New Communication Technology Challenges for Law Enforcement

By: Sarah Kabli
Edited by: Robert Osgood

May 2013
Contents
Introduction .................................................................................................................................................. 2
Lawful Interception ....................................................................................................................................... 4
Bitcoin ........................................................................................................................................................... 6
   What is Bitcoin? ........................................................................................................................................ 6
   How is it used? ........................................................................................................................................ 10
   How else is it used? ................................................................................................................................. 11
   How can we intercept it? ........................................................................................................................ 13
BitTorrent .................................................................................................................................................... 16
   What is BitTorrent? ................................................................................................................................. 16
   How is it used? ........................................................................................................................................ 18
   How else is it used? ................................................................................................................................. 19
   How can we intercept it? ........................................................................................................................ 20
Skype ........................................................................................................................................................... 24
   What is Skype? ........................................................................................................................................ 24
   How is it used? ........................................................................................................................................ 25
   How else is it used? ................................................................................................................................. 26
   How can we intercept it? ........................................................................................................................ 27
Twitter ......................................................................................................................................................... 30
   What is Twitter? ...................................................................................................................................... 30
   How is it used? ........................................................................................................................................ 33
   How else is it used? ................................................................................................................................. 35
   How can we intercept it? ........................................................................................................................ 36
WhatsApp ................................................................................................................................................... 39
   What is WhatsApp? ................................................................................................................................ 39
   iMessage ................................................................................................................................................. 40
   How is it used? ........................................................................................................................................ 41
   How else is it used? ................................................................................................................................. 41
   How can we intercept it? ........................................................................................................................ 42
Conclusions ................................................................................................................................................. 45
References .................................................................................................................................................. 47
Introduction

Technology is advancing at an incredible rate, and the number of people using that technology is constantly on the rise. The number of people worldwide who have access to the Internet has grown over 566% from the year 2000 to the year 2012. Access to the Internet means having an incredible amount of resources right at your fingertips. Things that used to be done in person are moving more and more into the digital world. People keep in touch with old friends, send messages, buy clothes and food, play games, and start businesses all over the Internet. As with almost everything else, though, new technologies can be used for bad along with good.

Alongside seeing family from across oceans and keeping in touch with friends from elementary school, people have begun to use the internet for online stalking and bullying, sharing of copyrighted and contraband material, and finding victims for illegal activity that will be conducted both on and offline. Because of this, it is important to have a way to legally intercept communication sent over these new technologies to both catch bad guys and prevent crimes from happening.

The government has strict laws regarding interception. It is not as widely - or easily - done as television shows would like you to believe, but sometimes it is necessary. There are limitations on what, how, and how long a law enforcement officer may intercept a person’s communications that stop them from just tapping everyone’s phones and sniffing everyone’s Internet traffic. As technology advances, though, these are not the only obstacles they face. It is getting harder to keep up with new technologies. It is important to find ways to intercept online communication when the need arises. Finding new ways to intercept technology includes things that range from writing new laws, changing a company’s policy, developing and adapting technology, and everything in between.

While the computer forensics community has tried to develop tools and techniques to analyze computers and phones as they are being introduced, it is sometimes difficult to keep up with all of the new things being put out there. The computer forensics field is still growing, and compared to the number of people around the world that are constantly developing new programs and launching new technologies, it is almost miniscule. Just like with security, computer forensics is rarely one of the first priorities of a developer of a new technology. In some cases, the owners of the technology may actually actively try and hinder computer forensics, or take part in anti-forensics.

This paper will go into a few of the new technologies that are being used by today’s society, explain what they are, how they are meant to be used, how some people use them in ways that may require the interception of the communications, and possible ways that this communication can be
intercepted. It will also briefly discuss the idea of lawful interception and end with some concluding thoughts on new technologies and our society. The technologies covered here are: Bitcoin, BitTorrent, Twitter, Skype, and WhatsApp. These technologies cover a wide range of capabilities and purposes ranging from social media to online currency.
Lawful Interception

Lawful interception is the act of obtaining communications network data in accordance with lawful authority for analysis or collection of evidence. Intercepted data is generally signaling or network management information, but it can include the content of the communications as well. This is not frequently the case, though. If it is not collected in real-time, it is known as access to stored data.

Hollywood law enforcement agencies, where every crime is solved by the big dramatic breaks, have the benefit of “find all evidence” and “spy on all citizens” buttons. While extremely convenient, even if these buttons existed outside of a television screen, in most cases, law enforcement officers would not be allowed to use them. Though most people do not seem to realize this, there are several laws in place that restrict what and when a law enforcement officer can intercept communications.

The main federal statutes that apply to lawful interception are the Foreign Intelligence Surveillance Act, or FISA, which governs wiretapping of communications for intelligence purposes of foreign nationals or agents of a foreign power¹, and the Criminal Wire Tap Laws, or Title III, which includes the 1968 Omnibus Crime and Control Act. The Electronic Communications Privacy Act (ECPA) was an amendment to Title III and also dictates what information law enforcement can get. The laws go into great detail, giving exact definitions for everything from what “intercept” means to what constitutes as a “person.”

The laws state what is required to get what type of information and how long the intercept can last. For example, according to the Omnibus Crime and Control Act, a court order is needed for real time interception of communications. However, before a court order is given, law enforcement must show probable cause that a crime is being committed and that the device being intercepted is being used to commit the crime. Evidence for probable cause must be current, and all other techniques must have been tried first or shown that if tried, will fail. The interception can only go on for 30 days at most. The law enforcement agency must also write 10 day letters to the judge.

There are also laws in place, like the Communication and Law Enforcement Assistance Act (CALEA), which help with lawful interception from the other side. Instead of requirements on officers, they require organizations to assist law enforcement agencies in collecting evidence by providing tactical information. In the case of CALEA, it sets rules regarding how telecommunications providers must cooperate with law enforcement in the interception of electronic communications.

¹ Under U.S. federal law terrorist organizations are considered foreign powers for the purpose of FISA.
Another point to mention is that, while a government may get a warrant to intercept communications, it cannot prevent the communications from happening. For example, a government cannot block email or prevent a call from going through.
Bitcoin

What is Bitcoin?

Bitcoin is an excellent example of how technology can and does change the world. It completely does away with how money is conventionally exchanged and thought of, and makes everything about it digital. Bitcoin, which was developed in 2009, is based on open-source peer-to-peer (P2P) technology. It is basically an online decentralized bank. Personal computers are able to trade bitcoins internationally, without ever having to go through an intermediate financial institution. Each bitcoin can be divided down to eight decimal places. Bitcoin is related to BitTorrent, which will be discussed in more detail later in this paper. The “torrent” file in this case is a file with the currency’s entire transaction history stored in it.\(^2\) Bitcoins are sent and received through websites and apps aptly called wallets. To distinguish between the Bitcoin protocol, software, and the actual currency, the protocol will be capitalized (Bitcoin) and the currency will not be (bitcoin).

Bitcoin is the first decentralized electronic currency that is not controlled by any one organization or government. Instead, the network is made up entirely of users. Though people were suspicious of it when it first started, it is now being used by over 100,000 people worldwide. As of March 29, 2013, the monetary base of Bitcoin was valued at over $1 billion US dollars. Users can trade hundreds of dollars worth of bitcoins without ever having to go through a middle man or credit card company. Since these organizations that usually make a profit when money is spent are taken out of the equation, making transactions with Bitcoin is virtually free.\(^3\)

Bitcoin transactions are irreversible by design, and they are extremely fast. Once a transaction is made, bitcoins are available for spending within minutes. Transactions also cost significantly less than other payment networks. Bitcoin supply is regulated by software and the agreement of the users of the system. It cannot be manipulated by anyone, including governments, banks, organizations, or individuals.\(^4\)

Users can get bitcoins in several different ways. They can be “mined,” where “miners” set their computers to solve problems in exchange for bitcoins. The level of difficulty of the problems increases with the number of miners there are. This helps to create a stable rate of supply. A recent average for

\(^3\) [https://www.weusecoins.com/questions.php](https://www.weusecoins.com/questions.php)
\(^4\) [https://en.Bitcoin.it/wiki/Main_Page](https://en.Bitcoin.it/wiki/Main_Page)
bitcoin mining was $30 worth of bitcoins a day for a high-end machine. It takes a lot of energy to mine, and machines have been known to overheat in the process. The other way to get bitcoins is similar to the way you get traditional money: trading goods or services. People have traded things ranging from hacking techniques to alpaca socks in exchange for bitcoins. Cash can also be traded in for bitcoins. Mt. Gox is the largest Bitcoin exchange. It charges 0.65% per transaction to connect buyers with sellers. In March 2013, a bitcoin cost between $40 and $95.

Bitcoin exchanges are services that allow users to buy and sell bitcoins for traditional currencies. Mt. Gox is not only the largest exchange but also the oldest. Launched in 2010, it was handling 80% of the bitcoin exchanges worldwide in 2011. It accepts cash deposits, wire transfers, and online payment services like Dwolla. PayPal does not allow its users to purchase electronic currency with its service. Other popular exchanges are Bitcoinary, AurumXchange, and Bitcoin-24. BitInstant allows users to buy bitcoins from large physical stores like Walmart, 7-11, and CVS. The user would order the coins online, print out a receipt, and pay for them at the store. When purchased this way, coins take around an hour to be delivered to the user’s wallet.

In the “real world” there is a central authority that controls the money supply. In most countries, governments secure and control their national currency. In Bitcoin, this work is divided among all of the users, but most of the work is done by the miners. Miners collect the transactions on the network into large bundles, or blocks. The blocks are concatenated and made into one continuous, authoritative record. This record is called the block chain. Because all of the previous transactions are stored in the block chain, users cannot spend the same bitcoin twice, or sign the same bitcoin over to two different addresses. This prevents someone from spending more than they have and ensures that a bitcoin transaction won’t bounce like a bad check.

To ensure that multiple block chains are not made for the same bitcoin, Bitcoin makes the producing of blocks very difficult. To make a block, miners have to compute a cryptographic hash of the block that meets certain criteria. Users of Bitcoin refer to this process as “hashing,” and the hash is sometimes called the proof-of-work. Finding an acceptable hash is not as easy as it sounds, and a miner has to try several times before getting lucky and finding one that works. This process is referred to as the “lottery” since miners that successfully create a block are rewarded with bitcoins. As mentioned above, the criteria for the hash are adjusted based on mining activity. The more miners there are, the harder it is to compute. Miners use specialized hardware to find hashes, otherwise they would be

spending more on time and electricity than they make back in the lottery. Once a hash is found, the block is broadcast back to the network.

Hash criteria are not the only thing a miner has to worry about when mining, though. In order to get rewarded for their work, the block chain can only contain valid, non-conflicting transactions. This means that along with finding an acceptable hash, miners have to carefully validate all of the transactions that go into their block. The amount of work that goes into the making of block chains is what makes the network so secure. The block chain that was the most difficult to produce was the one that was being worked on by the most miners and is therefore the most trustworthy. If a person tries to fake a block chain to keep money that they have spent, they will need to put in as much work as all of the other miners on the network combined to make their chain look trustworthy. This is improbable, though there is code to choose between two conflicting blocks just in case.7 Every time a transaction record is confirmed, the ones before it are made more permanent. After six confirmed records, and at 10 minutes per confirmation this tends to take about an hour, a transaction is usually considered confirmed beyond reasonable doubt.

The money supply, which has a 21 million bitcoin limit that was hard-wired into the protocol, is automated and given to servers or miners that confirm transactions as they are added to the decentralized and archived transaction log every ten minutes. The log is authenticated by end-users through digital signatures and confirmed by hashing. Because of the limit on bitcoins, the reward for creating a new block is halved every 210,000 blocks which is estimated to be every four years. It started with a 50 bitcoin reward per block. As of 2012, the reward was at 25 bitcoins. It is estimated that in the year 2017, the reward will be halved again to 12.5 bitcoins, and the currency is estimated to reach its limit around the year 2140.8

Payments are made to Bitcoin addresses which are based on digital signatures and public keys. The addresses are alphanumeric, human readable strings around 36 characters long. Addresses always start with either a 1 or a 3. Users get new addresses as necessary. The idea behind having multiple addresses is that it provides a loose type of privacy for transactions. Bitcoin transactions are inherently public since they are broadcast to the entire network for miners to use them in the making of new blocks. The addresses are stored in a wallet file with links to the private keys that allow for the access and transfer of bitcoins. Wallets are usually encrypted with an additional password for added security.

7 https://www.weusecoins.com/questions.php
The following is a visual depiction of how a bitcoin is created and used.

While Bitcoin sounds like the perfect currency, there are still some drawbacks to using it. Though the popularity of bitcoins has risen since their introduction, they are still not widely accepted. This means that people cannot rely on bitcoins as their only currency. Contributing to this is also the fact that most people still have to go to physical stores, where bitcoins are not accepted. Another potential drawback is that since everything is digital in the Bitcoin world, money can be lost quickly and forever. If a hard drive crashes or a virus corrupts the wallet file, bitcoins can be lost, and there is nothing to do to recover them. A bitcoin user could become bankrupt in a matter of seconds, and all of his or her bitcoins will be permanently orphaned in the system. Because the value of bitcoins fluctuate significantly according to demand, it may be hard for users to know exactly how much they have and what things are really worth. If a shirt is valued at 1 bitcoin, should it matter whether a bitcoin is worth ten or one hundred US dollars?
Because of the way Bitcoin transactions are secured, users have no buyer protection. If they sign bitcoins over for a product, the transaction is permanent. If the seller does not send the product, there is really nothing that the buyer can do. Third party escrow services, like ClearCoin, have popped up to try and help in this regard, but some people strongly oppose them. They would essentially be taking on the role of banks which would make Bitcoin similar to traditional currencies, undermining the main point for it altogether. Some people are worried about the fact that, with a built in limit of bitcoins, Bitcoin has built deflation into their system. As the number of bitcoins available maxes out, they will become more and more valuable. This could lead to spending surges and unpredictable fluctuations in the Bitcoin economy. The very nature of what makes Bitcoin so alluring, the lack of a central authority, could also be its potential downfall. Without that authority to govern bitcoins, its minimum value cannot be guaranteed. If all of the large Bitcoin merchants decide to stop accepting bitcoins, their value would decrease quickly and significantly, potentially hurting users that have invested most of their wealth in the system.\(^9\) The largest Bitcoin merchants may not be the largest merchants outside of their network. As of February 26, 2013, the top five bitcoin merchants were Wordpress, Reddit, Internet Archive, 4chan, and Namecheap. All of these fall within the top 1,000 sites visited worldwide, with Wordpress being the 22\(^{nd}\) most visited site and Namecheap being the 891\(^{st}\) most visited site.\(^{10}\)

A major advantage of bitcoins though, despite the listed drawbacks, is that bitcoins are nearly impossible to steal. The ownership address of a bitcoin can only be changed by the owner. Another user cannot steal a bitcoin without physical access to the victim’s computer. This makes it a lot harder than stealing “real world” currency which only requires the knowledge of some authentication details.\(^{11}\)

How is it used?

Nicolas Christin, the associate director of Carnegie Mellon University’s Information Networking Institute, declared his view that Bitcoin has moved beyond just being a fun online thing to becoming a real and respected currency.\(^{12}\) Bitcoins are used for the same things as any other currency is used for. Online commerce is their most obvious use, but certainly not the only one. Exante Ltd., an investment

firm based in Malta, has launched a bitcoin hedge fund marketed towards institutional investors and high net-worth individuals. The Bitcoin shares are currently traded through the Exante Hedge Fund Marketplace platform and regulated by the Malta Financial Services Authority. As of March 2013, the firm holds over $3.2 million in bitcoin assets.13

Bitcoins are used for several types of legitimate transactions. For example, Reddit, the popular social news and entertainment website, allows its users to upgrade services using bitcoins. Wordpress, the blogging platform, accepts bitcoins as a form of payment in their store. There are also sites that allow you to use bitcoins for transactions with companies that may not accept them on their own. For example, pizzaforcoins.com allows bitcoin users to pay for pizza deliveries with bitcoins instead of traditional cash.14

Some people like to use bitcoins to buy things online because they do not give up as much personal information as paying with your credit card would. Though not all stores accept bitcoins, you can find stores that do that sell practically everything. Stores that do accept bitcoins sell the following types of products: gift cards, precious metals and coins, clothing and accessories, toys and games, video games, home and garden products, office supplies, exercise and recreational products, pet supplies, artwork and craft supplies, photography supplies, electronics, automotive products, musical instruments, real estate, food, books, educational materials, music, web hosting, and digital downloads.

How else is it used?

Bitcoin can also be used in ways that may not be exactly legal. Despite the fact that transactions are broadcast to the entire network and block chains include the addresses for participants in a transaction, Bitcoin transactions are still relatively anonymous. Though it is possible to connect a real-life identity to a Bitcoin address with enough external information, it is usually very difficult to do. Users of Bitcoin have taken advantage of this fact to abuse the system.

The Silk Road, an online black market, uses bitcoins as the medium of exchange. Only accessible through Tor, an anonymous network, the site is a lot like an underground eBay. One of the biggest differences between the two sites is that instead of electronics being the highest selling item, the Silk

13 http://www.reuters.com/article/2012/04/01/traders-bitcoin-idUSL6E8ET5K620120401
Road’s high seller is drugs. People feel comfortable buying drugs online because of the anonymization provided to them by both Tor and Bitcoin.\footnote{http://www.theatlantic.com/technology/archive/2011/06/libertarian-dream-a-site-where-you-buy-drugs-with-digital-dollars/239776/}

In June 2011, Symantec warned that it was only a matter of time before people started using botnets to engage in covert mining of bitcoins. They also warned of the fact that some malware could use the parallel processing capabilities of GPUs that are built into modern video cards to take part in bitcoin mining. Employees have been caught using their company’s servers for these exact reasons. Though not necessarily illegal uses of Bitcoin itself, these are direct results of the allure of mining and getting data blocks first to win the lottery.

Stealing bitcoins from individuals is extremely difficult, but it gets a little easier to steal them from bitcoin exchanges. This has happened multiple times since Bitcoin’s initial launch. For example, on June 19, 2011, there was a security breach of the Mt. Gox bitcoin exchange. A hacker was able to use credentials from an auditor’s compromised computer to illegally transfer a large number of bitcoins to himself.\footnote{https://mtgox.com/press_release_20110630.html} In August 2011, MyBitcoin, a bitcoin transaction processor, was hacked. It had to be shut down and could only pay 49% on customer deposits, leaving over 78,000 bitcoins unaccounted for.\footnote{http://betabeat.com/2011/08/mybitcoin-spokesman-finally-comes-forward-what-did-you-think-we-did-after-the-hack-we-got-shiftaced/}

Bitcoinica, a bitcoin trading venue, was hacked twice in 2012. In September 2012, Bitfloor, another bitcoin exchange, also reported being hacked. During this hack, 24,000 bitcoins were stolen.\footnote{http://www.bbc.co.uk/news/technology-19486695}

There have also been allegations that bitcoins were used in a Ponzi scheme, which is a fraudulent investment operation where investors are not getting paid returns from profit and are instead being paid from the owner’s pocket or from money taken from subsequent investors. New investors are enticed into investing because of the high returns promised. In August 2012, Bitcoin Savings and Trust was shut down by its owner. It allegedly left behind $5.6 million in unpaid bitcoin debts. There were cries that the operation was a Ponzi scheme, and the US Securities and Exchange Commission started investigating the case in September 2012.\footnote{http://www.dailytech.com/Pirateat40+Makes+Off+56M+USD+in+BitCoins+From+Pyramid+Scheme/article25538.htm}

Bitcoin can also be used for money laundering. There are bitcoin “mixers,” like Bit Laundry, that will exchange bitcoins and cash for “clean” bitcoins. The mixers usually take a 1% transaction fee for the service. Once a transaction is made, a user can easily liquidate the account and open a new one at any

\footnote{https://mtgox.com/press_release_20110630.html}
\footnote{http://www.bbc.co.uk/news/technology-19486695}
\footnote{http://www.dailytech.com/Pirateat40+Makes+Off+56M+USD+in+BitCoins+From+Pyramid+Scheme/article25538.htm}
time. This allows them to remain as incognito as possible to stay out of the law’s crosshairs. Moving large amounts of money through credit card payments and bank transactions the traditional way leaves a paper trail which is monitored by government regulators.

There are many reasons why someone would not want a payment being linked back to them. Though some of them may be legitimate and completely legal, a lot of them are not. For example, Internet gambling and child pornography are two places where people spend money online that they would not like to be traced back to them. Terrorists buying weapons and human traffickers may also view Bitcoin as the perfect answer to one of their biggest problems: getting caught.

How can we intercept it?

As it is now, transactions on Bitcoin are almost impossible to intercept with any meaning. Though transactions themselves can be intercepted easily since they are broadcast to the network, not knowing who each Bitcoin address belongs to makes the information almost useless. To rectify this situation, there would have to be changes made to both laws and Bitcoin itself.

In March 2013, the Wall Street Journal announced that the US government will start to apply money-laundering rules to online currencies, like Bitcoin. This means that bitcoins will begin to be regulated like traditional money to help prevent people from using it for illicit acts. The rules require there to be bookkeeping and mandatory reporting of transactions over $10,000. This is a good step in the right direction, though some conspiracy theorists claim that it is just a ploy to get people to use US dollars instead of any other currency. They claim that what the FBI is doing is making it seem like every transaction is borderline illegal to spook Bitcoin’s users into returning to the dollar. Since the fact that it is not feasible to have bitcoins as a person’s only currency has already been covered, their arguments seem a little far-fetched. Some firms, though, like BitInstant, a bitcoin processor, were expecting the rules eventually. BitInstant’s CEO Charlie Sherm says that his company is already compliant.20

While implementing rules and laws is helpful, if a law enforcement official cannot trace a Bitcoin address to a specific person, they are not of much use. Some third party bitcoin exchanges require users to register with valid documentation to convert between bitcoins and traditional money, ultimately pinning an address to a real person. Users who register with those are traceable. Since IP addresses are published along with the transaction, law enforcement may be able to trace a user back through that

information provided that the user was not using a proxy. They shouldn’t have to rely on hoping that those conditions are met, though. It should be a requirement for users to verify themselves before they start using the currency. These authorization details should still be kept hidden from the rest of the network to ensure some form of privacy when transactions are being broadcast, but they should be stored somewhere in case law enforcement needs them.

Although this inserts a form of centralized management into Bitcoin, tweaking the technology, it is centralizing the users rather than the actual money. Bitcoin exchanges that require and store personal information about a user are already being widely used. Most people do not feel that this takes away from the bitcoin experience. Rather, it gives them a sense of security. This adjustment to the protocol would make sure that all of the users do this.

There is an ongoing battle between ensuring security and privacy and ensuring law enforcement’s ability to get the information they need. Having a centralized system that manages Bitcoin users introduces security vulnerability. Bitcoin will need to make sure that users’ personal information remains secure and private. The best way to maintain this security and privacy is not to actually store the information anywhere. This, as previously mentioned, makes law enforcement’s work nearly impossible. A good balance needs to be found between the two.

The connecting of an address to a person creates some similarity to services like PayPal. Building off of those similarities, certain investigative tools that are available for eBay and PayPal could be made available for Bitcoin. For example, law enforcement should be able to get a list of transactions made with a certain Bitcoin address, whether money was going to or from the wallet, over a period of 30 days. eBay requires law enforcement officers to provide them with the name, email address, and eBay username to locate the account. Depending on what personal information is required to authorize a Bitcoin user, law enforcement should be required to have multiple pieces of information before being granted access to records. PayPal keeps all of its records indefinitely. eBay keeps its account records indefinitely and its transaction records for two years. Transaction records are kept in the block chain of Bitcoins. That does not need to be changed. However, a record should be kept of the different addresses a person creates and deletes. This way, if a person gets a Bitcoin address, participates in money laundering, liquidates and closes his or her account, they can still be traced.

Another thing to take into consideration would be the difference between users and Bitcoin addresses. Since each user could have multiple addresses, while getting a warrant, should it be for the

---

21 [https://www.eff.org/sites/default/files/filenode/social_network/EBay_Paypal_SN_LEG_Airforce.pdf](https://www.eff.org/sites/default/files/filenode/social_network/EBay_Paypal_SN_LEG_Airforce.pdf)
actual user or for the address? When possible, warrants should state both the user and the specific Bitcoin addresses that should be intercepted.

Bitcoin may be changing on its own, though. In Europe, Bit-Coin Central, a Bitcoin exchange, teamed up with Aqobo, a payment service provider in France, to keep funds on behalf of third-parties in payment accounts. It is not a bank since it cannot invest the bitcoins it holds, but it does perform bank-like functions. This may be the first step in centralizing Bitcoin a little.22

Though people have taken to the Internet to shout that making any changes to Bitcoin will ultimately be its downfall, I don’t think that that’s the case. Though the allure of the currency may be lost to some, it will become a lot more popular with others. A lot of everyday people and legitimate merchants around the world have avoided Bitcoin. Its lack of regulation and association with criminals, money launderers, and drug dealers had them keeping their distance. If it does become subjected to laws and potential government regulation, though it may lose the patronage of people who used it to stay in the shadows, it will gain many more legitimate users.

BitTorrent

What is BitTorrent?

The word BitTorrent is used to describe both a peer-to-peer (P2P) file sharing protocol and the official BitTorrent client released by BitTorrent, Inc. The protocol was developed by Bram Cohen in April 2001, and made available to the public on July 2, 2001. It is a very popular protocol, and offers a layer of anonymity for its users. BitTorrent, Inc. reportedly had 150 million active users as of January 2012. Taking into account the number of BitTorrent clients available, the number of people using the protocol is closer to a quarter of a billion.

BitTorrent works to make file sharing both fast and efficient. To do this, the protocol breaks a file up into smaller pieces. The file is downloaded in separate pieces, which can come from multiple sources. This allows for fast downloading without using much bandwidth. When a person wants to upload a file for others to download, they make it into a torrent. Other users, or peers, can then start to download the pieces. As a file is downloaded, it immediately starts to upload the pieces again for others to download. This allows for faster downloads for others. It also means that once a person’s torrent is downloaded, it remains available even if the original uploader removes it.

There are certain words that are often used in relation with BitTorrent that should be explained in order to fully understand the protocol. First, a torrent is a file that describes which files are being shared, where to find the parts to download, and information about the computer that coordinates the distribution. The instance of a file being distributed via BitTorrent is commonly known as a torrent. A client is the BitTorrent software that is used to share the files. A peer is one of a group of clients that are downloading the same file, and a seeder is the peer that is making the file available to others to be downloaded. A seed is a complete copy of the file that is available for download as opposed to just pieces of it, which are referred to as blocks. Blocks are generally 250kb, but this size can vary depending on the file. If all of the seeds are unavailable, a peer may only be able to download parts of a file. If this happens, someone can put up the complete file again for others to download from. This is known as re-seeding. Availability refers to the number of copies that are available for downloading. The higher the availability, the more likely it will be for the file to be downloaded quickly. A number less than one

23 http://finance.groups.yahoo.com/group/decentralization/message/3160
24 http://www.bittorrent.com/intl/es/company/about/ces_2012_150m_users
25 http://www.bittorrent.com/help/faq/concepts
means that there is no longer a complete file available for download, only parts. Once a file is finished downloading, the user can choose to stop it uploading and make it unavailable for others to download from. People who download lots of files and choose not to upload any are known as leechers. A swarm is a group of seeds and peers that are all sharing the same file, and a tracker is a server that keeps track of everyone in a swarm. Trackers do not have copies of the file being shared by the swarm.26

To describe the way the protocol works using this vocabulary, a file is broken into blocks and made into a torrent file, which includes information about the original file and where to download the blocks from, among other things. A seeder uploads the seed, or torrent file, to be downloaded by peers. As the peers download blocks, they in turn become seeders for those blocks. The swarm of peers and seeders is tracked by a tracker. Once a peer gets the entire file, s/he has the option to continue to make the file available to others or to stop seeding. To stop seeding, the peer would pause the torrent or remove it from their queue. If all of the seeders stop uploading blocks, some peers may be left with only partial files. If this happens, someone may choose to make their seed available again which is known as re-seeding.

As was mentioned earlier, BitTorrent has become an exceedingly popular way to share files over the Internet. Like other technology, it is more popular in some parts of the world than it is in others. With stricter laws regarding file sharing in the US, BitTorrent is beginning to see a decline in users. As of May 2012, BitTorrent made up 20.32% of all Internet traffic in peak hours in Europe. eDonkey, another file sharing client, brought the percentage up to 29.71%. While BitTorrent’s Internet share in the US is declining, it is still accountable for 11.3% of traffic during peak hours. P2P traffic in general accounts for 12.7% in the US.27

BitTorrent was designed for file sharing. In order to maintain a good reputation with its users, it has to ensure that the files being shared are actually what they say they are. To do this, the blocks of a file are hashed and compared with a valid hash of the block. A hash is an alphanumeric string of data that is derived from a file that is run through an algorithm. Any changes made to the data will change the hash. BitTorrent will automatically ban a peer after 5 hash fails. By doing this, they are helping to ensure the integrity of the files being downloaded.28

26 http://www.bittorrent.com/help/faq/concepts
28 http://www.bittorrent.com/help/faq/client
How is it used?

BitTorrent is used for many legitimate purposes. BitTorrent, Inc. obtained licenses from Hollywood studios to allow them to distribute some content from their websites. Bands, like Nine Inch Nails and The Libertines, and music record labels, like Sub Pop Records, have released demos, albums, tracks, and videos via BitTorrent. BitTorrent is also being integrated into some of the podcasting software, giving podcasters a way to deal with high download demands of their podcasts, or MP3 radio shows. DGMLive, a way for musicians and their fans to share music, diaries, photographs, and commentary, is another program that utilizes BitTorrent. A user could make a purchase from DGMLive and then download the song or video through a BitTorrent client.29

Broadcasters also use BitTorrent to share their media. The first time a full show was made available for download by the broadcasting company with BitTorrent in North America was in 2008. CBC released Canada’s Next Great Prime Minister through the file sharing client. NRK, the Norwegian Broadcasting Company, has been releasing selected material through BitTorrent since 2008 as well.30 VPRO, a Dutch broadcasting company, has also distributed four documentaries under a Creative Commons license.

Along with music and movies being distributed by their creators, BitTorrent can be used to share personal material. Amazon S3, which gives users online storage capabilities, has built-in BitTorrent support to aid with the transfer of user files. There are also programs, like Blog Torrent, that provide easy ways for non-technical bloggers to host different applications on their site. For example, Blog Torrent allows visitors to a certain blog to download a stub loader. This acts as a BitTorrent client and allows them to download torrents the blogger is offering without having to get a BitTorrent client first.31

Some companies also distribute software by using the BitTorrent protocol. For example, World of Warcraft, along with extra content and patches for the game, is available through Blizzard Entertainment’s proprietary BitTorrent client, Blizzard Downloader.32 This allows purchasers of the game to download it as quickly and efficiently as possible. Other computer game developers have started to mimic Blizzard Entertainment and are beginning to make launchers based on BitTorrent. There are quite a few open source software projects that have a torrent option for downloads as well as the

29 http://www.dgmlive.com/help.htm#whatisbittorrent
30 http://nrkbeta.no/bittorrent/ (translated)
31 http://grep.law.harvard.edu/articles/04/08/26/0236209.shtml
32 http://www.wowpedia.org/Blizzard_Downloader
conventional methods. This helps them to reduce the load on their servers as well as increase the number of people their software is available to.

The number, and type, of people that use BitTorrent is truly varied. The UK government has distributed information about how tax money was spent with BitTorrent. Florida State University uses it to provide researchers with large scientific data sets. Popular websites, like Facebook and Twitter, distribute updates to their servers with BitTorrent.

How else is it used?

With the benefits that BitTorrent provides in file transfers, it is not surprising that so many people use it for so many different things. It is also not surprising, then, that some of these ways are not as reputable as others. With the ability to share almost anything, and share it quickly and for free, it didn’t take long for people to start abusing the privilege.

The biggest legal issue facing BitTorrent is the sharing of copyrighted material, or online piracy. As of 2011, 22% of global Internet traffic was used for online piracy. 98.8% of all files being transferred through peer-to-peer networks were copyrighted. This means that only 1 out of every 10,000 blocks of data being transferred with BitTorrent was not copyrighted. In fact, 42% of all the software running in the world as of 2011 was illegally downloaded. Over 75% of computers around the world have at least 1 illegally downloaded program. What may possibly be one of the most shocking statistics, though, is that 70% of online users find nothing wrong with piracy.

When something is available for free online, should you have to pay for it? It’s surprising that so many people said no. Sharing files over the Internet gives people enough distance to forget that there is really no difference between an online copy of a movie and its tangible counterpart. If they properly equated the two, there would be a drastic drop in the number of people that thought online piracy was okay.

Copyrighted media are not the only illegal files being transferred with BitTorrent, though. Child pornography, which is contraband in the US and most parts of the world, is also being shared. BitTorrent

33 http://www.ubuntu.com/download/desktop/alternative-downloads#bt
35 http://www.hpc.fsu.edu/index.php?option=com_wrapper&view=wrapper&Itemid=80
37 http://torrentfreak.com/twitter-uses-bittorrent-for-server-deployment-100210/
38 http://www.go-gulf.com/blog/online-piracy/
allows child pornographers to quickly share their material and others to easily download it. In a study done on BitTorrent activity through MiniNova, a BitTorrent client, over the course of 67 days, over 99,639 keywords related to child pornography were searched for.\(^{39}\)

If most of the files being shared over BitTorrent are illegal, then why are all BitTorrent clients not being shut down? This is a very controversial issue. There are arguments made that, since the BitTorrent trackers never store any files – copyrighted or not – BitTorrent is not actually engaging in online piracy, even if the metafiles of the trackers link to copyrighted material without the owner’s consent. Quite a few BitTorrent clients have been shut down because of copyright infringement. The most notable of these are Supernova, TorrentSpy, MiniNova, and The Pirate Bay. Users of the sites are not getting away with online piracy, either. 200,000 people were sued for uploading or downloading copyrighted material in the two year span of 2010 to 2012.\(^{40}\)

This does not seem to be scaring people into compliance with the law enough, though. 2011 saw a 20% increase in the number of illegal shared files online. In North America that year, 61% of files uploaded to the Internet consisted of pirated movies, music, television, games, software, and books.\(^{41}\)

Along with pirated material and child pornography, studies have shown that BitTorrent is used to distribute malware. In a 2008 study by Andrew Berns, it was found that 18% of executable files available for download through BitTorrent clients contained malware.\(^{42}\) A later study done by Finn Michael Halvorsen and Rune Walso Nergard claimed that up to 14.5% percent torrent downloads contain zero-day malware, and that 47% of zero-day malware was distributed with BitTorrent. With statistics like these, it is no wonder that law enforcement would want to intercept BitTorrent traffic.

How can we intercept it?

Because of the way that peer-to-peer networks break up files and send each piece along a different path, stopping the sharing of these files is more difficult than it would be if one person was just emailing something to someone else. It would be a lot easier if the files had to pass through some centralized servers.

Engineers at the Oak Ridge National Laboratory in Tennessee have developed new software designed to automate the tracking of torrents that may help law enforcement to intercept BitTorrent traffic.

---


\(^{40}\) [http://www.pcworld.com/article/237593/copyright_trolls_200_000_bittorrent_users_sued_since_2010.html](http://www.pcworld.com/article/237593/copyright_trolls_200_000_bittorrent_users_sued_since_2010.html)


traffic. The trick to their software is focusing on new files coming out of RSS feeds and entering P2P networks before they have a chance to get widely distributed. The more times a file is downloaded, the more widely distributed the contents of the file are, making it much more difficult to track. If they can get the file before this happens, law enforcement has a better chance of tracking down suspects. Their software will immediately grab the torrent file and investigate the IP addresses of the different computers the pieces of the file come from. The software then prioritizes which IP addresses should be investigated based on data-traffic patterns and creates a short list for the police.43

Filters can be used to flag inappropriate content, whether it is copyrighted material or child pornography or something else altogether. Some BitTorrent clients have agreed to partner up with law enforcement to at least stop child pornography from spreading. The client isoHunt was the first foreign website to partner with New York Attorney General Cuomo to try and get child pornography off of the Internet. The site will use the Attorney General’s hash value database to filter its search results and prevent known child pornography images from spreading. Along with hashes, names and file sizes of content files are given. With the three pieces of metadata, isoHunt can build a database for automated takedown of known contraband files. IsoHunt said that if people would provide this same metadata for files they have copyrights to, they could build a similar database to target copyright infringement on their site.44

While this might help prevent illegal files from being shared on the Internet, it does not necessarily make it any easier for law enforcement to intercept BitTorrent traffic. One suggestion would be to have users register to use BitTorrent. This way, it may be easier to track activity back to a specific user. Before a user can download a BitTorrent client to share files, they will have to create an account. Of course, this would not help with sites that use stub loaders since users can download files without downloading a BitTorrent client.

Another technology that can be looked into for methods to intercept BitTorrent traffic is the MarkMonitor AntiPiracy platform which is used for the Copyright Alert System (CAS). The CAS is a private system used by AT&T, Cablevision, Time Warner, Verizon, and Comcast that alerts and punishes internet subscribers that are sharing copyrighted material through BitTorrent. It is known as the six strikes program because users get six warnings, starting from a cautionary email and moving forward to forcing the user to watch videos about copyright infringement before s/he is able to access the internet.

43 http://www.scientificamerican.com/article.cfm?id=software-against-p2p-bittorrent-abuse
44 http://torrentfreak.com/isohunt-partners-us-attorney-general-to-ban-child-porn-100630/
After the six warnings, more severe punishment, like bandwidth throttling, is seen. The ISPs do not alert the government to the copyright infringement, though. The CAS was implemented in February 2013.45

The MarkMonitor AntiPiracy platform consists of an enterprise client-server environment that scans P2P networks and websites to collect and preserve evidence. It includes scanning systems, multiple databases, collection mechanisms, and configuration systems. MarkMonitor personnel search for potentially offending files and add the results to a database that captures metadata about each file to identify infringing files. The metadata includes the file name, hash value, and size. This is the same data that is used in Attorney General Cuomo’s database to stop the spreading of child pornography.

Using either an automated fingerprinting technology or by reviewing the files manually, it is determined whether they are actually illegal copies of copyrighted material or not. The database is then updated to indicate that the file is confirmed copyright infringement. At the same time, the confirmed infringing searches and torrents are sent to the platform’s collection mechanisms, which are custom-built software that run on servers in geographically spread datacenters. The collection mechanisms search for, download parts of, and create evidence packages of infringing works. The evidence packages include information like IP address, port, time and date, PeerID, and hash values. Scripts are then run to verify the collected evidence. Once evidence is verified, infringement notices are generated and sent to the appropriate ISP.

The following will describe what MarkMonitor does in a little more detail. First, Content Owner Representatives give lists of copyrighted material they want monitored to MarkMonitor. Infringing online versions of the titles are found and verified. MarkMonitor uses a distributed network of servers equipped with custom designed scanning and collection software. The software collects information from P2P networks and websites by integrating and functioning on P2P networks as a standard peer. It communicates with and downloads data from other peers like a standard P2P client. Because of this, it is able to access the data without being thwarted by BitTorrent encryption. The software goes beyond what a standard P2P client does, however, and documents user activity and generates evidence collections complete with relevant supporting information. It also only downloads a portion of a file from each peer. The portions are verified by hashes, and if it is determined to be part of a copyrighted file, the download is stopped. This minimizes the required amount of storage space and increases efficiency as the software is able to target more peers than it would otherwise be able to.

The evidence packages that are generated with this platform follow forensic data collection practices. It generates audit trails, provides robust documentation, uses hash verification, and is

repeatable. Along with collection portions of infringing material, XML-formatted log files, both activity and communication logs, are also obtained with case specific information, a packet capture (PCAP) file, and an html report including several pieces of key information. The evidence package also includes a traceroute of the user’s IP address in connection with a reverse DNS lookup of all devices encountered. This gives the IP address, ISP, and geographic location of the peer taking part in the sharing of the copyrighted material. The PCAP file allows for the entire communication session between the software and peer to be reviewed. The evidence package is verified again by checking that the IP address is active and sharing a file, the IP address is detected as having a P2P client, and that the hash reported by the peer matches a hash in MarkMonitor’s database of confirmed infringing files.46

This system can be adapted to support lawful interception of BitTorrent traffic. It already implements several recommended practices of computer forensics. The repeatability of the system will make it a tool that, once peer reviewed, can be supported well in court.

It would also be helpful to have a law that requires BitTorrent to make their data accessible to law enforcement when they need it. To do this, there could be centralized nodes on the network where the packets should pass through. Traffic could be intercepted at these points. The traffic could also be intercepted at the tracker. Although the tracker does not contain the actual file, it does contain information on who is sharing the file with whom and where the file is located. The IP addresses obtained from trackers could lead to further investigations.

Skype

What is Skype?

Skype is a Voice over IP (VoIP) service and software application that was released in 2003. As of 2011, when it was bought by Microsoft for $8.5 billion, it had gained over 600 million users. Microsoft is even retiring its own Windows Live Messenger and promoting Skype as its messaging service beginning in April 2013. Skype users can communicate in three different ways: by voice with a microphone, by video with a webcam, and by instant messaging. Skype can also place calls to recipients on traditional phone networks, and SkypeIn allows traditional phones to call Skype accounts in some countries. However, since the US Federal Communication Commission (FCC) ruled that Skype is not an interconnected VoIP provider, emergency calls cannot be made from Skype. Skype to Skype calls are free, but Skype calls to and from traditional phone line are not. Users are offered features like file transfer and videoconferencing of up to 10 people. Conference calls of up to 25 people are also supported.

Skype is not like every other VoIP service around, though. It is a combination of peer-to-peer and client-server systems and makes use of the background processing on computers that are running it. Skype protocol is the proprietary VoIP network Skype uses. Unlike a lot of the other technologies discussed in this paper, it is not open source. It operates on a peer-to-peer model originally based on the Kazaa software, which the developers of Skype also founded. The instant messaging aspect of Skype has similar functionalities to other instant messaging services, like group chats, the option to store chat history, user profiles, and online status indicators.

Users that register with Skype create a unique username, or Skype Name, that can be listed in the Skype directory, which is like a virtual phone book of Skype users. Like other communication platforms that have popped up over the past few years, Skype does not verify that a user is who s/he says s/he is. When registering for Skype, there is nothing stopping a user from putting in a fake name to hide his or her identity.

This brings up the controversial topic of whether or not anonymous communication should be prohibited by law. Similar to the argument over security that was touched on earlier in this paper,

47 http://www.bbc.co.uk/news/business-13343600
48 http://www.access-board.gov/sec508/refresh/teitac8th/itf-report.htm
50 http://www.skype.com/en/features/
anonymous communications toe the line between increasing user privacy and making it more difficult for law enforcement officers to retrieve data they may need from internet communications. People have argued both sides of the debate, but it does not look like we are any nearer to reaching a decision about its legality. In my opinion, traceable pseudo-anonymity is a good balance between the two.

Skype’s popularity is still increasing. In 2005, Skype had 2.9% of the international call market share. This went up to 34% in 2012.\(^51\) Along with their software that can be downloaded onto computers, Skype also has apps that can be downloaded for smartphones. As of June, 2012, the Skype app for Android had over 70 million downloads.\(^52\)

Skype takes security seriously. Encryption, which is invisible to the user, cannot be disabled, thereby helping to make the conversations secure. It uses RSA encryption for key negotiating and AES to encrypt the conversations, both of which are widely accepted encryption methods.\(^53\) There are several claims that the service is not as secure as they would like us to believe. Some people are worried that using proprietary software and protocols could lead to security vulnerabilities and privacy issues. Others have speculated that the reason Skype tries so hard to obfuscate its traffic and the functioning of its program is because it has a backdoor.\(^54\) Unlike with open source programs, the users cannot see what is going on behind the scenes. In a society where transparency is becoming more and more valued, this is viewed with some suspicion.

How is it used?

Skype is used for a myriad of different things. To start with the obvious, Skype, like other communication services, is used to keep people together. Its VoIP services allow users a free alternative to long distance phone calls, letting them get in touch more often than if they had to pay for every minute. It goes beyond that, though, with its video capabilities. With a sister living overseas, it has been great to be able to watch my nephews grow up, have them show me their artwork after a day at school, and be able to feel like we are still in each other’s lives despite being half a world away from each other.

On their website, Skype claims that “you can share a story, celebrate a birthday, learn a language, hold a meeting, work with colleagues – just about anything you need to do together every day.”

Skype is being widely used in education. Students around the world are being paired off with native speakers of a language that they wish to learn. By having conversation in the two languages, each student becomes more fluent in the one they wish to learn. Skype has also been used to hold virtual field trips, allowing students to experience a place they may never get a chance to see otherwise. Skype in the classroom is a free tool that Skype offers on their website. Teachers can sign up and let their students meet other students, participate in Skype lessons, and find experts in many different fields to talk about their careers.

Skype is also used in businesses. It offers small-business-oriented products that allow small businesses to enjoy call service options typically reserved for big companies. These include Skype Manager, which has features including, but not limited to, customizable numbers, voicemail, centralized administration, and call forwarding. It also has Skype in the workplace, which allows small businesses to connect with potential customers, suppliers, and partners.

In 2012, courts in Hempstead County, Arkansas, began integrating Skype into their trial system. In a trial in April 2012, four witnesses testified virtually through Skype. Without Skype, the state of Arkansas would have had to pay for them to travel to the court to testify.

How else is it used?

Skype can also be used to help in illegal activities. Suburban gangs have been known to use Skype to organize crimes and other gang activity. The FBI claims that 48% of violent crimes in suburban jurisdictions are caused by gangs. There have also been several counts of people using Skype to record and take part in child pornography. A high school football coach named Joseph J. Ostrowski plead guilty and was sentenced to serve 25 years in prison for producing child pornography and engaging in “sextortion” of youths in more than a dozen states. He persuaded computer users to engage in sexually

http://www.skype.com/en/about/
http://languagemagazine.com/?page_id=2565
http://en.wikipedia.org/wiki/Skype
http://www.entrepreneur.com/article/219431
http://www.hopestar.com/article/20130401/NEWS/130409969/-1/entertainment%20life
http://www.legalatmosphere.net/gang-violence-moves-suburbs-york/
explicit acts that he viewed over Skype. He also attempted to get the youths to send him nude photographs of themselves over the service.  

Alex Ernesto Calderon Velasquez, a resident of Reston, VA, was charged recently with producing child pornography through Skype. He allegedly sexually groomed a 14 year old girl and then extorted her to strip and engage in sexual acts over Skype chats. He recorded these chats and stored them on his computer along with other child pornography.

Robert Branson was arrested in 2012 after AOL and Yahoo flagged his emails for containing known images of child pornography. When law enforcement searched his house, they found that he was sending child pornography to others through Skype as well as email.

Some terrorist organizations have also moved their communications to Skype. In 2011, Indian intelligence agencies were especially frustrated by this as they tried to move forward with their post-Mumbai blasts investigations. Since the terrorists used Skype instead of traditional phones to communicate, the usual search of telephone records for suspicious phone calls, which used to prove essential for every investigation, was giving them no results.

**How can we intercept it?**

With Skype being used for things like terrorism and child pornography along with all of the legitimate uses, law enforcement needs a way to intercept the data. It is still unclear whether or not Skype falls under a phone service that is subject to the Communications Assistance for Law Enforcement Act, CALEA. The FCC has interpreted CALEA to cover Skype, but in 2009, Skype said that, since they are not a telephone company that owns phone lines, it is exempt from the law. Cell phone services, like Verizon Wireless, do not own wires either but are subject to CALEA, weakening Skype’s argument.

Despite the confusion over whether the laws apply to the technology or not, Skype seems to be making moves to work with law enforcement and make their data available to them. In 2012, the *Washington Post* reported that Skype was cooperating with law enforcement to make online chats and user information available to the police. The article also says that Skype has implemented changes that

---

63 [http://oakhillva.com/2013/03/01/reston-man-accused-of-creating-child-pornography-through-skype/#.UVs8JhxtIOM](http://oakhillva.com/2013/03/01/reston-man-accused-of-creating-child-pornography-through-skype/#.UVs8JhxtIOM)
let law enforcement access addresses and credit card numbers where applicable. It has also been speculated that Microsoft has been implementing several changes since they bought the service that make wiretapping of Skype conversations easier.

Microsoft is centralizing Skype supernodes. The decentralization of Skype was one of its most appealing features, to those who worry about the backend side of things, and one that made the conversations so secure. They are replacing peer-to-peer supernodes with Linux grsec systems. The centralization makes wiretapping possible on a system where it had previously been all but impossible. Microsoft also applied for a patent on a technology called Legal Intercept which is designed to monitor and record Skype calls. Since they applied for the patent before buying Skype, conspiracy theorists think that the purchase was made for the sole reason of making the service able to be wiretapped, which would explain why they paid such a high price for it.

How exactly does centralizing the supernodes make wiretapping easier? Skype used to connect calls using a P2P network which meant that data never passed through a central server on its way to its destination. With Microsoft’s changes, the supernodes will not just make the introduction, but they will actually route the data as well. The supernodes used to be third-party Skype users, but now Microsoft will own the supernodes. Because of this, they will be able to give the data passing through it to law enforcement agents if asked. While this might cost Skype the users that were using it because of its secured conversations, most users just like the fact that it is a free way to talk to people around the world. Though some may be outraged over this change, the vast majority of its users won’t know – or care – that it’s even happening.

Microsoft is not the only one trying to patent Skype interception tools. Dennis Chang, the president of VOIP-Pal, has recently obtained a series of patents related to online voice calls. One of them will allow government agencies to silently record VoIP calls. Suspects under investigation would be identified by their username and other subscriber information if available. According to the patent, video streams and multimedia data could be intercepted along with the call. His patent, which is similar to Microsoft’s, will restructure the way VoIP calls are routed over the Internet.

---

68 [http://www.itworld.com/cloud-computing/286482/was-skype-reworked-microsoft-make-it-easier-wiretap](http://www.itworld.com/cloud-computing/286482/was-skype-reworked-microsoft-make-it-easier-wiretap)
69 [http://www.itworld.com/cloud-computing/286482/was-skype-reworked-microsoft-make-it-easier-wiretap](http://www.itworld.com/cloud-computing/286482/was-skype-reworked-microsoft-make-it-easier-wiretap)
Once Skype’s supernodes are centralized, the main obstacle in the face of interception would be the legal aspect. It would have to be determined definitively whether or not Skype is subject to the same rules as other telephone companies under CALEA. If they are found to fall under CALEA, it should be better enforced. If they are found not to fall under it, new laws should be made similar to CALEA that cover VoIP services. The new laws should cover sections like warrants and how Skype’s policies should be changed to better implement the laws. Judging from what Microsoft has done so far, this does not seem like it will pose much of a problem should it come up.
Twitter

What is Twitter?

Twitter is an online social media network, built on open source software that has gained popularity over the last few years. It is sometimes referred to as “SMS for the Internet.” In the years since its launch, it has become one of the top ten visited websites worldwide and the 13th most visited website in the US. People on Twitter communicate through updates of 140 characters or less called “Tweets.” Though only registered users can post Tweets, anyone can read public Tweets. Tweets can be posted through the web interface, SMS, or one of the many smartphone apps that exist for Twitter. It was created by Jack Dorsey in 2006, and has over 500 million registered users and over 400 million Tweets generated a day as of July, 2012.

Users can follow others and get notified when they tweet. Twitter users group Tweets together by using hashtags. Hashtags are words or phrases that are preceded by a “#” sign and contain no spaces. To mention another user in a Tweet, the “@” is used, immediately followed by the Twitter username. Users can retweet others, which is basically sharing a Tweet they liked with their own followers. Retweeted Tweets are preceded by “RT.”

Twitter is marketed as more than just a social media network, though. It is said to be “an information network.” With Twitter, people are able to get the latest stories, ideas, opinions, and news about and from whatever and whomever they find interesting. Since Twitter is used all over the world and is available in more than 20 languages, users can connect with people and ideas they may have never gotten a chance to otherwise. Tweets are not just limited to words, either. Photos and videos can be shared on Twitter. People can hold conversations through Tweets, and there are even sites that allow for expanded Tweets, allowing a user to have thoughts that go beyond the character limitation without having to break things up into multiple Tweets.

According to their website, Twitter values both transparency as well as security. Along with their team, they have a group of independent security research volunteers that help to spot potential security

---

74 https://twitter.com/about
issues in the site. They have forms available that anyone who claims to have found a security vulnerability can fill out to alert the team to the issue.\(^75\)

As mentioned above, Twitter utilizes open source software. Without open source software, there probably wouldn’t be a Twitter. Because of the popularity of Twitter, they are faced with many real-time engineering problems that other sites may never have to deal with.

In his speech, “The Open Source Technology Behind a Tweet,” given at a Linux Foundation event in September 2012, Chris Aniszczyk, the Open Source Manager at Twitter, explained what goes on behind the scenes when a Tweet is sent. Aniszczyk said that there are around 2.8 billion Tweets sent a week, which equals to about 5,000 Tweets per second. This is not counting award shows, sporting events, etc when people Tweet even more. The process of a Tweet being sent out from a person to the service and then to all of his or her followers is called “fan out.” It sounds simple, but that is not the only thing that happens when a Tweet is sent.

When a user types in a Tweet to share, it first goes to Twitter’s api endpoint, status/update. Each Tweet has a unique ID to help in indexing, searching, and storage. The next stop a Tweet makes is to Snowflake, their open source program that quickly generates an ID for the Tweet that is guaranteed to be unique. After that it goes to Rock Dove which is a reverse geoservice. This finds out where the Tweet was sent from and can find what places the user is nearby. The Tweet then moves on to Talon which deals with links that are sent in a Tweet. All links are wrapped with tico, which is used for two reasons. It makes analytics easier, and it helps with spam control. After that, the Tweet is sent to Gizzard, which is Twitter’s open source layer that runs on top of MySQL to let them scale it. Here is where the Tweet is stored.

After the Tweet is stored, it gets the HTTP okay response and the Tweet is rendered. It then moves to Fire Hose which is for clients that need real time access to Tweets, like Microsoft. These clients get all Tweets with no more than a 100 millisecond delay. It then moves on to their Early bird infrastructure which is basically their search functionality. Here is where the Tweet is indexed. Then it moves to the analytics infrastructure which archives Tweets. Archived Tweets can later be looked through for trends, etc. After it is archived, it is finally time for the fan out. Because there is no limit to how many followers a user can have, and because some users, especially celebrities, have an incredible number of followers, the Tweet may then move on to Flock. Flock.db runs on top of Gizzard and helps to store Tweets for people with huge followings. Most of these are open source and available at github.\(^76\)

\(^75\) [https://twitter.com/about/security](https://twitter.com/about/security)
\(^76\) [http://www.youtube.com/watch?v=q0HWq4DwTAQ](http://www.youtube.com/watch?v=q0HWq4DwTAQ)
The following chart allows the movement of the Tweet to be viewed visually.

Aniszczyk said that open source software was chosen for Twitter because it allows for more customization and the ability to tweak code to meet different engineering needs as the Twitter community grows. He also claims that the Twitter team uses open source software as an opportunity to teach and learn from the communities that they work with.

Examples of open source software that are used at Twitter include, but are not limited to, the following. First, MySQL is used for the storage of Tweets. Services like analytics and search within their infrastructure are powered by Cassandra, Hadoop, Lucene, and Pig, as well other Apache projects. Their caching infrastructure, Twemcache, which is used to scale their growing traffic, was heavily inspired by Memcached. They also produce their own open source software.\(^7\)

\(^7\)[http://opensource.com/business/12/8/open-source-technology-behind-twitter]
In 2010, Twitter went through a redesign which allowed them to make changes to the underlying technology of the website along with design changes to the look of the site. During this redesign, Twitter moved from Ruby on Rails to an architecture almost entirely made up of JavaScript, focusing on ease of development, extensibility, and performance. One of these changes was making Twitter.com a client of its own API, meaning that the data is fetched from the same endpoints as the mobile site, smartphone apps, and other applications. All data is now fetched from an optimized JSON fragment cache. They also have a JavaScript API that is used to minimize the number of network requests made while using the website. They also made changes to page management, using a page routing system that maintains a strong relationship between a URL and its content; the rendering stack, to support crawlers and users that do not have JavaScript; and inline media, to embed third-party content linked to in Tweets directly on the website.\(^78\)

**How is it used?**

Twitter is used by a variety of different people for a variety of different uses. Twitter is used by everyday people keeping in touch with family and friends. It is used by celebrities that want to connect with fans on a more personal level. It is used by people who believe that what they had for dinner is worthy enough news to share with the world and by people who have discovered its potential as a new literary form. Though it would be impossible to list out every way that Twitter has been, and can be, used, here are some examples.

In a study done in 2009, Pear Analytics, a market research firm, analyzed 2,000 Tweets over the course of two weeks and broke them down into six separate categories. 40% of the Tweets consisted of “pointless babble” which was explained as social grooming or the desire of users to know about how the people around them were doing, 38% of the Tweets were conversational, 9% had pass-along value, 6% were self-promotion, 4% were news, and 4% were spam.\(^79\) With hundreds of millions of Tweets being generated a day, this seems like a very small amount to test.

Twitter connects customers with the businesses that they support in real time. It allows them to get timely updates about products, services, and promotions. Businesses can use Twitter to

---


interact with an engaged audience, gain market intelligence and feedback, and build relationships directly with the customers and influencers. Twitter has also been used for direct sales.  

The term “Twitter Revolutions” sprung up a couple of years ago when people started to use Tweets to organize protests. This happened during the 2011 Egyptian Revolution, the 2010 Tunisian Revolution, and the 2009 Moldova civil unrest, among others. The use of Twitter in this way led to some governments, like Egypt and Iran, trying to block the service. 

People turn to Twitter when they feel that traditional journalism is being censored to spread the real news of what is really going on. Twitter has also been used as an emergency communication system. Recently at George Mason University, a study was started that tested the effectiveness of Twitter as a means of communication during an emergency. The use of the service as an emergency communication system was also used by the company itself to communicate during earthquakes in San Francisco, CA, the location of Twitter headquarters. Twitter can also be used to track the spreading of epidemics. 

Some colleges and universities have adopted Twitter as a learning tool. It has been used to promote student interaction in large lectures, thus increasing participation of students and communication between students and faculty. Twitter has also been used as a new form of literature. Rick Moody, a novelist, wrote a short story made up entirely of Tweets called “Some Contemporary Characters.”

According to an analysis of Twitter accounts, the service is also very popular with world leaders and politicians. The heads of state of 125 countries and 139 other leading politicians have Twitter accounts. Together, they have 52 million followers. Most of these, however, do not do their own tweeting. 

Twitter is also being used to make television more interactive. Not only can fans follow and send Tweets to the stars of their favorite shows, but the television show may suggest hashtags to promote Tweets about an important scene or a new character in the show. They do this to engage fans of the show in conversation. This has sometimes been referred to as “chatterboxing.” Chatterboxing has also been used to encourage users to watch televised events like the Super Bowl and award shows.

---

80 [https://twitter.com/about](https://twitter.com/about)
82 [http://www.guardian.co.uk/media/2011/may/22/scottish-newspaper-identifies-injunction-footballer](http://www.guardian.co.uk/media/2011/may/22/scottish-newspaper-identifies-injunction-footballer)
84 [http://www.utdallas.edu/~mrankin/usweb/twitterconclusions.htm](http://www.utdallas.edu/~mrankin/usweb/twitterconclusions.htm)
The possibilities of Twitter are endless. A man named Chris Strouth tweeted that he needed a kidney and got one. People have gotten jobs through Twitter and made music using the Tweets as lyrics. Twitter has been used to fight crime, lose weight, and get health insurance. Twitter is also being used to help save dying languages.

**How else is it used?**

Though there are hundreds of different ways that people can use Twitter that are legal, helpful, creative, and encouraged, there are still people who to choose to use it illegitimately instead. These include using it to abuse others, plot terrorist acts, and spread gang activity. The following is an assortment of ways that Twitter has been used that show that the interception of Tweets is sometimes necessary.

Some people use Twitter to promote bigotry. They post racist, sexist, and other prejudicial comments that they may not feel comfortable saying in person. The layer of anonymity offered by the Internet gives them the courage to let their inner bullies out. For example, a student at Swansea University, Liam Stacey, was jailed for racist and offensive comments that he made on Twitter. Public figures, like TV presenter Kirstie Allsopp and Olympian Rebecca Adlington, have suffered from abusive comments on Twitter. These range from people calling them fat to death threats. Tulisa Contostavlos, a judge on the X Factor, received Tweets from people who threatened to “fire bomb” her home. Some celebrities, choosing not to put up with the abuse, have left Twitter rather than endure it.

Gang members have also turned to Twitter to promote gang activity and fuel gang rivalry. They spread inflammatory messages about rival gangs, encouraging them to respond. Many fights that start online are then moved into the real world. Gangs have used social media, like Twitter, to recruit new members, spread plans about meetings or parties, and, according to the Chicago Crime Commission, even commit crimes. Gang members have admitted to sending taunting Tweets to other gangs and posting homemade rap music videos to promote their gang and insult others.

Terrorist groups have also been known to turn to Twitter. A London researcher, Murad Batal al Shishani, says that although the Internet has always allowed terrorists a way to communicate with each other, extremists have recently turned to Twitter for its relative simplicity in mobilizing international

---

88 [http://stories.twitter.com/](http://stories.twitter.com/)
masses at a moment’s notice. He also says, though, that his research has shown that terrorist groups use Twitter more as a recruiting tool and newswire than a place for calls to action. They post about current events and hope to gain sympathizers for their cause.91

Some people have also abused Twitter’s ability to act as a communication channel in times of emergency. In the city of Veracruz, Mexico, two people were arrested for terrorism and sabotage after posting Tweets about false school attacks. After Tweets stating that there was a kidnapping at the school, real-life chaos broke out on the streets. The suspects could face up to 30 years jail time.92

Twitter has also been used as a means to make drug deals. In Sandy, Utah, three teenagers were arrested after a Twitter conversation led to a marijuana bust at a local middle school. The mother of a 13 year old girl found marijuana with her daughter, which led her to search through her text messages and Twitter account. The mother was shocked to find that information about who had marijuana, who smoked, and who was coming to get some were all posted pretty openly. Using the information that she found, a sting was set up at the school.93

How can we intercept it?

There are a few different obstacles to be faced in trying to intercept Twitter messages. First, the sheer number of Tweets that are generated a day is overwhelming. Second, when signing up for Twitter, users only have to enter a name, email address, and set up a password. There is no way to check if people are really who they say they are, giving users the anonymity that many internet sites offer. While they do have “verified accounts” to distinguish between real and fake Twitter accounts for celebrities and public figures, there is no requirement for every account to be verified. Finally, interception laws should be looked at to ensure that they cover Twitter communication.

Twitter traffic interception is not a concern unique to America. The English government is working towards extending the police’s power of surveillance of internet activity to cover social networks like Facebook and Twitter and determine who talked to whom. The proposed measures build on law enforcement’s ability to investigate email and SMS (text) messages as part of the Home Office’s Communications Capabilities Development Programme, which is a government initiative to create an all-encompassing mass surveillance scheme for the UK by logging phone calls, emails, and text messages.

93 http://fox13now.com/2013/02/18/intercepted-twitter-messages-lead-to-marijuana-bust/
between residents. They hope to establish a new framework for retaining and collecting communication data by communication service providers.

ISPs would be responsible for both handling and monitoring the storage of data. This would incur additional costs to the ISPs, such as the cost of “black box” equipment that would be used to intercept communications and the cost to regularly update the algorithms that are used. The draft also has proposed measures to limit the disclosure of data and unauthorized access to records. The collection of data by ISPs would be overseen by the Interception of Communications Commissioner. People would also be able to complain to the Investigatory Powers Tribunal about abuse of surveillance powers.

There are people, like Joss Wright of the Oxford Internet Institute, that have complained that the new interception laws are too invasive. They argue against the overly simplistic comparison between access to phone records and combined access to email, web activity, social media, and other internet traffic. They claim that the extent to which people use these newer services is significantly greater, and the information that it reveals about a person’s habits and interactions is much more telling than phone records. Despite arguments about its invasiveness, the government hopes to see the new laws in effect by the end of June 2015.94

One of the main complaints about the draft, aside from its invasiveness, is that the British government did not talk with the ISPs about it beforehand. Considering the fact that the responsibility of the storage falls to them, the ISPs felt that they should have been consulted about how best to implement the desired plans.

Another country that is looking at ways to intercept Twitter communication is Saudi Arabia. Saudi Arabia is most concerned about the anonymity of Twitter. The government said that militants are using the platform to create social unrest, hiding behind the anonymity that it provides. Their solution to this is to require Twitter users to register with more than just a username and password. The Saudi Arabian Communications and Information Technology Commission (CITC) wants to uncover social media users’ real identities and plans to do this by requiring Twitter users to register an ID connected with their phone records. This would link each account to a real person.

The ID numbers would preserve anonymity of users with each other, but the government would be able to trace Tweets back to a specific person and to intercept all Tweets made by a specific person. To do this, though, they’d need the agreement of Twitter administration.95

Both of these methods have been said to be too invasive. They both tackle different parts of the interception problem and have their own ups and downs. An interception method that draws from both of these as well as attempting to fix the problems with both should be considered. First, as is evident from both cases, no one group can handle the interception alone. Therefore, no one group should be able to decide on the method of interception.

The government, including both law enforcement and the legislative branch, ISPs, and Twitter itself should get together and discuss the best way to intercept Twitter traffic. Since Twitter already stores all of the Tweets. They would just need to make sure that their method of storage allows for easy retrieval should law enforcement require it. A method of verifying all users of Twitter could be discussed, however may not be necessary immediately. Just like with intercepting email, law enforcement could be required to get a name and Twitter username before they can ask to intercept a person’s Tweets.
WhatsApp

What is WhatsApp?

WhatsApp is an instant messaging application for smartphones. The name is a pun on “What’s up?” It was developed to be a better alternative to SMS messaging for smartphones. It is the number one downloaded app in several different countries around the world and handles 10 billion messages a day as of August, 2012. Along with text messages, users can share images, videos, and audio messages through the service. With the rise in its popularity, the number of SMS messages has seen a significant decline. Provided the user has an adequate data plan for their smartphone or is connected to a WiFi network at the time, sending and receiving messages over WhatsApp is free.

WhatsApp runs on a customized version of XMPP. XMPP, or Extensible Messaging and Presence Protocol originally called Jabber, is an open source communications protocol developed in 1999 for near real-time instant messaging, presence information, and contact list management. When it is installed on a phone, it creates a user account with the user’s phone number and country code— or Jabber ID - as a username. It then automatically adds contacts from the phone’s address book to the user’s WhatsApp contact list by comparing the phone numbers stored on the phone to the central database of WhatsApp users. IMEIs and MAC addresses were originally used for passwords. In the updated version of WhatsApp, a password is randomly generated on the server side for the account. Passwords are generally not obtained by the user.

Messages are sent as TCP packets, and up until August 2012, they were sent in unencrypted plain-text format. WhatsApp assures its users that all messages sent through the latest version of WhatsApp for iOS and Android are encrypted, though they did not release the cryptographic method. Multimedia Messages, or MMS, which include pictures, video, and audio, that are shared with contacts are uploaded to a server via HTTP before being delivered to the recipient as a Base64 thumbnail of the image, video, or audio.
media, if applicable, along with the HTTP link as the message body. This allows users to view a thumbnail version in the conversation windows before deciding on whether or not they want to view the media. As with any technology that allows users to send and receive information, security is a big concern for its users. WhatsApp has been addressing security concerns recently that it did not focus on before becoming so popular. As mentioned earlier, WhatsApp messages are now encrypted. They also market the fact that chat history is not stored on their servers for lengthy amounts of time. Messages are only stored until they are delivered. The company makes sure to let its users know that messages are not protected from someone gaining physical access to their phone, though.

**iMessage**

With the release of OS X Mountain Lion in July 2012, Apple replaced iChat with iMessage. By October of that year, 300 billion messages were sent with the service. This means that iMessage was delivering roughly 28,000 messages per second. iMessage is similar to WhatsApp in that it provides users with an alternative way to send both text and multimedia messages. Unlike WhatsApp, however, iMessage is not a multi-platform service and is only available for devices running iOS 5 or later. When a user that has iMessage and an active data connection sends a message, Messages will check with Apple to see if the recipient also has iMessage set up. If they do, all messages will automatically be sent via iMessage instead of SMS. If they don’t, messages will be sent as SMS. Green buttons and text bubbles let a user know that the messages are SMS, while blue buttons and text bubbles mean they are iMessages.

Some features of iMessage include being able to see when the other user in the conversation is typing, being able to carry the same conversation on multiple iOS devices, being able to see when a message is read if Read Receipts is enabled, and being able to take part in group chats. Although a user can send a lot of the same information through iMessage that they can through WhatsApp, it is not always as easy. WhatsApp allows users to send most things through the app itself. iMessage only allows photos and videos to be shared through the app. Contacts have to be shared through the address book, and locations have to be shared through the Maps app. Because of these inconveniences and the fact

---

102 [https://github.com/venomous0x/WhatsAPI](https://github.com/venomous0x/WhatsAPI)
that it is only available for people who use Apple devices with iOS 5 and later, WhatsApp is still the more popular messaging application for smartphones.

The imessage protocol is based on Apple Push Notifications (APNS) instead of XMPP. This is a proprietary, binary protocol that sets up a Keep-Alive connection with Apple servers. Each connection has a unique code that identifies the route messages should use. Connections are encrypted with TLS using a client side certificate that the device requests when iMessage is activated.106 Apple has not published how long iMessages are saved on their servers, if they are saved at all.

How is it used?

WhatsApp is used like many other instant messaging services. People use it to send messages and pictures to friends and family. It is a great way to keep in touch with people in real time no matter where they are in the world since international text messaging rates don’t apply. A popular feature of WhatsApp is the group chat option where users can set up a group conversation. With family in a few different countries, my cousins and I set up a group chat in WhatsApp that keeps us all connected. You can also send broadcasts to everyone on your WhatsApp contact list. Broadcasts can cover a wide range of topics, like self-promotion, companies that are currently hiring, and missing people.

Unlike Twitter and other social media platforms, though, you can only communicate with people on your contact list. You cannot have any “public messages,” nor can you find people to contact without having their phone number first. WhatsApp also allows users to have a profile where they can upload a picture and a status that they want to share with everyone on their contact list.

How else is it used?

Though stalking and harassment can be done on almost every communication platform, WhatsApp has a block feature that tries to protect its users from this kind of abuse. When a person blocks a contact, the blocked contact will no longer show up on his or her phone, s/he will not be able to receive or send messages from or to them, profile changes will not be seen, and the blocked contact will

---

lose access to the “last seen on” feature which shows when the last time a user was on WhatsApp. The person will not be deleted, though, and status messages will still be seen by the blocked individual.\textsuperscript{107}

People can use WhatsApp to plan nefarious acts. Since WhatsApp does not store messages, users are given a sense of security they may not have on other platforms. Nefarious acts can include gang activity, drug sales, crimes, and terrorist activity. For example, in March, 2012, the son of Banten Deputy Governor Rano Karno in Indonesia was arrested for drug possession after ordering ecstasy from a drug dealer via WhatsApp.\textsuperscript{108}

Just like SMS messages began to be used in armed robberies, drug sales, and wire fraud when texting rose in popularity, WhatsApp is beginning to be used in these circumstances too.

How can we intercept it?

At the moment, WhatsApp and iMessage are considered instant messaging services. Because of their inherent similarities, they should be subject to the same laws and interception policies as SMS instead. SMS laws are still being discussed in America, with an ECPA reform being argued over. Law enforcement wants to make it mandatory for carriers to store SMS logs for two years, in case they are needed in criminal investigations. With an increase in the number of cases that deal with some technological aspect, like SMS messages, it is not surprising that these laws are being called for by law enforcement.\textsuperscript{109}

As a guide for a potential interception method for WhatsApp messages, this paper will look into other interception laws implemented around the world for similar technologies, namely email and SMS. These laws will include the Australian Telecommunications (Interception and Access) Act 1979 (C’th) and the UK’s Regulation of Interception Powers Act 2000.

The Australian Telecommunications (Interception and Access) Act 1979 prohibits both the interception of traffic moving over a telecommunications system and the access to stored communications, which includes things like email, SMS, and voicemail, without authorization. As of June 13, 2006, an amendment that established a new regime governing access to this information has been in effect. Part of this regime was the creation of a new type of warrant, referred to as a “stored
communications warrant” that law enforcement agencies are required to obtain to access information stored by a carrier.110

The stored communication warrant is issued for a specific person and not a specific telecommunications service. This means that if a warrant is obtained for John Smith, law enforcement could get both his SMS and voice mail stored at the carrier with the same warrant. The warrant will grant the officer access to any traffic sent from John Smith or to John Smith that became a stored communication before the warrant was executed. The warrant remains in force until it is first executed or until 5 days after it was issued, whichever comes first.111

In accordance with the UK’s Regulation of Interception Powers Act 2000 (RIPA), ISPs use “black boxes” to intercept email messages. The captured data is stored with the ISP and indexed to make searching it more efficient. ISPs are required to provide the ability to maintain interception capability, which means that the government can monitor a person’s email activity when the need arises. Under RIPA, email header information should be stored for no less than 12 months and no more than 24 months.112 Data should be stored in a way that allows for requests to be responded to as fast as possible.113

Drawing from both of these laws, an interception law for WhatsApp and iMessage could be suggested. The first thing that would change would be WhatsApp policy of not storing messages after they are delivered. Due to the volume of messages that are being sent over WhatsApp, this is not a trivial thing. Messages should be stored for 12 months. They should also be indexed and stored in a way that allows for easy accessibility.

To effectively implement a law like this, though, several things have to be determined. First, there should be a set way for messages to be stored that other technologies similar to WhatsApp should follow as well. Currently with the ECPA, data that has been stored for over 180 days only needs a subpoena to be viewed, while data stored less than 180 days needs a search warrant. The same rules would be applied to WhatsApp messages. Finally, it may be difficult to know who has jurisdiction over the messages. Though WhatsApp headquarters are located in California, the messages they will have to store may be kept elsewhere. This could cause issues with the evidence obtained from WhatsApp messages being admissible in court.

111 https://www.efa.org.au/Issues/Privacy/tia.html#asc
Unlike the Australian Telecommunications (Interception and Access) Act 1979, where warrants only allow law enforcement to obtain data that was stored before the warrant was served, warrants should allow for data to be collected for a certain amount of time, e.g. 30 days, after the warrant was served as well. This would allow law enforcement to lawfully intercept data instead of just accessing the stored messages.
Conclusions

As new technologies are being developed, we, as a society, are becoming more dependent on them. We use technology in every aspect of our life and share a lot more on and with these technologies than previous generations have, and sometimes more than we should. It is no wonder, then, that any form of interception seems too invasive. Current technologies reveal more about us on a personal level than older technology did or could. This inherent exposure does not make people more comfortable with others reading their communications, though. People put things on the Internet for everyone to see, but are then surprised when people view it aside from the people they choose.

The very fact that technology has become so ingrained in our society, however, is what makes it necessary to have the ability to intercept it. People, especially the Facebook and Twitter generation who have known nothing else, have forgotten how to filter. Because they are so used to posting everything about their lives online, they don’t stop to think about whether or not they actually should be saying this over the Internet. This is why there are teenagers tweeting about buying drugs and gang members talking about the latest crime they’ve committed on platforms where the entire world can read what they’re writing.

Perhaps it’s a cynical view, but as long as technology exists, people will find a way to abuse it. And as long as people are abusing it, law enforcement needs a way to investigate and stop them. The abuse of new technologies is becoming more complex, too. Law enforcement officers now have to worry about more than one technology being used at a time to do something illegal. For example, just this month a new malware appeared that combines Skype and Bitcoin. The malware tries to get a Skype user to click a link. Once the link is clicked, a Bitcoin miner application is dropped on the computer and the malware uses that computer to mine for bitcoins.¹¹⁴

People have always been outraged by the idea of government wiretapping and interception and they always will be outraged by the idea. Having the technology to intercept communication, however, does not automatically turn a government into an Orwellian Big Brother. As long as there are laws in place that protect the citizens’ privacy and that explicitly state that the “spy on all citizens” button is not to be used, having the technology should put people’s minds at ease. With both the technology and the laws, what the government is basically saying is, “We won’t read your emails, but if there’s a child predator after your kids, we’ll be able to protect them.”

For the services mentioned in this paper at least, adapting the technologies to make them easier to intercept will not affect their user base. Businesses are using the services to connect with customers and partners. Whether or not the government has the ability to listen in on their conversation or read what they tweet will not change that. Individuals are using them to connect with family and share their lives with friends. They are sharing files and engaging in online commerce. Whether the networks are centralized or decentralized, whether the companies agree to cooperate with law enforcement agencies or not, as long as the services remain free and do not decline in quality of service, the users will most likely not even know the difference.

The ones that are using Bitcoin and BitTorrent, etc, to try and get around laws and stay out from under the government’s radar may complain, but a lot of them will just go off in search of the newest technology for the added security. And the ones that don’t probably didn’t understand the benefits of the technology they were using in the first place.
References


translated


<http://fox13now.com/2013/02/18/intercepted-twitter-messages-lead-to-marijuana-bust/>.


"High Performance Computing at FSU." *HPC Data Repository*. The Florida State University. Web.


<http://languagemagazine.com/?page_id=2565>.


