. On June 1, 2015, the Connecticut House passed SB 949, a bill which would provide greater protections for data obtained by any entity contracting with the state or doing business in the state. The bill would require notice be given within 90 days after discovery of a data breach compromising a person’s personal information, as opposed to current law which requires notification “without reasonable delay.” Among other provisions, the bill also requires the notice of breach to include an offer of at least one year of free identity theft prevention and monitoring services. The Senate passed the bill on May 28, 2015.

Warrant Requirement for Searches of Electronic Devices
CALIFORNIA. On June 3, 2015, the California Senate passed SB 178, a bill which would require law enforcement to obtain a search warrant or wiretap order before searching an individual’s smartphone, laptop or other electronic device or accessing information stored on remote servers.
Revenge Porn
VERMONT. On June 17, 2015 Governor Peter Shumlin signed H. 105 into law, a bill criminalizing the distribution of sexually explicit images of another person without that person's consent. Under the new law, sharing sexually explicit images of another with intent to harm the victims is a misdemeanor. Distributing the image for monetary gain is a felony punishable by up to five years in prison and a $5,000 fine. Victims may also file a civil action for damages. The legislation, codified as Act 62, becomes effective on July 1, 2015.

In the Courts

Fourth Amendment: Search for Cell Phone Serial Number
State v. Green, 2015 La. App. LEXIS 715 (April 15, 2015). The Louisiana Court of Appeal found the removal of the back of defendant’s cell phone to obtain the serial number was not a search. Justin Green was arrested as a suspect in a case involving the online solicitation of a minor, and his cell phone was seized. A detective removed the back of Green's cell phone and its battery to obtain the serial number and data card information. The detective subsequently obtained a search warrant for the seized cell phone as well as the victim’s cell phone. A computer forensic lab was able to retrieve all text messages from the victim's phone, but Green's cell phone was not compatible with their equipment, so the detective turned on Green's phone and took pictures of the text messages. Green was charged with computer-aided solicitation of a minor and indecent behavior with juveniles. Green moved to suppress evidence obtained from his cell phone, arguing a search was conducted prior to issuance of the search warrant, which the trial court denied. Green was found guilty at a bench trial of computer-aided solicitation of a minor, but not the indecent behavior charge, and was sentenced to 10 years in prison without benefit of parole, probation or suspension. He appealed, and among other issues, again argued the court erred in not suppressing evidence from his cell phone. The appeals court disagreed, finding the officer’s removal of the back of Green’s cell phone was not a “search” within the meaning of the Fourth Amendment and, as such, the officer was not required to obtain a search warrant prior to retrieving the identifying information. The judgment was affirmed.

Fourth Amendment: Use of P2P Software to Remotely Access Files
State v. Peppin, 2015 Wash App. LEXIS 748 (April 9, 2015). In a case of first impression, the Appeals Court of Washington ruled law enforcement’s use of
enhanced peer-to-peer file sharing software to remotely access the shared files on defendant's computer was not illegal. An undercover detective used advanced peer-to-peer file sharing software to access and download shared files containing child pornography. He learned the IP address was connected to Casey Peppin via a search warrant to Quest Communications, and then obtained a search warrant for Peppin's computer. A forensic examination uncovered more than 100 videos of child pornography. Peppin was charged with three counts of first degree possession of child pornography and one count of first degree dealing in child pornography. He moved to suppress the files downloaded by the detective, arguing law enforcement's access of his files via the Internet was an intrusion into his privacy and an unlawful warrantless search. The trial court found Peppin had no reasonable expectation of privacy in the files and denied the motion. Peppin was found guilty at a bench trial on the possession counts, but not guilty on the dealing count, and was sentenced to 46 months in prison. On appeal, he challenged the denial of his motion to suppress. The appeals court found Peppin did not have a constitutionally protected privacy right in the image files he shared with the public and, thus, law enforcement's use of enhanced peer-to-peer file sharing software to remotely access the shared files on his computer was not illegal. The judgment was affirmed.

Expectation of Privacy: Search of Contents of GPS Device

State v. Clyburn, 2015 N.C. App. LEXIS 269 (Apr. 7, 2015). The Court of Appeals of North Carolina reversed because the trial court did not make sufficient findings of fact to establish whether defendant had a reasonable expectation of privacy. Kenneth Clyburn was arrested for possession of drug paraphernalia. Officers searched him incident to arrest, finding a Garmin GPS and attached charger he claimed was his own. Without permission, the officers pressed the “Home” button and scrolled through the address history, finding the closest address. Officers sent a patrol car to that address and located a car with a broken window in the driveway and an owner’s manual on the seat for a GPS of the same make and model as found on Clyburn. Officers contacted the homeowner, who identified the GPS as his. Clyburn was indicted on felony breaking and entering a motor vehicle, misdemeanor larceny, possession of drug paraphernalia and being a habitual felon. He moved to suppress the evidence obtained as a search of his person, testifying he purchased the GPS from a man on the street. The trial court concluded that the search of the GPS was not necessary nor justified as a search incident to arrest, and any evidence obtained as a result of the search of the digital contents of the GPS was inadmissible. The State appealed the order, and the appeals court
reversed, concluding the trial court, although properly concluding the search was not justified as a search incident to arrest, did not make sufficient findings of fact based on the evidence to establish that Clyburn had the necessary expectation of privacy. Specifically, the court found the trial court failed to make a factual determination as to whether Clyburn purchased the GPS and, if so, whether he knew or should have known it was stolen. The case was reversed and remanded.

*Ed. note: Assistant Attorney General Derrick Mertz of the North Carolina Office of Attorney General represented the State on appeal.*

**Fourth Amendment: Warrantless Search of Cell Phone Location Data**

*Herring v. State*, 2015 Fla. App. LEXIS 7750 (May 22, 2015). A Court of Appeal of Florida ruled that law enforcement’s failure to obtain a warrant violated defendant’s Fourth Amendment rights. Kendrick Herring shot two men with whom he was arranging a drug deal, killing one of them. The other man contacted law enforcement, telling them he and Herring had been communicating by cell phone. Law enforcement, using an exigent circumstances form, obtained Herring’s real time cell phone location data from his cell phone provider, located and arrested him, recovering his cell phone and a handgun that matched the bullets found at the scene of the shooting. Herring was charged with second-degree murder, attempted first-degree murder, aggravated assault on a law enforcement officer, possession of a firearm by a convicted felon, carrying a concealed firearm and resisting arrest with violence. He moved to suppress evidence obtained as a result of the search and seizure of his real time cell phone location data, arguing it was illegally seized because law enforcement did not obtain a warrant. The trial court denied the motion, finding exigent circumstances abrogated the warrant requirement. Herring appealed, and the appeals court ruled the trial court erred in denying the motion. The court found Herring had an expectation of privacy in the real time cell phone location data, and law enforcement’s failure to obtain a warrant violated his Fourth Amendment rights. The court further found the facts presented did not demonstrate exigent circumstances that would overcome the warrant. The judgment was reversed.

*Ed. Note: Assistant Attorney General Justin Chapman of the Florida Office of Attorney General represented the State.*

**Intent to Harass: Twitter Messages**

defendant's conviction for electronically distributing a harassing message. After an encounter with his ex-wife, in violation of a restraining order, Francis Shivers posted numerous harassing tweets, falsely alleging he had a restraining order against his ex-wife and that she was stalking him and making death threats against him. He was charged and convicted by a jury with electronically distributing a harassing message and with violating a restraining order. He appealed, arguing insufficiency of the evidence. The appellate court found sufficient evidence supporting the conviction because a reasonable trier of fact could conclude Shivers acted with intent to incite or produce unlawful action by a third party when he electronically distributed messages about his ex-wife using social media. The judgment was affirmed,

Admissibility: Cell Phone Tracking Information
State v. Smith, 2015 Conn. App. LEXIS 134 (Apr. 14, 2015). The Appellate Court of Connecticut found admission of the cell phone tracking information was harmless. Kendall Smith appealed his conviction by a jury of robbery in the first degree and conspiracy to commit robbery in the first degree. Among other claims, he argued the trial court erred in denying his pretrial motion to suppress historical cell site location information from his cell phone records, which police obtained without a warrant from Smith's cellular service provider. The appellate court found the admission of the cell site information, even if erroneous, was harmless, given that 1) Smith's truck was involved in the robbery; 2) Smith was the principal driver on the morning of the robbery; 3) Smith matched the physical description of the robber; and 4) Smith's DNA was recovered from a crack in the windshield of the truck. The judgment was affirmed.

Fourth Amendment: Inference Drawing Ability for Probable Cause
State v. Castagnola, 2015 Ohio LEXIS 977 (Apr. 28, 2015). The Supreme Court of Ohio ruled the search warrant was not supported by probable cause. A police officer investigating damage to a prosecutor's vehicles sought an arrest warrant for Nicholas Castagnola and a search warrant for his residence. The warrant application included references to text messages received by an informant from Castagnola as well as the informant's concealed recording of Castagnola, who stated on the recording that he had to "look up" the prosecutor's address. Other than that reference, the affidavit did not otherwise indicate that Castagnola had conducted an online search, or used a computer, to locate the address. The search warrant was executed and two computers were seized. A forensic analysis revealed files that could contain child pornography, so a second search warrant for
the contents of the computers was obtained. Castagnola was subsequently indicted on 10 counts of pandering child pornography, a fourth degree felony offense. Castagnola moved to suppress, arguing the first warrant was not supported by probable cause because 1) the affidavit did not indicate there was a computer in his home and 2) he had never used the word “online,” so the police officer’s use of the term in the affidavit was an unwarranted inference. Castagnola further argued that since the first search warrant led to the second warrant, evidence from both were fruit of the poisonous tree. The trial court denied the motion, finding the police officer provided a fair characterization and had acted in good faith. In the vehicle damages case, Castagnola was found guilty of two counts of retaliation and one count each of criminal damaging, vandalism, criminal trespass and possessing criminal tools. He was found guilty on all counts in the pandering case and received a total of 30 months in prison and was classified as a Tier II sex offender. On appeal, Castagnola asserted the trial court had erred in denying his motion to suppress. The appellate court agreed, finding the search warrant was not supported by probable cause because the affiant police officer negligently usurped the magistrate’s inference drawing authority. The judgment was reversed and remanded.

Fourth Amendment: Warrantless Search of Probationer's Cell Phone

_ State v. Roberts_, 2015 ND 106 (April 28, 2015). The Supreme Court of North Dakota ruled defendant’s rights were not violated by further review of the data on his cell phone. Garron Gonzalez was on probation after having pled guilty to two counts of gross sexual imposition. His probation was subject to conditions, including that he not have unsupervised contact with minor females and not purchase, possess or use sexually stimulating materials. His probation officer received information that Gonzalez was being investigated for contact with a minor, so he searched Gonzalez’ residence and vehicle, finding two smartphones. The probation officer searched the phones and found evidence Gonzalez had violated the conditions of his parole and arrested him. The State petitioned to revoke Gonzalez’ probation, alleging Gonzalez violated the probation conditions. The lower court revoked Gonzalez’ probation and resentenced him to 20 years’ incarceration on each count, to run consecutively, with credit given for time served. Gonzalez appealed, and the Supreme Court affirmed. Gonzalez then applied for post conviction relief, also moving to suppress evidence obtained from the search of his cell phones, arguing the warrantless search was unreasonable and violated his Fourth Amendment rights. The trial court denied the motion, and Gonzalez appealed on the same grounds. The Supreme Court found Gonzalez’
probation officer had reasonable suspicion that Gonzalez was engaging in unlawful activity because Gonzalez has been convicted of gross sexual imposition; the conditions of his probation required him to have no unsupervised contact with minor females; and the probation officer received information about Gonzalez' alleged contact with a juvenile. The court ruled that once the probation officer found evidence of probation violations on Gonzalez' cell phones and seized the phones, Gonzalez no longer had a privacy interest in the data on the phones, and his rights were not violated by further review of that data. The judgment was affirmed.

**Plain View Doctrine: Seizure of Memory Cards**

*Commonwealth v. Tarjick*, 2015 Mass. App. LEXIS 51 (May 18, 2015). The Massachusetts Appeals Court held that police properly seized the memory cards under the plain view doctrine. Aaron Tarjick's minor stepdaughter accused him of sexually abusing her and her friend, telling police he also took sexually explicit photos of her on his cell phone and made sexually explicit video recordings of her with his video camera. Police suspected Tarjick transferred the photos and videos to the family computer since the stepmother said he watched explicit images of young girls on the computer. State police obtained a search warrant for the home, listing the family computer, Tarjick's cell phone and his video camera as items to seize. Police also seized three memory cards from the camera that were not listed in the warrant, and they obtained a second warrant to search the contents of the cards. Police found photos of Tarjick posing partially nude with his minor son, but no explicit photos of the stepdaughter. Tarjick was indicted on three counts of rape of a child with force (stepdaughter), eight counts of indecent assault and battery of a child under age 14 (stepdaughter), one count of rape of a child with force (friend) and one count of posing with a child in a state of nudity (son). He moved to suppress the contents of the memory cards because they were not listed in the original search warrant; the motion was denied. Tarjick was found not guilty on the count of posing with a child in a state of nudity, was convicted of rape of a child without force (friend) and was found guilty of all other charges. He appealed, and among other issues again argued the evidence from the memory cards should have been suppressed. The appeals court ruled police properly seized the memory cards under the plain view doctrine as the stepdaughter stated that Tarjick took sexually explicit photos of her with his cell phone. The court noted the police properly obtained a second search warrant to view the images stored on the cards. The judgments were affirmed.
But see…

*Commonwealth v. Sodomsky*, 2015 Pa. Super. 133 (June 5, 2015). The Pennsylvania Superior Court found suppression of the evidence was warranted. Kenneth Sodomsky authorized Circuit City to install an optical drive and DVD burner on his desktop computer. During installation, the technician searched Sodomsky's files for a video that he said was necessary to test the burner. He found a video file appearing to be child pornography and contacted police, who viewed the file. When Sodomsky came for his computer, police told him it was being seized for suspected child pornography. Police obtained a warrant to search the computer and found child pornography. Sodomsky was charged with two counts of sexual abuse of children and one count of obscene materials. He moved to suppress the evidence obtained from his computer, arguing he had a privacy interest in his computer, which the trial court granted. The Commonwealth filed an interlocutory appeal, arguing Sodomsky relinquished his privacy interest when he gave the computer to Circuit City for installation, and a Superior Court panel reversed. Sodomsky filed a petition to introduce new evidence, and two experts testified on his behalf that the technician's search of the computer files was not standard procedure nor a proper method for testing the burner. The court found in light of this evidence that Sodomsky had a privacy interest in his computer and again granted his suppression motion. The Commonwealth again appealed, arguing Sodomsky failed to establish he had a reasonable expectation of privacy before he relinquished the computer, and the panel again reversed and remanded. Sodomsky filed a Petition to Re-Open Suppression Hearing based on Intervening Change of Law, namely, the U.S. Supreme Court decision in *U.S. v. Jones*, 565 U.S. ____, 132 S. Ct. 945 (2012). The court found suppression was warranted based on the Commonwealth's search of Sodomsky's computer files and the seizure of his computer because the digital data forming the basis of the charges against him were not in plain view. The order of the suppression court was affirmed.

**Cyberstalking: Statutory Requirements**

*Horowitz v. Horowitz*, 2015 Fla. App. LEXIS 4665 (April 1, 2015). A Florida Court of Appeal ruled the husband's Facebook posts did not constitute cyberstalking. Maureen Horowitz sought an injunction for protection against Sammie Horowitz, her estranged husband, alleging she was a victim of domestic violence, namely cyberstalking. The trial court granted the injunction, and the husband challenged the judgment. The wife argued she was the victim of cyberstalking based on two posts on her husband’s Facebook page; one post contained the lyrics to Atlantic
Starr’s “Secret Lovers,” and the other post contained the text of a private conversation the wife had with a third party via her Facebook account. The wife testified the posts showed the husband had hacked her account or was spying on her via a keylogger program, although she presented no supporting evidence. The appeals court found the husband’s Facebook posts did not constitute cyberstalking because they were not directed at a specific person, as required by §748.048(1)(d), Fla. Stat. (2013), and the wife failed to show the posts caused her substantial emotional distress. Further, the court found the wife failed to establish she was, or was in imminent danger of becoming, a victim of domestic violence. The judgment was reversed.

Eighth Amendment: Lifetime Electronic Monitoring
People v. Hallak, 2015 Mich. App. LEXIS 1133 (May 28, 2015). The Michigan Court of Appeals ruled lifetime electronic monitoring did not violate defendant’s Eighth Amendment rights. A jury convicted Kassem Hallak, a medical doctor, of second-degree and third-degree criminal sexual conduct (sexual conduct with a victim under 13 years of age) and six counts of fourth-degree criminal sexual conduct. He was sentenced to a prison term of 57 to 180 months for the second-degree conviction, 85 to 180 months for the third-degree conviction and 16 to 24 months for each fourth-degree conviction. The trial court also ordered lifetime electronic monitoring as part of his second-degree conviction. He appealed his second-degree conviction, arguing among other issues that the lifetime electronic monitoring violated his Eighth Amendment right against cruel and unusual punishment. The appeals court disagreed, finding it did not violate Hassak’s rights because there was evidence of improper sexual acts involving 13 women or children. The judgment and sentence were affirmed.

High Tech Cases in the U.S. Supreme Court
On June 1, 2015, in the first time the Court has heard a case involving the limits of speech on social media, reversed a Third Circuit decision and held that a conviction for threatening another person over interstate commerce under 18 U.S.C. § 875(c) requires proof that the defendant was aware of the threatening nature of the communication. In Elonis v. U.S., 13-983, Anthony Elonis was convicted under the statute for posting threats to injure his ex-wife, former co-workers and others on Facebook. Elonis appealed the decision, arguing that the jury instruction did not contain an appropriate definition of what constitutes a threat. The U.S. District Court for the Eastern District of Pennsylvania had instructed the jury to consider whether a reasonable person would foresee that others would view the posts as a
“serious expression of intention” to hurt or harm someone, and the Third Circuit affirmed. Elonis had argued his posts should be considered threats only if he intended them as such. Justice Thomas dissented, finding the majority’s approach unsatisfactory and throwing judges into “a state of uncertainty.”

On May 26, 2015, the Court granted the petition for certiorari in Lockhart v. U.S., 14-8358. In that case, Avondale Lockhart pleaded guilty to possession of child pornography and was sentenced under 18 U.S.C. § 2252(b)(2), which requires that a district court must impose a 10-year mandatory-minimum sentence if a defendant convicted of possessing child pornography “has a prior conviction … under the laws of any State relating to aggravated sexual abuse, or abusive sexual conduct involving a minor or ward.” The U.S. District Court for the Eastern District of New York found Lockhart was subject to the mandatory minimum based on his prior state conviction for sexual assault of an adult woman. On appeal, Lockhart argued that his prior conviction did not qualify because it did not involve “a minor or ward,” thus interpreting the clause “involving a minor or ward” as applying to all of the listed categories of state law offenses. The Second Circuit affirmed, holding that the phrase modifies only “abusive sexual conduct” and not the other two offense categories. There is a circuit split on the meaning of the clause, with the Eighth Circuit finding that the phrase modifies all offense categories.

Articles of Interest
“Botnet Takedowns and the Fourth Amendment,” by Sam Zeitlin, NYU Law Review, Volume 90, No. 2. This article examines the Fourth Amendment implications of the government’s use of remote control of malware on private computers to neutralize botnets. The author argues the government could take more intrusive action on infected computers without performing a search or seizure under the Fourth Amendment. He posits that remotely finding and removing malware on infected computers does not necessarily trigger Fourth Amendment protections. The article may be accessed at http://www.nyulawreview.org/issues/volume-90-number-2/botnet-takedowns-and-fourth-amendment.


A. Bitcoin as a payment network protocol.
Bitcoin is a digital form of currency not backed by any commodity or institution. Unlike a commodity currency, which is based on a tangible good such as gold or silver, or a fiat currency, which derives its value from government regulation such as the Euro, Bitcoin's value comes from those who are willing to trade it for goods and services. The Bitcoin protocol is an open source, peer-to-peer (P2P) transfer system that enables irreversible push payments of digital currency from one cryptographically signed address to another.

Bitcoin as a payment system appeals to both legitimate purchasers and criminals alike. It also appeals to civil libertarians who do not want government involvement in their transactions, political activists who value the pseudonymous nature of transfers, speculators who seek to profit from the enormous fluctuations in the Bitcoin exchange rate, geeks who appreciate the technology, drug-seekers who want to avoid street violence and law enforcement scrutiny, and hackers who strive to mask their online footprint through anonymizing networks such as TOR. The level of privacy in a Bitcoin transaction is user-defined. A Bitcoin address, which is a Bitcoin user's public key, can be advertised to the world, such as by a startup seeking public donations, or it can be “mixed” by inserting multiple receipt addresses branching off from the publicly-visible transfer chain to distance a receiver from an earlier transaction.

The increasing popularity of Bitcoin may cause distress for traditional banks. With virtual currency becoming mainstream, banks could be effectively cut out of retail transactions. The Bitcoin ecosystem, with features such as no transaction fees, no interest rates, no chargeback concerns and no control over the value of the currency, has become an attractive market sector. Consumers, previously worried about point of sale vulnerabilities, need not rely on third parties in their transactions. Retailers are “jumping on the bandwagon” as well. As of early 2015, there were 100,000 retailers, most of them online, that accepted bitcoin currency (BTC), and that trend is increasing. $158,800,000 in BTC was processed in 2014, up from $107,575,000 in 2013, an increase of almost 50 percent.

The Bitcoin protocol software sets the supply of bitcoins at a limit of 21 million, which is validated and enforced by protocol participants known as “miners.” Miners observe and validate transactions as legitimate and add valid transactions to the blockchain, a public ledger that permanently documents all payment transfers. Although the cryptography is complicated, the concept of the blockchain permanently recording all electronic transactions is simple and transparent. One need only follow the transactions in the ledger to see the Bitcoin address involved
in the money transfer. Similar to a ticker tape in stock transactions, the time and size of trades are permanently public. The individual users of Bitcoin addresses are not immediately identifiable, but they are not anonymous.

There are only three ways to receive bitcoins: 1) by receipt as a reward for computationally validating a block in the blockchain, known as mining; 2) by transfer from another user; or 3) by purchase, typically from a bitcoin exchange service. Individual bitcoins, or portions thereof, are transferred from one Bitcoin address to another and recorded as part of a block of transactions posted to the blockchain with a date, time and amount of transfer. The software uses mathematical algorithms to create a hash value of the transfer. That hash value, a cryptographic nonce, appends to the previous transaction within the network, forming a chain and confirming that the transfer is the first in time. The blockchain is therefore publicly documented proof of the chronological order of transfers, which effectively prevents double spending. Because everyone in the system is aware of all transactions at all times, they know that the input they receive came from a verified source.

1. Bitcoin Mining

Based on public key cryptography, Bitcoin was developed in 2008 by a programmer (or group of programmers) known only as "Satoshi Nakamoto" as a proof-of-concept for a transparent closed-loop digital economy. It was intended to simulate a gold-based economy in that users expend computational resources to mine currency and place a finite amount of bitcoins into circulation. Inflation rates were also intended to simulate gold so that a total of 21 million bitcoins will ever be created. By limiting the supply, the protocol creates a monetary incentive to validate the network by obtaining more coins rather than attacking or undermining the system.

Bitcoins are minted through a “mining” process that uses computing power to validate transactions on the Bitcoin blockchain. This computational solving of the algorithm is called hashing. Miners use their computers’ processing power to search for a sequence of data that matches the nonce of the current block of transactions. For every match, the miner is rewarded with bitcoins, along with any transfer fees that are part of the transaction being validated. Once the block is validated, or approximately every ten minutes, 25 new bitcoins are created and
awarded to the miner or group of miners, and the block is recorded onto the blockchain.

The Bitcoin protocol is designed to halve its creation rate every four years, which means the more it is used, the more difficult it is to mine. The "genesis block," which is the original block of 50 bitcoins in the blockchain, was generated by Nakamoto as proof-of-concept for the Bitcoin protocol. In the first four years of use, the reward for validating a block was 50 bitcoins. It was once possible for individual computer users to mine coins, but today it is largely done by pooled miners because the computational requirements now necessitate large-scale server equipment. As of June 2015, the reward for mining is 25 BTC. After 2,016 more blocks are validated, in approximately four years, the reward will be halved again. The Bitcoin minting process is expected to cease sometime in 2140. As of block 350,000, which posted on March 30, 2015, two-thirds of all expected bitcoins have been mined and distributed.\textsuperscript{vii}

2. Bitcoin Transfers

Bitcoin circulates and can only be divided by transfer among addresses. Transfers require both a public and a private key. A Bitcoin address, which is an identifier of 27 to 34 alphanumeric characters beginning with the number 1 or 3, serves as the public key in the cryptographic transfer of virtual currency. The address is typically generated by a Bitcoin wallet, which may be obtained through an exchange service. An individual user has a private key that unlocks the hashed algorithm, allowing access to the data containing stored bitcoins. Online exchange services, discussed below, maintain possession of the private key and provide custodial wallets for their users. The transaction data information is hashed; the hash value is injected into a block; and the block is appended to the blockchain and confirmed by miners. Each validated transaction updates the blockchain with the sender’s and receiver’s Bitcoin addresses, the amount of bitcoins, a date and time stamp and a transaction fee.

Once the block is validated, the miner is rewarded with a block reward and all fees from transactions included in the block. The block is then recorded onto the blockchain. The entire process is completed in approximately ten minutes and the data is publicly available on the Internet. The block becomes effectively immutable after six blocks so that it is computationally impractical to overwrite it.
If translated into English, a Bitcoin transaction appears similar to:

\begin{quote}
I, my publicly-known name am giving to this publicly named individual 100 BTC that I received from the computationally-proven valid transaction on April 1, 2015 at 12:00:01, along with a .0001 transaction fee.
\end{quote}

The smallest denomination recognized by the Bitcoin protocol is a Satoshi and amounts to one hundred milli- bitcoin. In order to spend or transfer a portion of a bitcoin, the remainder or balance of the Bitcoin address must also be accounted for in the transaction. Thus, each transaction for a portion of a bitcoin requires an input source (the sender’s address), an output source (the receiver’s address) and an additional output source (the change address) for any remainder amount. A user sends an agreed-upon amount to the intended recipient and the remainder to a change address. Typically, there will be either a single input from a larger previous transaction or multiple inputs of smaller amounts and at most two outputs: one for the payment and one returning the change, if any. The change address can be a valuable source of information and a first step in conducting a blockchain investigation.

3. Bitcoin Exchange Services

Bitcoin exchange platforms act as nodes through which bitcoins can pass in the P2P network. In order to cash in, cash out or convert large sums of money in the Bitcoin ecosystem, an exchange service is typically used. Exchange services collect and store a significant amount of information about the transactions that pass through them. Many of them collect personal information about their customers, although it is not required by law to do so. When users open exchange accounts, they typically provide multiple layers of personal identifying information depending upon the volume of their transactions. If an exchange service customer uses a mobile exchange app, the exchange service provider will have the customer’s cell phone number, email address, banking information, device ID and wallet and transaction history. Bitcoin exchanges constantly monitor Bitcoin network data and often find and report suspicious activity.

Similar to traditional brokerage companies, exchange service providers offer varying levels of services and typically charge small transaction fees for services such as currency exchange or very large or very small trades. They are thus more convenient and low cost in comparison to traditional funds. However, a Bitcoin user’s private key is a physical data file that is vulnerable to theft or hacking, so
exchange services face significant security risks as do other financial service providers.

Coinbase is currently the most active US-based bitcoin exchange service with more than two million consumer wallet accounts. It allows users to create a Bitcoin wallet, convert currency, accept payments as a merchant and directly transfer money from a bank account. There is a one percent fee for exchanging bitcoins, but sending and receiving them is free. Merchants incur no fees in transactions up to one million dollars, and approved charities pay no fees. In 2014, Coinbase began offering instant purchases for verified users.

Coinbase is proactive and has a vested financial interest in seeking to prevent illegal activity. It is registered with the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) as a Money Services Business, and as with other commodity-backed financial institutions, is required to file Suspicious Activity Reports (SARs) with FinCEN. It has a threshold level of activity that triggers an internal examination of transactions and accounts and has a track record of cooperating with law enforcement. Coinbase has a process designed to assist in criminal investigations and a law enforcement guide to help investigators ask for and receive necessary data. Additionally, Coinbase honors non-disclosure requests and, under some circumstances, may honor a stay-open request.

Mt. Gox, a bitcoin exchange service that experienced massive DDOS attacks in 2013, declared bankruptcy in February 2014. It claimed that its loss, estimated at hundreds of millions of dollars, was the result of a system hack. However, most industry experts agree that poor business practices and lapses in security were the primary cause of the failure. Journalist Paul Vigna of the Wall Street Journal called it an example of "digital Darwinism."

B. Tracing a Bitcoin transaction to a user IRL

Inspecting the blockchain and following the flow of transactions back to a known business or owner of a specific wallet is the key to identifying a specific user. The blockchain data is available on multiple websites, and numerous programs offer blockchain browsing. The websites typically provide a list of a chain's recent blocks; the actual transactions in a given block; links to the previous and next transaction involving each input and output; a list of all transactions involving a given address, including current and historical address balances; and any service-specific memo or text associated with a transaction. By visually inspecting the blockchain, one can trace the flow of inputs and outputs, observing not only
publicly-identified keys, but also distinct patterns of behavior that provide circumstantial evidence of identity.

The most definitive way to identify a public key is to conduct a transaction with it. A user can purchase goods online through a Bitcoin payment interface, store bitcoins in an online wallet service, open a Bitcoin account at an online gambling site, join a mining pool or transact with a mixing service to obfuscate the payment path on the blockchain. Once the transaction is documented on the blockchain, a user can identify the payout address as a hashed value of a public key definitively belonging to that individual or service. If a Bitcoin user’s identity is ever linked to a public key, all transactions associated with that key are listed on the blockchain.

There are some investigative methods that lead to likely identification of individual Bitcoin account users. The blockchain displays at least one input and zero or more outputs for each transaction. Change for a particular transaction does not have to, and rarely does, go back to the original address. Users can have many addresses and can even generate a new address for every transaction. Typically, a certain amount of output goes to a receiver, and an amount of change goes to a new address, often one under control of the sender.

Suspicious transactions are sometimes readily discernable just by looking at the input address, the output address, the transaction pattern and the timestamp of the transaction. For example, a multi-input transaction will reveal that the previous inputs were under the control of the same owner. That transaction can then be linked to other transactions establishing the owner of a key. Similarly, the reuse of one address for multiple transactions could indicate that one individual is using that address as well as every other input address in that transaction. For example, if X and Y are both inputs to one transaction, and Y and Z are both inputs to another transaction, X, Y, and Z are all within the control of the same user.

Sets of addresses can be ascribed to a single controller, such as a wallet service. Some public addresses are collected and tagged by third parties or user forums, so they are easily found in an Internet search. A user could use a QR code as a public address, taking advantage of mobile payment apps to receive bitcoins. Search engines can scrape forums to find Bitcoin addresses, and many online services collect user details such as IP address, email, bank account information or physical address. Some users, such as charities or crowd-funded organizations, publicize their addresses to solicit donations. In 2011, Wikileaks tweeted its
public key in order to solicit “anonymous” donations to the website, making every transaction to and from that address publicly available.

In a private user transaction, a change address typically gives bitcoins in change back to the user of the input address and thus can be linked to an input address. There are applications called tumblers, mixers, scramblers or laundry services that create large batches of addresses offline using freely available software tools. Essentially, the fabricated transaction addresses are inserted between addresses for the legitimate purpose of protecting the privacy of the recipient, or for the nefarious purpose of obscuring the washing of the transaction. Generating batches of Bitcoin addresses is not inherently illegal; it can serve a legitimate purpose, such as when e-commerce websites assign a unique pre-generated address to each customer who chooses Bitcoin payment. However, frequent, high volume transactions with mixing may indicate an attempt to launder illicit activity. An investigation of that laundering requires tracing each transaction and checking each address for clues as to the identity of a user or exchange service.

In a recent case, investigators found the same address was used multiple times in a 24-hour period as a change address. That pattern, coupled with a high volume transfer, drew attention, and an investigator followed each transaction. At the 24th address back in the chain, that investigator was able to find the online dark market site Sheep Marketplace, which had been associated with a recent theft of several million dollars in bitcoins.

If a user makes a Bitcoin purchase through a website, that user’s IP address is usually captured by the website and may be traceable. A suspect’s Internet service provider (ISP) may be able to read the address associated with a purchase because the date and time of the transaction is recorded on the blockchain. If you are investigating a suspicious Bitcoin transaction and know the ISP involved, your search warrant should include any Bitcoin addresses, any information at or near the same time as a Bitcoin transaction and any alphanumeric values that appear to be hashed Bitcoin transactions or keys to Bitcoin wallets.

Cryptocurrency exchanges are valuable sources of information in criminal investigations and dark market activity. Bitcoin exchanges often have information associated with a Bitcoin address, such as email address, name, IP address and a bank account. When a transaction transfers bitcoins to an exchange, the initial input address is known, and the direct flow of an illicit transaction to an exchange
can establish the probable cause needed for a search warrant to the exchange. If a user converts bitcoins to dollars at a bitcoin exchange website, the user’s IP address is also recorded. An exchange node could track the network traffic, detect that the same IP address is sending bitcoins from two different addresses, and thus associate those addresses. Dark market users are often sophisticated enough to employ privacy-enhancing technologies, such as a virtual private network (VPN) or TOR, but unless they are constantly vigilant, they may be identified. User names tied to transactions within an exchange service can be identified years after an exchange. Users may reuse pseudonyms or their variants, allowing a manual or automated search for that pseudonym. Many exchange services also provide a short text memo field with the transaction data. These fields allow a word search or visual inspection of the memos for comments associated with suspicious transactions or a link to common information. Many users who conduct transactions using Bitcoin mistakenly believe their exchange is anonymous, so they may include descriptions of their purchase that could be incriminating.

Finally, forensic searches of seized computers suspected of conducting Bitcoin transactions should include wallet files, software, hash values and online exchange services. If you are investigating a Bitcoin transaction and have seized the suspect’s computer, your forensic examiner should search for Bitcoin wallet software, wallet files, visits to exchange sites or online wallets and any data sets that may be cryptographic keys to Bitcoin wallets.

C. Conclusion

Cryptocurrency should not be dismissed as inaccessible or enigmatic. A single bitcoin is simply a large number within the Bitcoin distribution network, and it is vulnerable to statistical analysis and good police work. The blockchain is a complete historical record of every Bitcoin transaction ever conducted. It is possible that every transaction will eventually be linked to an identified user. With the increasing credibility of, and cooperation from, bitcoin exchanges, an investigation into the virtual currency ecosystem can employ traditionally effective methods of capturing financial criminals: following the money.

NOTE: The author of the article would like to thank Regulatory Compliance Investigators Blake Ratliff and Dan Roseman of Coinbase for their technical assistance in reviewing this article.
1 The term Bitcoin is capitalized when describing the concept or protocol of the Bitcoin network. The term bitcoin is not capitalized when used to discuss the units of currency, although it is often abbreviated to BTC.
1 See e.g. https://sharedcoin.com/
1 http://blog/bitpay.com/2015/04/21/a-view-of-the-bitcoin-space.html
1 Hash value is a one-way mathematical re-creation of digital data in cryptography. It is used as a method of verification that two data sets are identical.
1 Nonce: a mathematical term for a number that only occurs once in a cryptographic system.
1 https://en.bitcoin.it/wiki/Controlled_supply
1 DDOS is a distributed denial of service attack in which the attacker floods the bandwidth of the victim’s system with incoming traffic, overloading the system, and causing it to crash.
1 http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228
1 Bitcoin includes a multi-signature feature allowing a transaction to require multiple independent approvals to be spent. Coinbase provides this multi-signature option for advanced users. https://www.coinbase.com/multisig
1 A QR code is a two-dimensional bar code readable by a cellphone camera.
See e.g. https://sharedcoin.com/


http://blog/bitpay.com/2015/04/21/a-view-of-the-bitcoin-space.html

Hash value is a one-way mathematical re-creation of digital data in cryptography. It is used as a method of verification that two data sets are identical.

Nonce: a mathematical term for a number that only occurs once in a cryptographic system.

https://en.bitcoin.it/wiki/Controlled_supply

DDOS is a distributed denial of service attack in which the attacker floods the bandwidth of the victim’s system with incoming traffic, overloading the system, and causing it to crash.

http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228


Bitcoin includes a multi-signature feature allowing a transaction to require multiple independent approvals to be spent. Coinbase provides this multi-signature option for advanced users. https://www.coinbase.com/multisig

A QR code is a two-dimensional bar code readable by a cellphone camera.