big_data

digital_age = [Privacy, Security, Technology, Legal, Issues]

NOLALawCorp.com

d0j3

BRACE YOURSELVES
POWERPOINT SLIDES
ARE COMING
DIYLOL.COM

DANK MEMES
ARE COMING

This presentation covers the intersection of Big Data, Technology, Privacy and the Law . . .

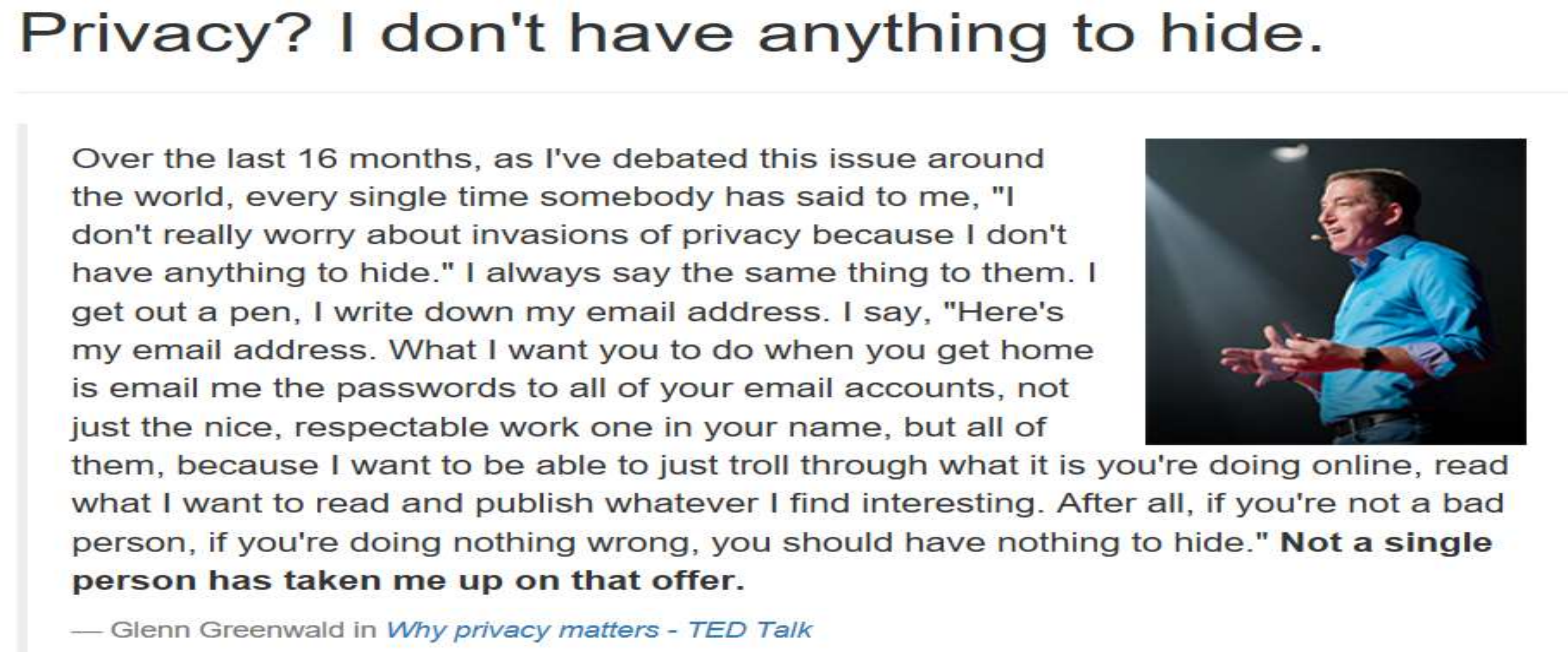
I intend to avoid death by powerpoint; therefore, prepare yourself for dank memes . Why?

For teh Lulz

About Me . . .

Why Does this matter?

- Knowledge is Power
- Knowledge is Contagious



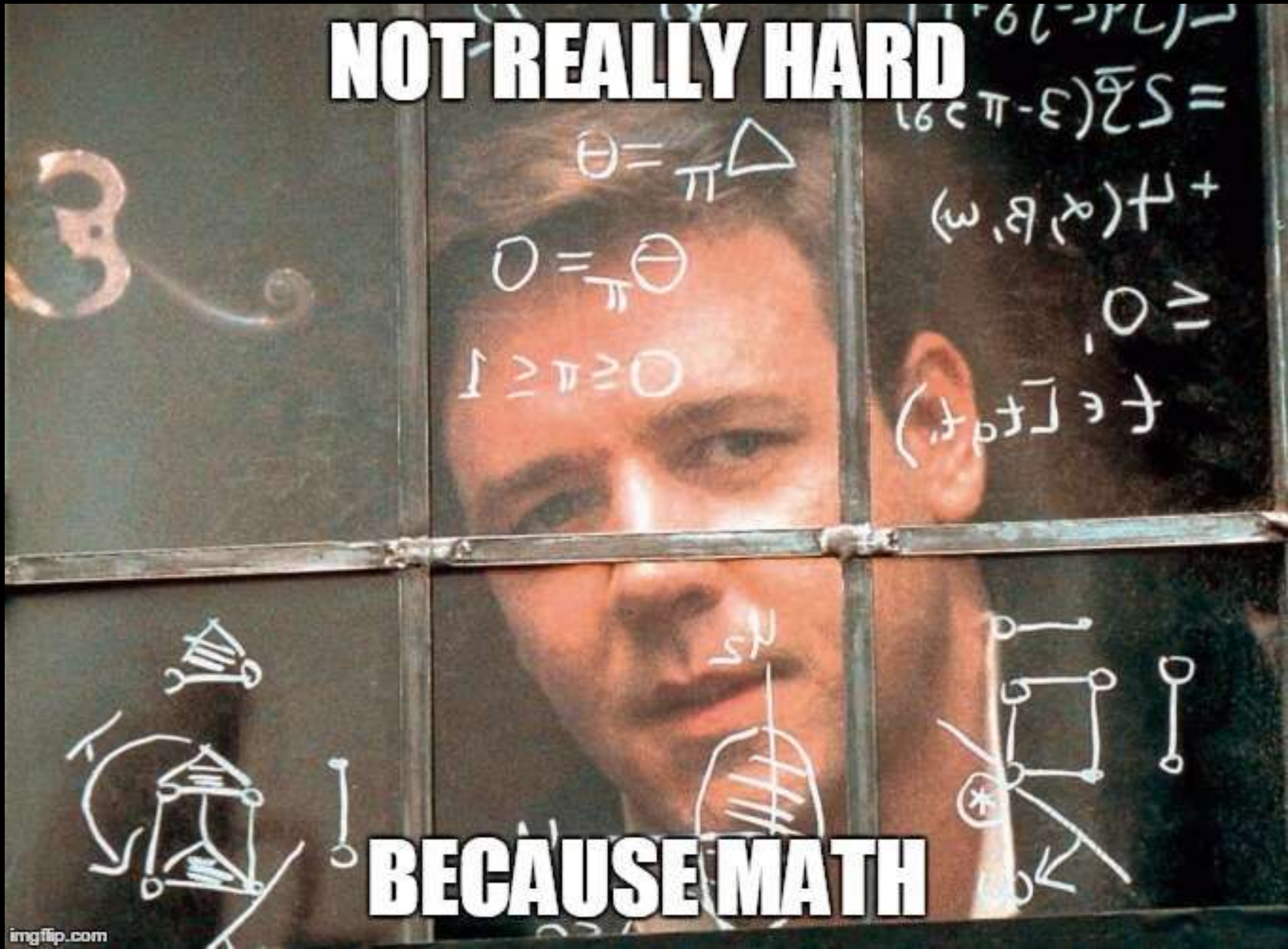
Privacy? I don't have anything to hide.

> Over the last 16 months, as I've debated this issue around the world, every single time somebody has said to me, "I don't really worry about invasions of privacy because I don't have anything to hide." I always say the same thing to them. I get out a pen, I write down my email address. I say, "Here's my email address. What I want you to do when you get home is email me the passwords to all of your email accounts, not just the nice, respectable work one in your name, but all of them, because I want to be able to just troll through what it is you're doing online, read what I want to read and publish whatever I find interesting. After all, if you're not a bad person, if you're doing nothing wrong, you should have nothing to hide." **Not a single person has taken me up on that offer.**
>
> — Glenn Greenwald in *Why privacy matters - TED Talk*

Glenn Edward Greenwald (born March 6, 1967) is an American journalist and author, best known for his role in a series of reports published by The Guardian newspaper beginning in June 2013, detailing the United States and British global surveillance programs, and based on classified documents disclosed by Edward Snowden Greenwald's work on the Snowden story was featured in the documentary Citizenfour, which won the 2014 Academy Award for Best Documentary Feature.

Cryptography

- Cryptography - aka ‘crypto’ is the foundation of most privacy related tech
- from Greek kryptós, "hidden, secret"; and graphein, "writing", or logia, "study“
- Cryptography is the practice and study of techniques for **secure communication** in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages



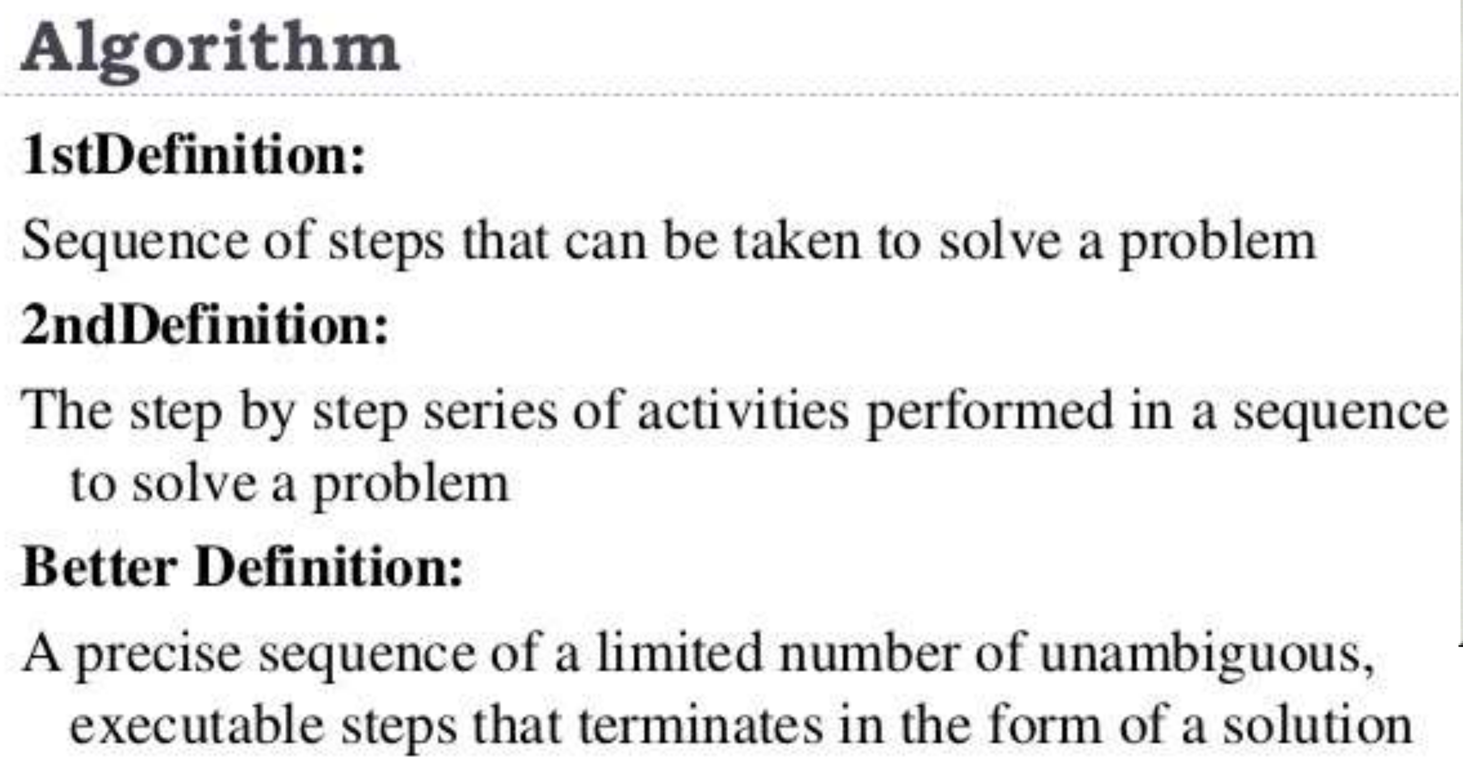
Cryptography in Practice

- Various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography.
- Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, and communication science.
- Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

It is important to distinguish Encryption & Hashing and understand their appropriate roles and applications.

Know your Role: Hashing v. Encryption

- MD5 and SHA are **hash functions** (SHA is actually a family of hash functions(**SHA-256**, the function **powering the Bitcoin Blockchain** is a member of the SHA-2 cryptographic hash functions designed by the **NSA**))
- A **Hash function** receives input in the form of a piece of data(*e.g.* a key or password), compacts it, and creates a suitably unique output (*e.g.* fixed length string of characters) that is very hard to emulate with a different piece of data.
- **Hash Functions** don't encrypt anything - you can't take MD5 or SHA output and "unhash" it to get back to your starting point. The difference between the two aforementioned hash functions lies in what algorithm they use to create the hash *(e.g.* the function's output, aka "digest").
- -note that MD5 is now vulnerable as a way was discovered to easily generate collisions and should not be used nor trusted anymore (also WPA2 KRACK *contra*)
- RSA is an **encryption algorithm**. In a nut shell, you have two "keys" (private and public) and you can perform a function with one key (encrypt or decrypt) and reverse with the other key. Which key you use depends on whether you are trying to do **a digital signature** or an **encryption**.



Algorithm

1stDefinition:

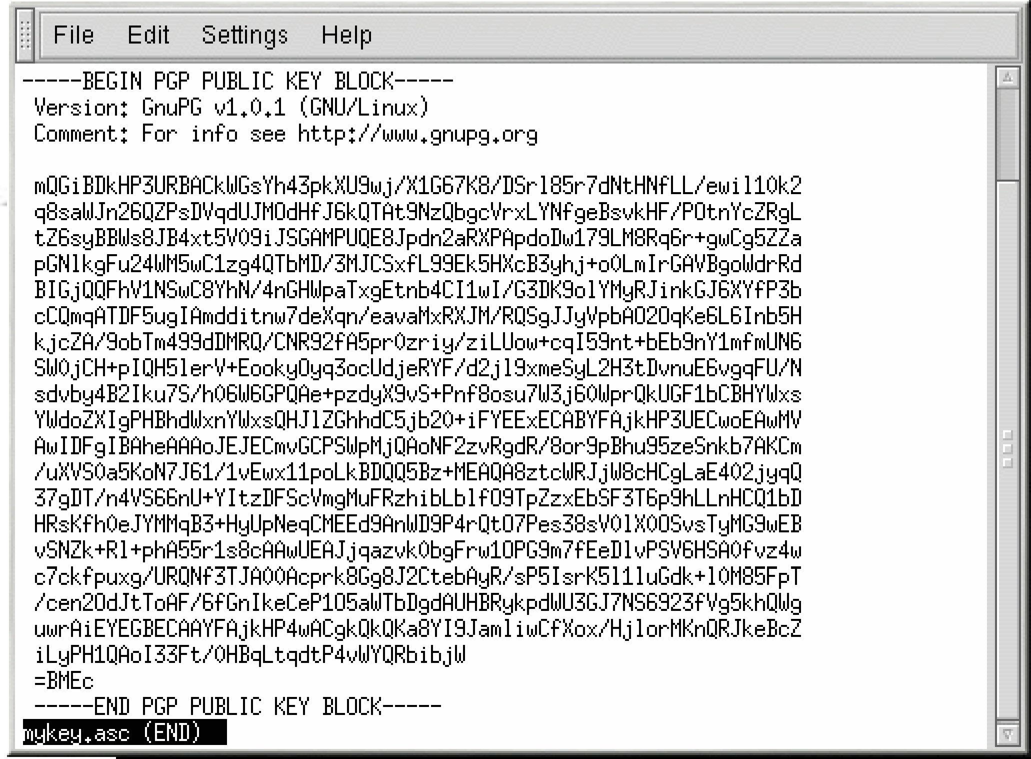
Sequence of steps that can be taken to solve a problem

2ndDefinition:

The step by step series of activities performed in a sequence to solve a problem

Better Definition:

A precise sequence of a limited number of unambiguous, executable steps that terminates in the form of a solution



```
-----BEGIN PGP PUBLIC KEY BLOCK-----
 Version: GnuPG v1.0.1 (GNU/Linux)
 Comment: For info see http://www.gnupg.org

 mQGiBDkHP3URBACkWGsYh43pkXU9wj/X1G67K8/DSrl85r7dNtHNfLL/ewil10k2
 q8saWJn26QZPsDVqdUJMOdHfJ6kQTAt9NzQbgcVrxLYNfgeBsvkHF/POtnYcZRgL
 tZ6syBBWs8JB4xt5V09iJSGAMPUQE8Jpdn2aRXPApdoDw179LM8Rq6r+gwCg5ZZa
 pGNlkgFu24WM5wC1zg4QTbMD/3MJCSxfL99Ek5HXcB3yhj+oOLmIrGAVBgoWdrRd
 BIGjQQFhV1NSwC8YhN/4nGHWpaTxgEtnb4CI1wI/G3DK9olYMyRJinkGJ6XYfP3b
 cCQmqATDF5ugIAmdditnw7deXqn/eavaMxRXJM/RQSgJJyVpbAO2OqKe6L6Inb5H
 kjcZA/9obTm499dDMRQ/CNR92fA5pr0zriy/ziLUow+cqI59nt+bEb9nY1mfmUN6
 SWOjCH+pIQH5lerV+EookyOyq3ocUdjeRYF/d2jl9xmeSyL2H3tDvnuE6vgqFU/N
 sdvby4B2Iku7S/hO6W6GPQAe+pzdyX9vS+Pnf8osu7W3j6OWprQkUGF1bCBHYWxs
 YWdoZXIgPHBhdWxnYWxsQHJlZGhhdC5jb20+iFYEExECABYFAjkHP3UECwoEAwMV
 AwIDFgIBAheAAAoJEJECmvGCPSWpMjQAoNF2zvRgdR/8or9pBhu95zeSnkb7AKCm
 /uXVSOa5KoN7J61/1vEwx11poLkBDQQ5Bz+MEAQA8ztcWRJjW8cHCgLaE402jyqQ
 37gDT/n4VS66nU+YItzDFScVmgMuFRzhibLblfO9TpZzxEbSF3T6p9hLLnHCQ1bD
 HRsKfhOeJYMMqB3+HyUpNeqCMEEd9AnWD9P4rQtO7Pes38sV0lXOOSvsTyMG9wEB
 vSNZk+Rl+phA55r1s8cAAwUEAJjqazvkObgFrw1OPG9m7fEeDlvPSV6HSAOfvz4w
 c7ckfpuxg/URQNf3TJAOOAcprk8Gg8J2CtebAyR/sP5IsrK5l1luGdk+lOM85FpT
 /cen2OdJtToAF/6fGnIkeCeP105aWTbDgdAUHBRykpdWU3GJ7NS6923fVg5khQWg
 uwrAiEYEGBECAAYFAjkHP4wACgkQkQKa8YI9JamliwCfXox/HjlorMKnQRJkeBcZ
 iLyPH1QAoI33Ft/OHBqLtqdtP4vWYQRbibjW
 =BMEc
 -----END PGP PUBLIC KEY BLOCK-----
mykey.asc (END)
```

Generally, random numbers are used to “seed” Key Generation Algorithms that generate unique “Keys” like the one pictured above.

Cryptographic Hashing Functions

Note- Right: changing the case of the character ‘a’, changes the output digest.

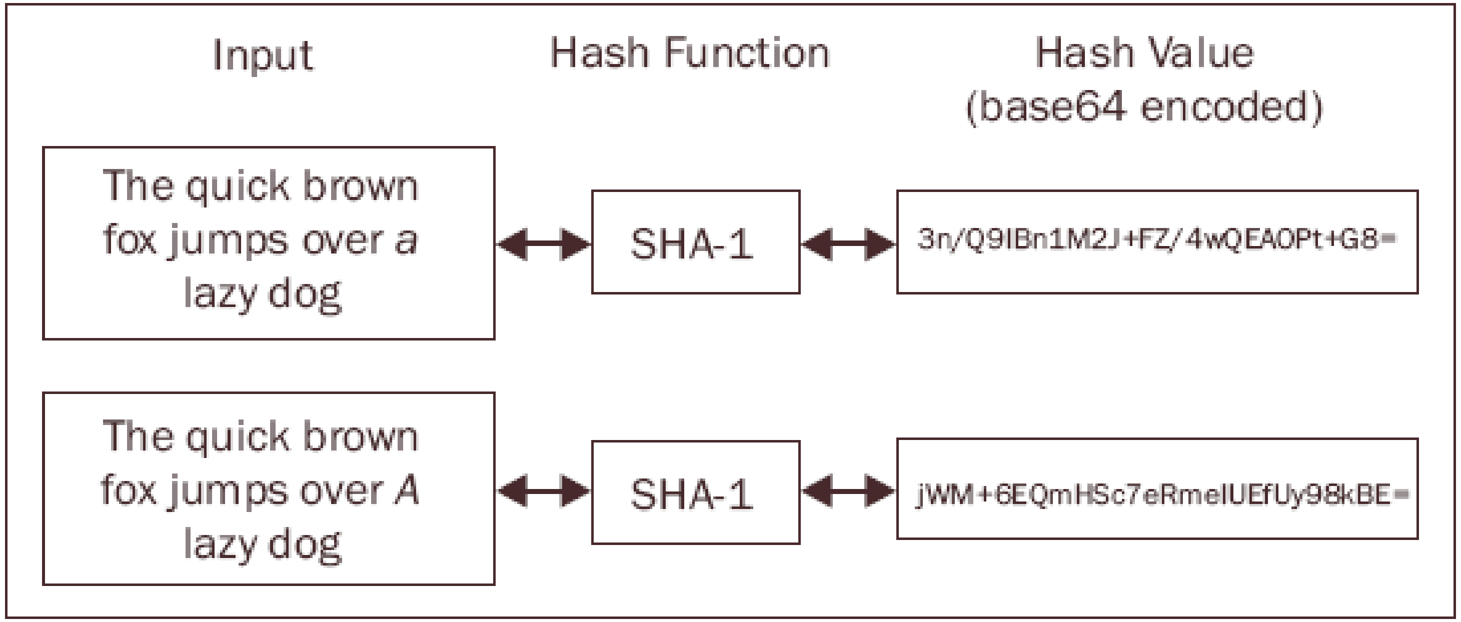

Input
Hash Function
Hash Value
(base64 encoded)
The quick brown fox jumps over a lazy dog
SHA-1
3n/Q9IBn1M2J+FZ/4wQEAOPt+G8=
The quick brown fox jumps over A lazy dog
SHA-1
jWM+6EQmHSc7eRmeIUEfUy98kBE=

Figure 17: Hash Function

- (ex) MD5, SHA-1,
- Hashes (the hashing function output) are known as "**digests.“**
  - THIS IS NOT "encryption“
- Often, the distinction between Hashing and Encryption confuses laypeople, especially because both of these words are in the category of "cryptography“; nonetheless, it's important to understand the difference.
- **Encryption** transforms data from a cleartext to ciphertext **and back** (given the right keys); moreover, the two texts should roughly correspond to each other in size: big cleartext yields big ciphertext, and so on. "Encryption" is a **two-way** operation.
- (ex) RSA is an Asymmetric encryption Algorithm – A **cipher** is a fancy name for an encryption or decryption algorithm. - *See Next Slide For Details*

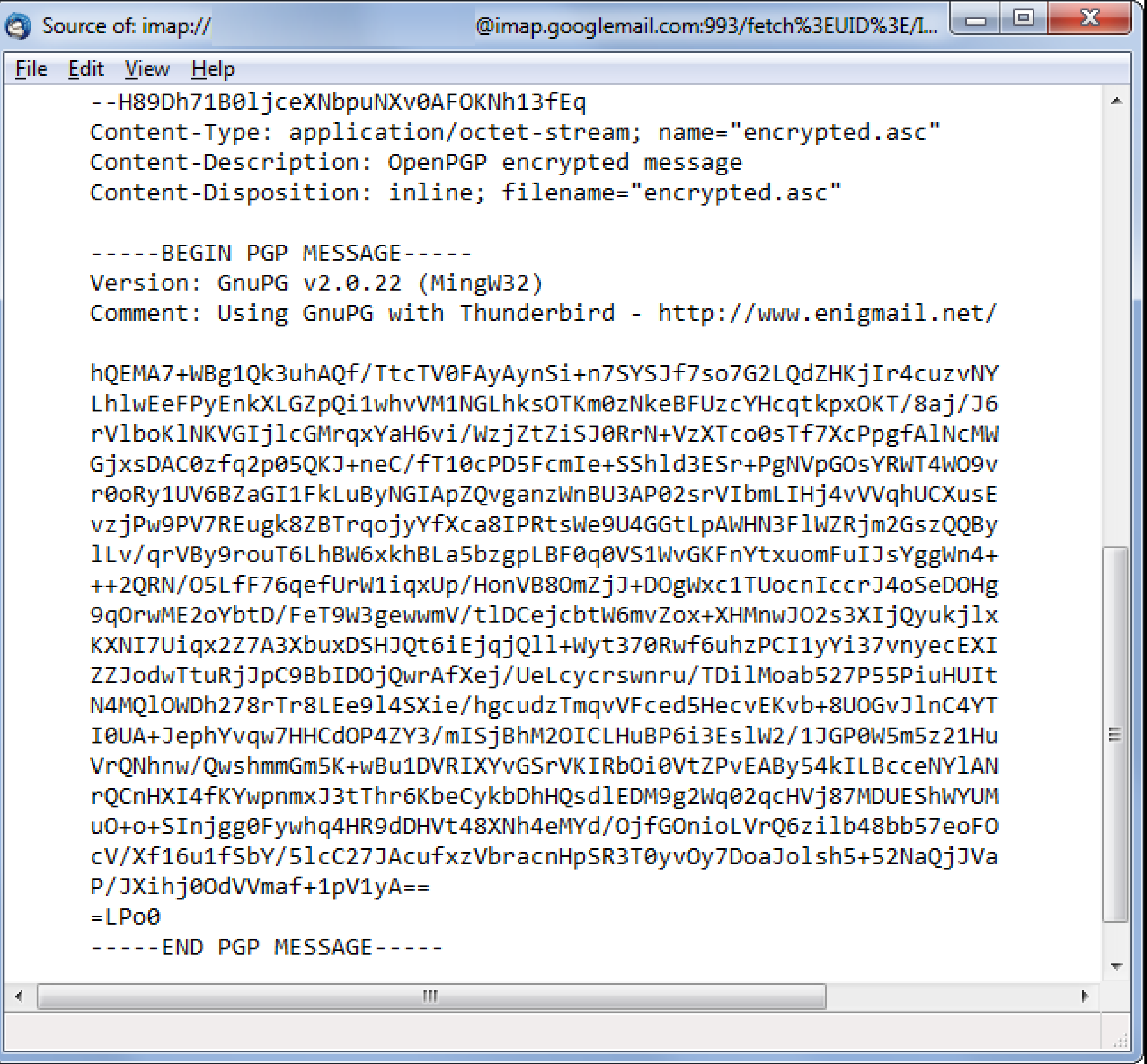
YOU CAN'T LEAK PASSWORDS
IF YOU DON'T STORE PASSWORDS

YOU DIDN'T PROPERLY SECURE YOUR PERSONAL DATA?
AAAAAAND IT'S GONE
made on imgur

MD5? TELL ME AGAIN
HOW SERIOUSLY YOU TAKE USER DATA
quickmeme.com

How Digital Signatures Work

- A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents. Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public.
- To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The **encrypted hash**, along with other information, such as the hashing algorithm, is the **digital signature.**
- The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time because hashing is much faster than signing..large computations cost $$$). *See* (1)



```
--H89Dh71B0ljceXNbpuNXv0AFOKNh13fEq
Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc"

-----BEGIN PGP MESSAGE-----
Version: GnuPG v2.0.22 (MingW32)
Comment: Using GnuPG with Thunderbird - http://www.enigmail.net/

hQEMA7+WBg1Qk3uhAQf/TtcTV0FAyAynSi+n7SYSJf7so7G2LQdZHKjIr4cuzvNY
LhlwEeFPyEnkXLGZpQi1whvVM1NGLhksOTKm0zNkeBFUzcYHcqtkpxOKT/8aj/J6
rVlboKlNKVGIjlcGMrqxYaH6vi/WzjZtZiSJ0RrN+VzXTco0sTf7XcPpgfAlNcMW
GjxsDAC0zfq2p05QKJ+neC/fT10cPD5FcmIe+SShld3ESr+PgNVpGOsYRWT4WO9v
r0oRy1UV6BZaGI1FkLuByNGIApZQvganzWnBU3AP02srVIbmLIHj4vVVqhUCXusE
vzjPw9PV7REugk8ZBTrqojyYfXca8IPRtsWe9U4GGtLpAWHN3FlWZRjm2GszQQBy
lLv/qrVBy9rouT6LhBW6xkhBLa5bzgpLBF0q0VS1WvGKFnYtxuomFuIJsYggWn4+
++2QRN/O5LfF76qefUrW1iqxUp/HonVB8OmZjJ+DOgWxc1TUocnIccrJ4oSeDOHg
9qOrwME2oYbtD/FeT9W3gewwmV/tlDCejcbtW6mvZox+XHMnwJO2s3XIjQyukjlx
KXNI7Uiqx2Z7A3XbuxDSHJQt6iEjqjQll+Wyt370Rwf6uhzPCI1yYi37vnyecEXI
ZZJodwTtuRjJpC9BbIDOjQwrAfXej/UeLcycrswnru/TDilMoab527P55PiuHUIt
N4MQlOWDh278rTr8LEe9l4SXie/hgcudzTmqvVFced5HecvEKvb+8UOGvJlnC4YT
I0UA+JephYvqw7HHCdOP4ZY3/mISjBhM2OICLHuBP6i3EslW2/1JGP0W5m5z21Hu
VrQNhnw/QwshmmGm5K+wBu1DVRIXYvGSrVKIRbOi0VtZPvEABy54kILBcceNYlAN
rQCnHXI4fKYwpnmxJ3tThr6KbeCykbDhHQsdlEDM9g2Wq02qcHVj87MDUEShWYUM
uO+o+SInjgg0Fywhq4HR9dDHVt48XNh4eMYd/OjfGOnioLVrQ6zilb48bb57eoFO
cV/Xf16u1fSbY/5lcC27JAcufxzVbracnHpSR3T0yvOy7DoaJolsh5+52NaQjJVa
P/JXihj0OdVVmaf+1pV1yA==
=LPo0
-----END PGP MESSAGE-----
```

To Learn More, *See:*

PGP or GPG

Pretty Good Privacy (or GNU Privacy Guard – the Open Source Alternative) is an encryption program that provides cryptographic privacy and authentication for data communication. (Snowden used it ;)

Let’s Recap & Really Nail this stuff Down, This Time with Pictures . . .

Redundant, for sure. Nonetheless, this material is the bedrock foundation upon which much of the modern technological battle for privacy is being laid.

note - this is a quick overview.

Cryptography is deep, complex subject.

Some practitioners devote their entire careers to the study of cryptography

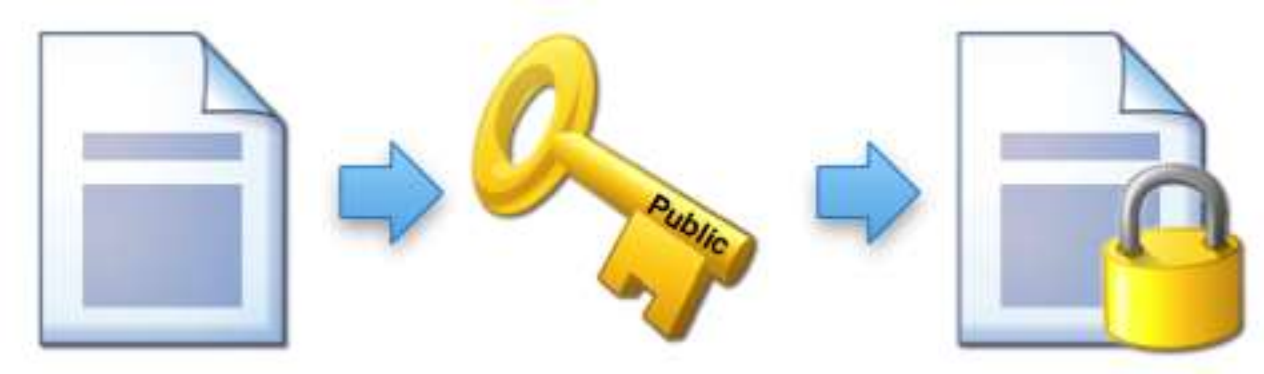
Encrypting a Document

See (2)

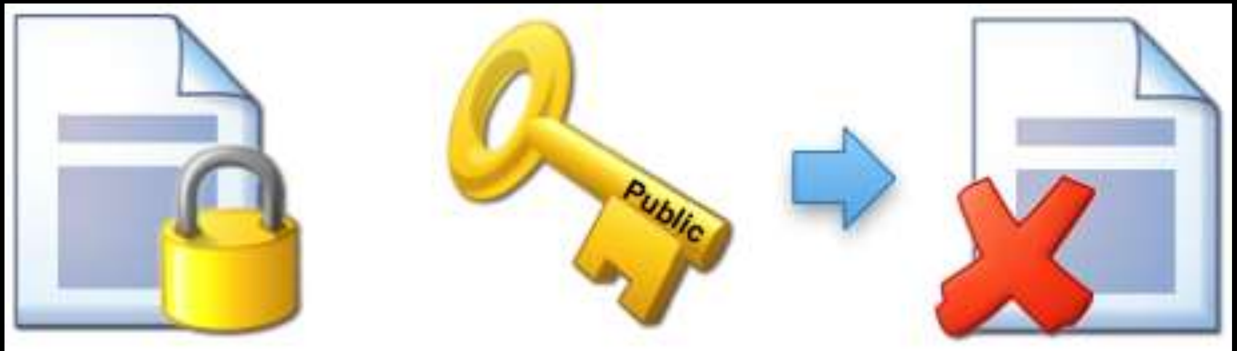
- To use a digital signature or encryption you must have a **digital id** also known as a **digital certificate**. A **digital id/digital certificate is used to do (2) two things**. First, **(1)** it can be used to do email encryption or encrypt files so that they can only be read by the person they are intended for. Second, **(2)** it can be used to "sign" or place a digital signature on a document to guarantee that it arrives in the same state it was originally sent and no one has added or changed things.

A digital id or digital certificate consists of a **public** and **private** key. Your public key is shared with everyone. Your private key is kept private. These keys are text documents full of what appears to be random numbers and letters, but with the proper algorithm, these numbers and letters have a very unique property. (much like a human fingerprint)

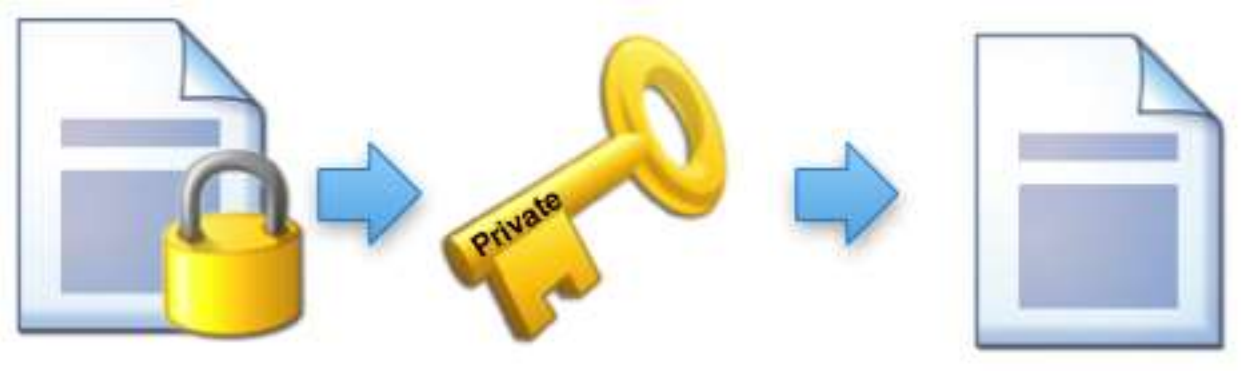
If you take a document and run it through an algorithm with your public key, you get back an encrypted document.



Once it is encrypted, the public key can't be used to decrypt the document. The process is one way so it doesn't matter if other people have the public key, they can't read the document.



To decrypt the document you must have the private key. If you give the encrypted document to an algorithm with the private key, you will get back the original document.



Signing a Document with a Digital Signature:

Checksums & Hashes

- A checksum (hash functions are a type of checksum) is a simple way to send an extra piece of information along with some data that can be used to make sure that the data is the same on both sides.
  - Checksums are traditionally used to detect errors or tampering which may have been introduced during the storage or transmission of data
  - if the computed checksum for the current data input matches the stored value of a previously computed checksum, there is a very high probability the data has not been accidentally altered or corrupted.
  - By themselves, checksums are often used to verify data integrity but are not relied upon to verify data authenticity. (generally, authenticity involves a combination of different processes/systems, see blockchain, etc)
  - Checksum function varieties include hash functions, fingerprints and randomization functions. However, each of those concepts has different applications and therefore different design goals.

Hashes for Digital Signatures

- In simple form, a hash is an algorithm (or set of steps or instructions designed to accomplish a clearly defined goal) that you can run a piece of data through (text, a file, etc.) and get out a number that represents the original. You can't recreate the original from the number, but for most practical purposes you can use that number to represent the input. In other words, it will be very difficult to find another input file (or text) that will produce the same output.

Let's construct a simple hash of the following text:

The quick brown fox jumped over the lazy hound.

Our hash is going to be created by multiplying the number of letters by the number of words.

38 letters

9 words

38 x 9 = 342

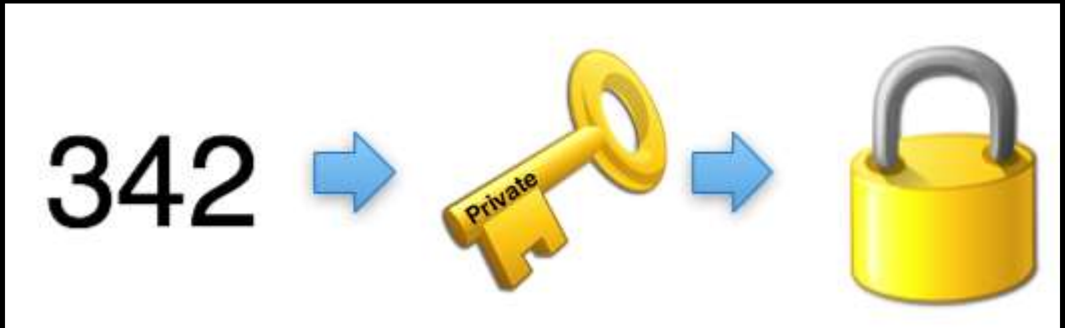
Accordingly, If I were to transmit this message to you, I can include the number 342 along with it as a form of checksum or hash. You could do the math required of the algorithm to compute the message's number and have a pretty good idea whether the message is the same as the one I sent you.

Obviously, this type of solution will only protect against unintentional changes in the data. If someone changes the email in route, they could just as easily change the number "342" to match whatever the hash is for their modified message

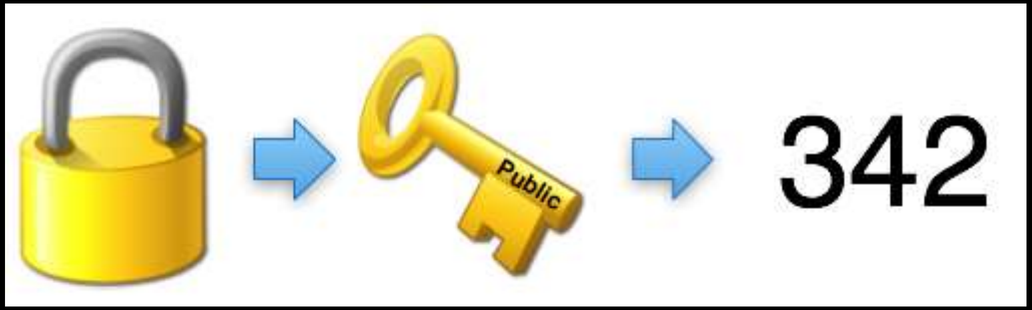
The best way to transmit the message and hash in terms of security and efficiency is to transmit them over a secure channel. Generally, unbeknownst to the majority of end users, most email clients implement secure channel technology as background services. (see next for example)

- If I try to encrypt the hash number with your public key, the message is only readable by you–I might as well just encrypt the whole message.
- If I encrypt it (the hash number) with my public key, then I'm the only one who can read it–not particularly useful either . . .

Alas, look what happens when I encrypt the Hash Value with my PRIVATE Key.



Presently, the Hash Value, 342, encrypted in a way that can be opened by anyone with my_PUBLIC_Key. Because my_PUBLIC_Key is the only thing that can decrypt that value, it guarantees them that I was the one who originally encrypted the hash number value 342.



If someone wants to change the message and change the hash value, they would have to be able to encrypt it with my_PRIVATE_Key . . .

Crypto Basics Roundup

- So, when you send messages signed with a digital signature, the hash value guarantees that the message hasn’t been changed.
- Encrypting the hash value with your private key allows anyone to verify that the hash value, itself, hasn’t been changed using your public key. (This is normally handled automatically by your software, and it will give you a warning if you get a message where decrypting the hash value produces a different number.)
- The encrypted hash value is added as a small attachment or added to the bottom of the email.

YO DAWG I PUT A TABLE IN UR HASHTABLE
SO U CAN HASH THE HASHING OF YOUR TABLEHASH
IN O(N) SPACE
quickmeme.com

OPSEC VIOLATIONS
BESIDES GETTING SOMEONE KILLED, THEY CAN RUIN YOUR CAREER.
NOT MY CAREER...BUT DEFINITELY YOURS.

I DON'T ALWAYS BREAK THE LAW AND PUT NATIONAL SECURITY AT RISK BUT WHEN I DO
IT'S BECAUSE IT WAS A MATTER OF CONVENIENCE AND I'M ABOVE THE LAW

OPSEC = Operational Security

It is a BIG DEAL, Especially NOW MORE THAN EVER.

If you don’t believe me, ask Hillary . . .

Poor OPSEC is part of **“What Happened”** to Her!

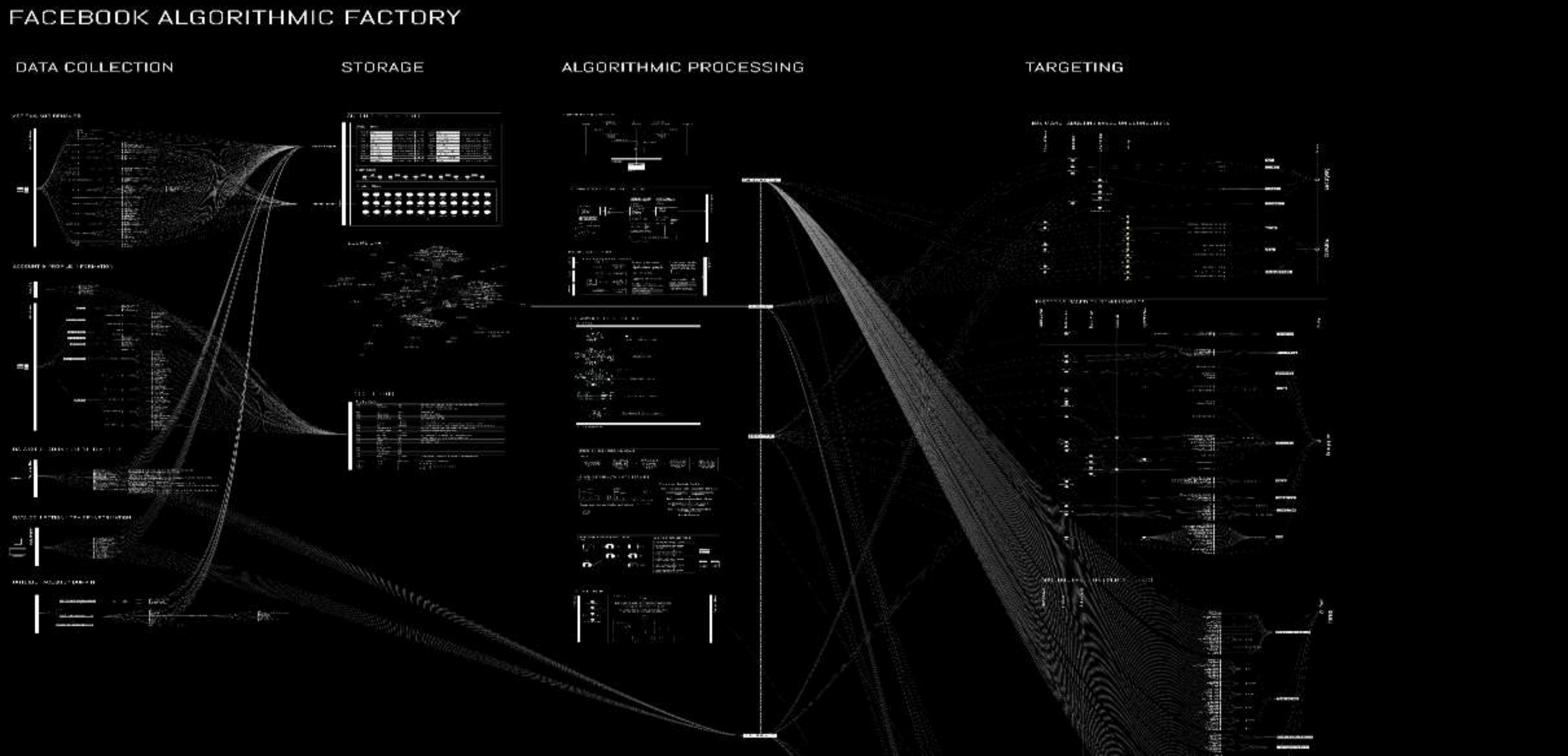
– note: I warned that dank memes were coming

Now, Let's Change Gears and Move on to the Grab Bag of Modern Issues related to Data Privacy, Security and the Law.

The Massive Data Collection by Facebook – Visualized

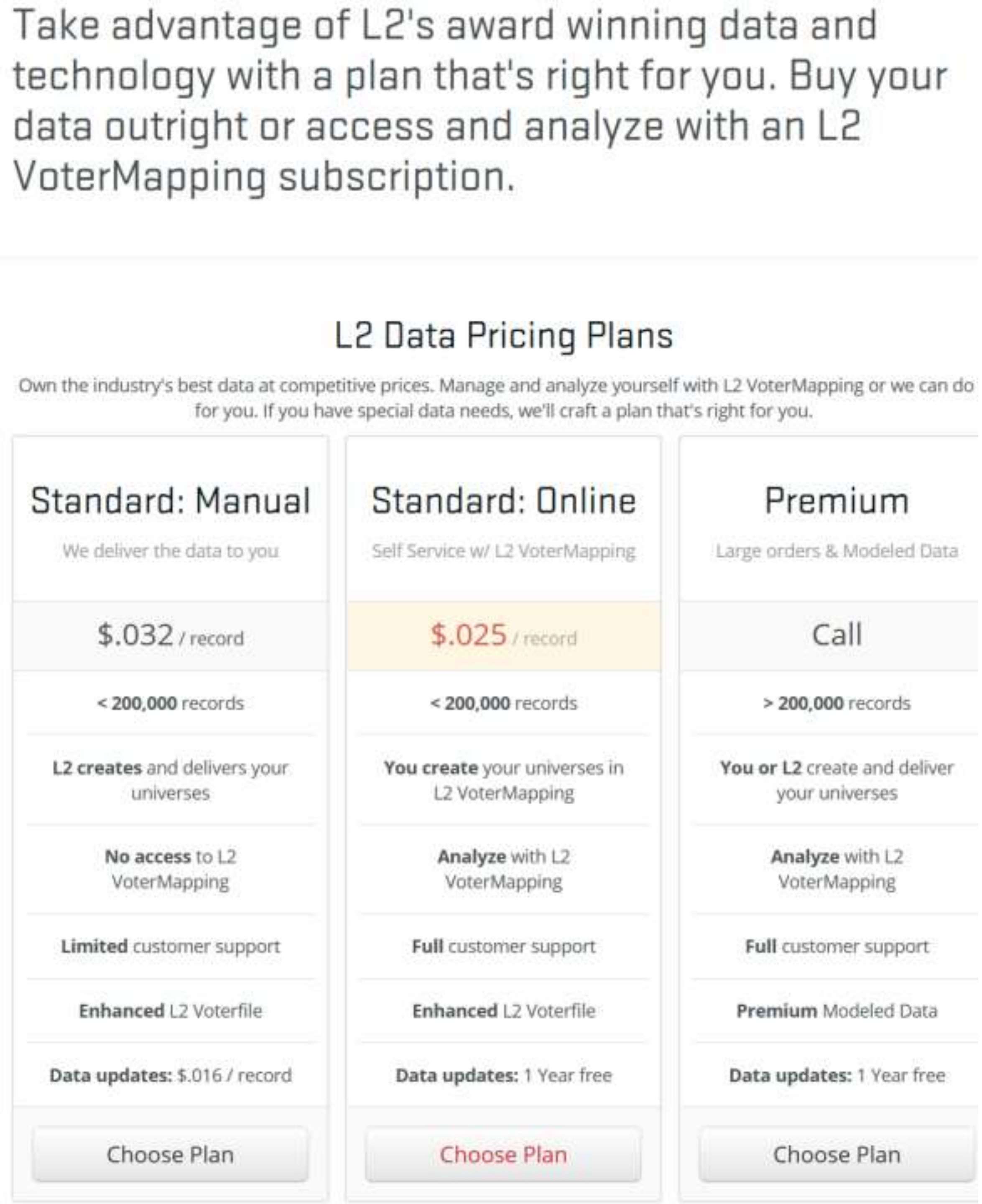
https://dataethics.eu/en/facebooks-data-collection-sharelab/

https://labs.rs/wp-content/uploads/2016/08/FacebookFactory-01.gif



“Facebook CEO Mark Zuckerberg has all but conquered the tech world, and based on his latest activities, it seems that he may have his sights set on the world of politics.”

Big Data Brokers: L2 Political

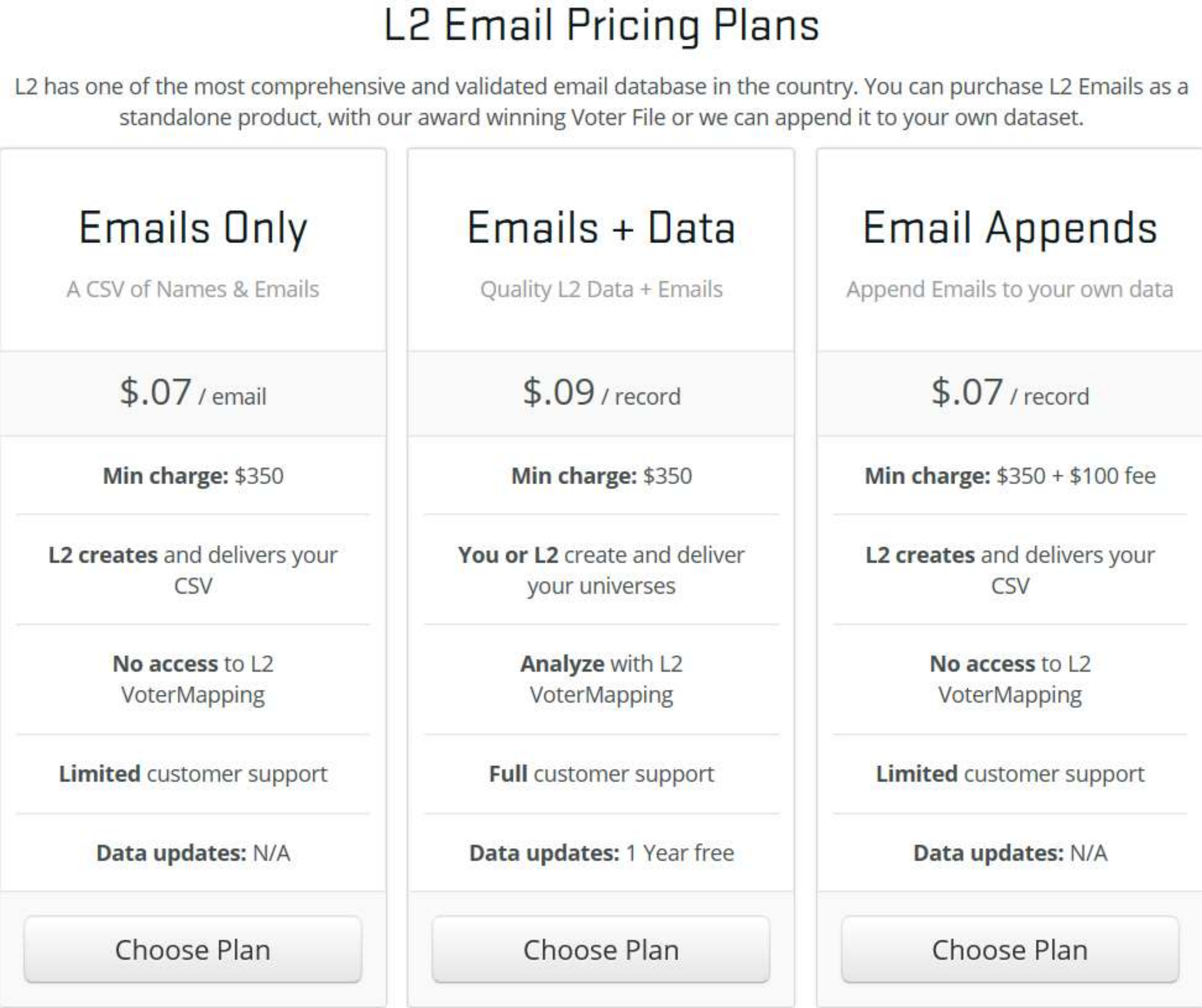


Take advantage of L2's award winning data and technology with a plan that's right for you. Buy your data outright or access and analyze with an L2 VoterMapping subscription.

L2 Data Pricing Plans

Own the industry's best data at competitive prices. Manage and analyze yourself with L2 VoterMapping or we can do for you. If you have special data needs, we'll craft a plan that's right for you.

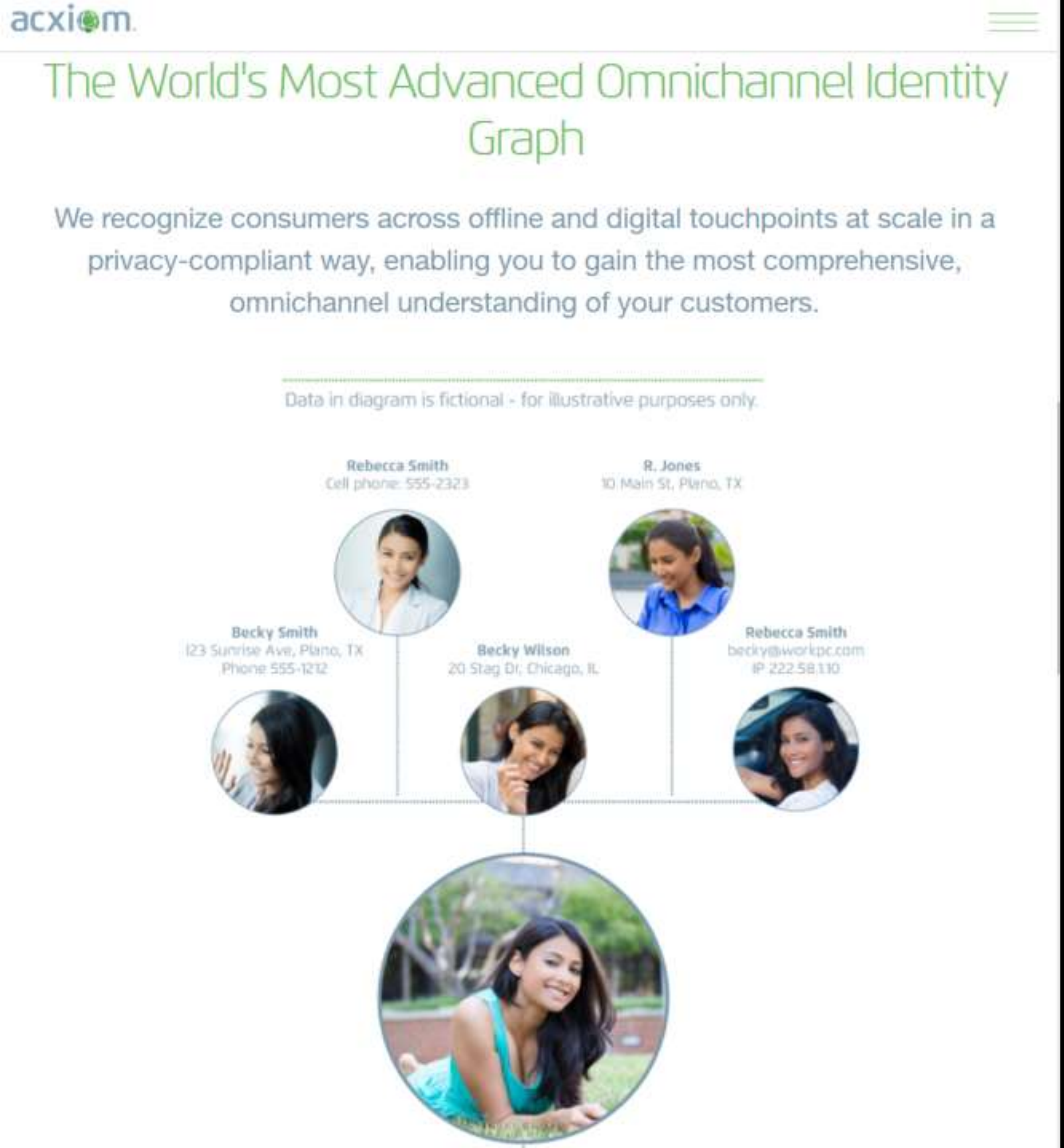
Standard: Manual	Standard: Online	Premium
We deliver the data to you	Self Service w/ L2 VoterMapping	Large orders & Modeled Data
$.032 / record	$.025 / record	Call
< **200,000** records	< **200,000** records	> **200,000** records
L2 creates and delivers your universes	**You create** your universes in L2 VoterMapping	**You or L2** create and deliver your universes
No access to L2 VoterMapping	**Analyze** with L2 VoterMapping	**Analyze** with L2 VoterMapping
Limited customer support	**Full** customer support	**Full** customer support
Enhanced L2 Voterfile	**Enhanced** L2 Voterfile	**Premium** Modeled Data
Data updates: $.016 / record	**Data updates:** 1 Year free	**Data updates:** 1 Year free
Choose Plan	Choose Plan	Choose Plan



L2 Email Pricing Plans

L2 has one of the most comprehensive and validated email database in the country. You can purchase L2 Emails as a standalone product, with our award winning Voter File or we can append it to your own dataset.

Emails Only	Emails + Data	Email Appends
A CSV of Names & Emails	Quality L2 Data + Emails	Append Emails to your own data
$.07 / email	$.09 / record	$.07 / record
Min charge: $350	**Min charge:** $350	**Min charge:** $350 + $100 fee
L2 creates and delivers your CSV	**You or L2** create and deliver your universes	**L2 creates** and delivers your CSV
No access to L2 VoterMapping	**Analyze** with L2 VoterMapping	**No access** to L2 VoterMapping
Limited customer support	**Full** customer support	**Limited** customer support
Data updates: N/A	**Data updates:** 1 Year free	**Data updates:** N/A
Choose Plan	Choose Plan	Choose Plan



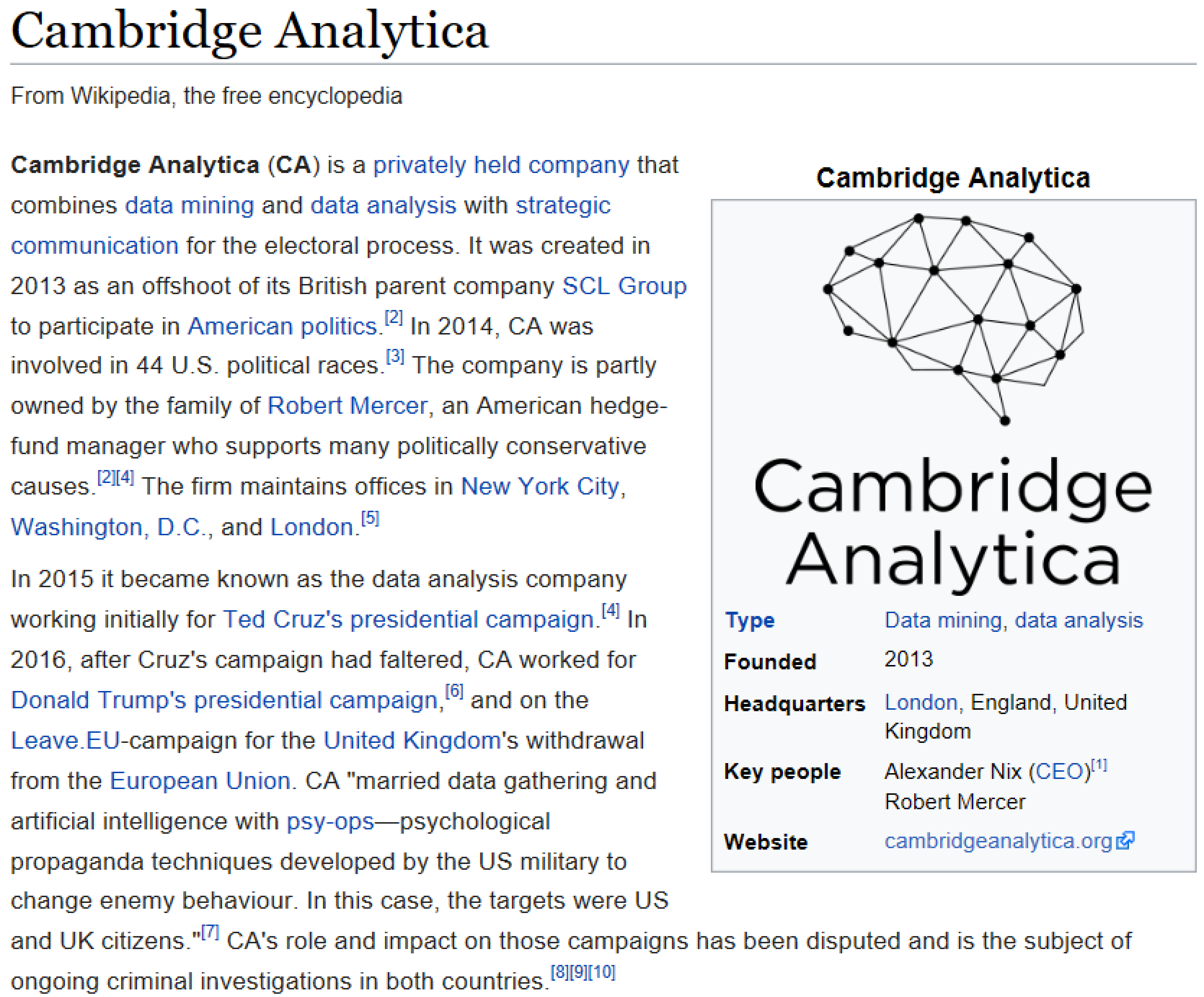
acxiom

The World's Most Advanced Omnichannel Identity Graph

We recognize consumers across offline and digital touchpoints at scale in a privacy-compliant way, enabling you to gain the most comprehensive, omnichannel understanding of your customers.

Data in diagram is fictional - for illustrative purposes only.

Acxiom's customers include "47 *Fortune* 100 clients; 12 of the top 15 credit card issuers; seven of the top 10 retail banks; eight of the top 10 telecom/media companies; seven of the top 10 retailers; 11 of the top 14 automotive manufacturers; six of the top 10 brokerage firms; three of the top 10 pharmaceutical manufacturers; five of the top 10 life/health insurance providers; nine of the top 10 property and casualty insurers; eight of the top 10 lodging companies; two of the top three gaming companies; three of the top five domestic airlines; six of the top 10 U.S. hotels." U.S. Senate Commerce Committee, A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes (December 2013) ("Rockefeller Report")



Cambridge Analytica

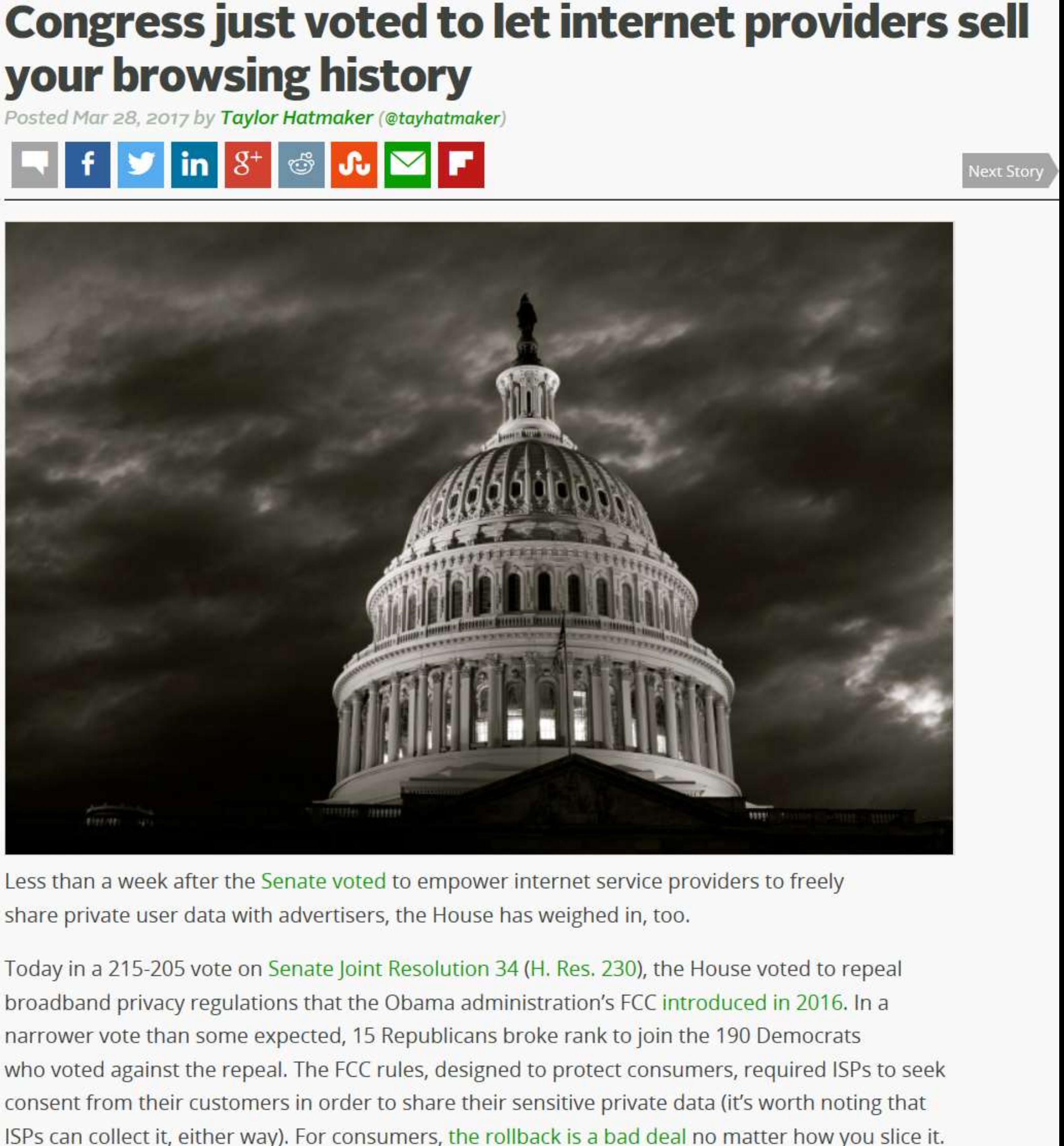
From Wikipedia, the free encyclopedia

Cambridge Analytica (**CA**) is a privately held company that combines data mining and data analysis with strategic communication for the electoral process. It was created in 2013 as an offshoot of its British parent company SCL Group to participate in American politics.[2] In 2014, CA was involved in 44 U.S. political races.[3] The company is partly owned by the family of Robert Mercer, an American hedge-fund manager who supports many politically conservative causes.[2][4] The firm maintains offices in New York City, Washington, D.C., and London.[5]

In 2015 it became known as the data analysis company working initially for Ted Cruz's presidential campaign.[4] In 2016, after Cruz's campaign had faltered, CA worked for Donald Trump's presidential campaign,[6] and on the Leave.EU-campaign for the United Kingdom's withdrawal from the European Union. CA "married data gathering and artificial intelligence with psy-ops—psychological propaganda techniques developed by the US military to change enemy behaviour. In this case, the targets were US and UK citizens."[7] CA's role and impact on those campaigns has been disputed and is the subject of ongoing criminal investigations in both countries.[8][9][10]

Cambridge Analytica

Type	Data mining, data analysis
Founded	2013
Headquarters	London, England, United Kingdom
Key people	Alexander Nix (CEO)[1] Robert Mercer
Website	cambridgeanalytica.org



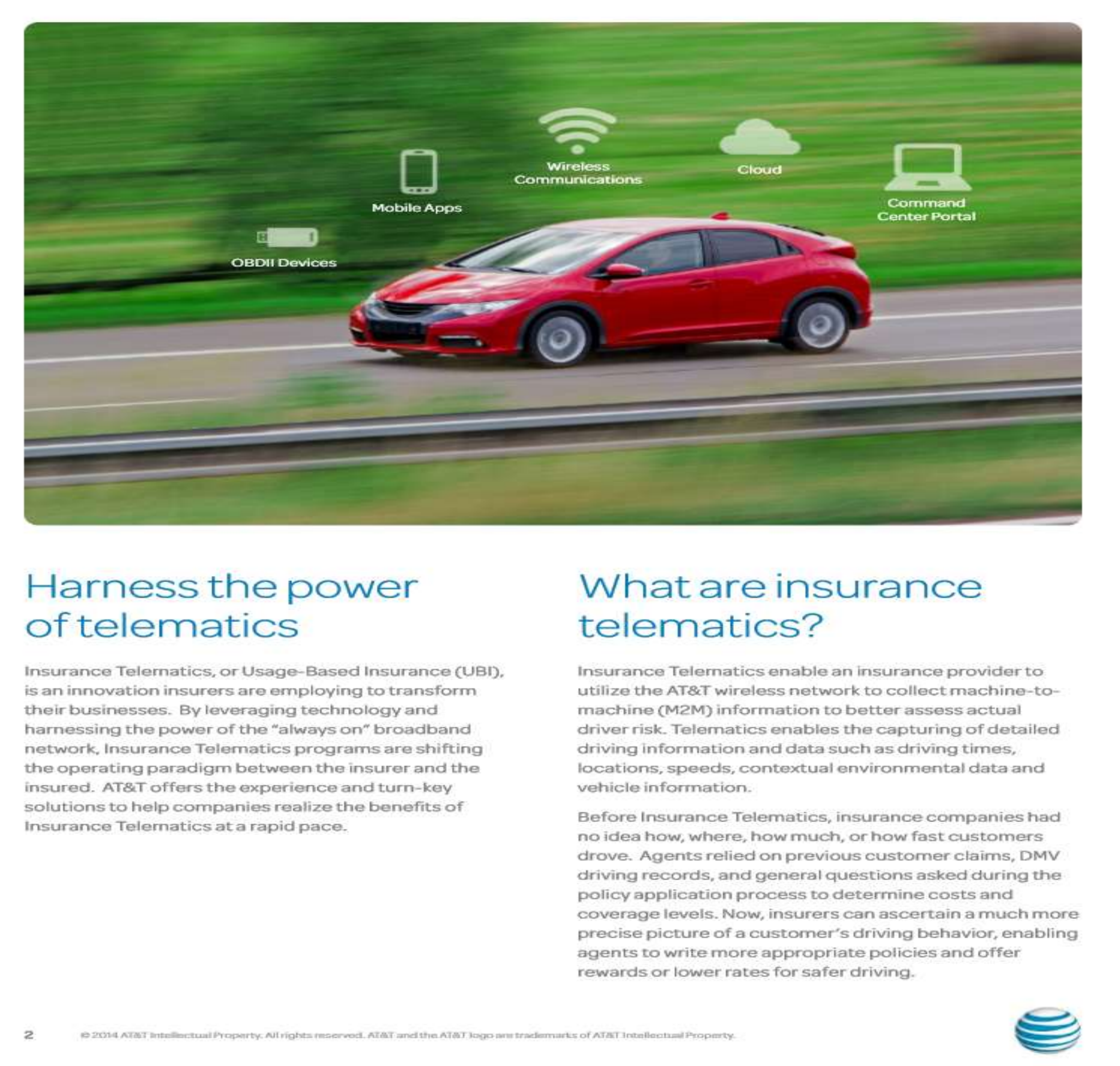
Congress just voted to let internet providers sell your browsing history

Posted Mar 28, 2017 by Taylor Hatmaker (@tayhatmaker)

Less than a week after the Senate voted to empower internet service providers to freely share private user data with advertisers, the House has weighed in, too.

Today in a 215-205 vote on Senate Joint Resolution 34 (H. Res. 230), the House voted to repeal broadband privacy regulations that the Obama administration's FCC introduced in 2016. In a narrower vote than some expected, 15 Republicans broke rank to join the 190 Democrats who voted against the repeal. The FCC rules, designed to protect consumers, required ISPs to seek consent from their customers in order to share their sensitive private data (it's worth noting that ISPs can collect it, either way). For consumers, the rollback is a bad deal no matter how you slice it.

See more:
https://www.alternet.org/civil-liberties/how-telecoms-sell-your-private-info-highest-bidder


Wireless Communications
Cloud
Mobile Apps
Command Center Portal
OBDII Devices

Harness the power of telematics

Insurance Telematics, or Usage-Based Insurance (UBI), is an innovation insurers are employing to transform their businesses. By leveraging technology and harnessing the power of the "always on" broadband network, Insurance Telematics programs are shifting the operating paradigm between the insurer and the insured. AT&T offers the experience and turn-key solutions to help companies realize the benefits of Insurance Telematics at a rapid pace.

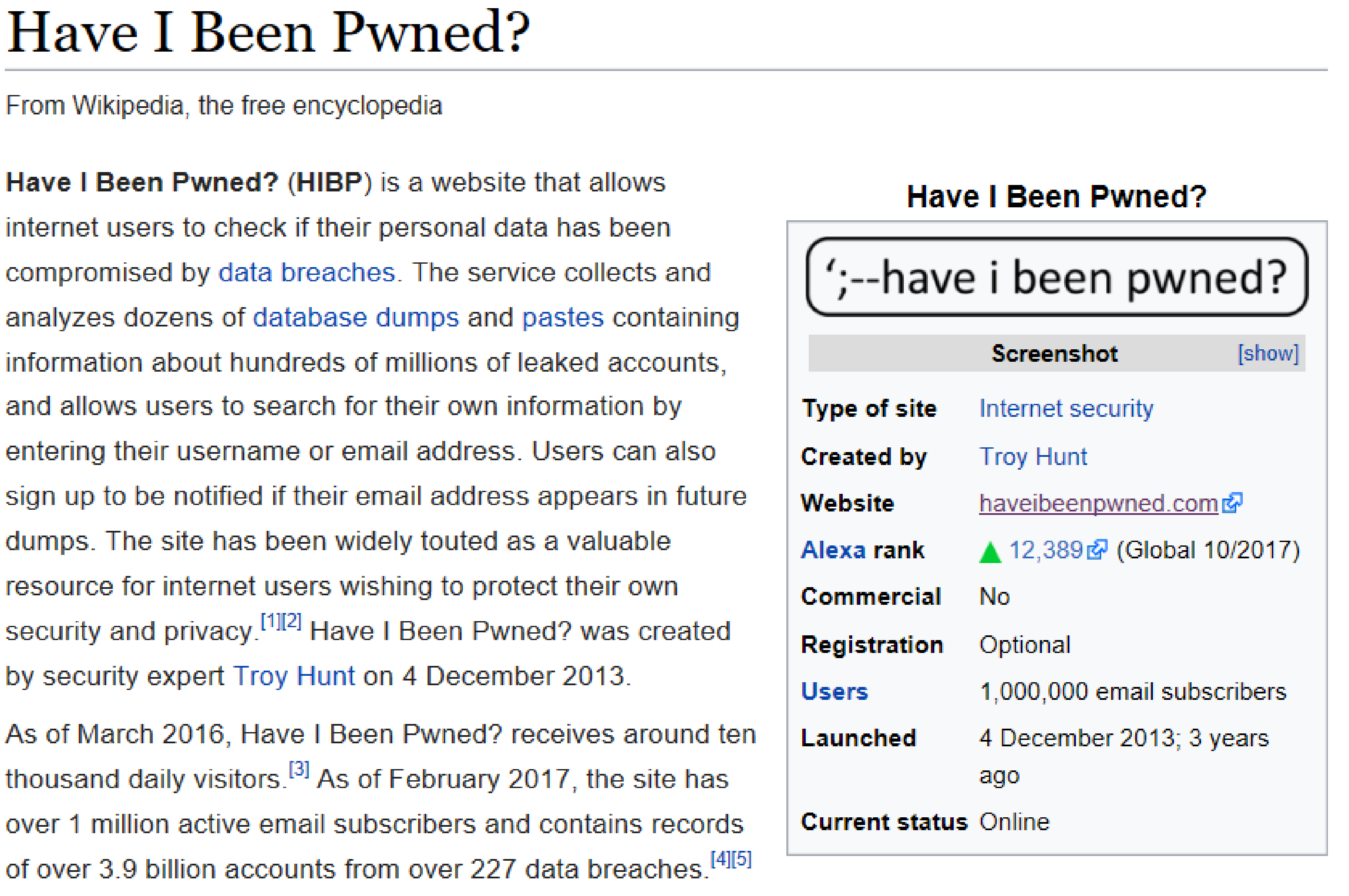
What are insurance telematics?

Insurance Telematics enable an insurance provider to utilize the AT&T wireless network to collect machine-to-machine (M2M) information to better assess actual driver risk. Telematics enables the capturing of detailed driving information and data such as driving times, locations, speeds, contextual environmental data and vehicle information.

Before Insurance Telematics, insurance companies had no idea how, where, how much, or how fast customers drove. Agents relied on previous customer claims, DMV driving records, and general questions asked during the policy application process to determine costs and coverage levels. Now, insurers can ascertain a much more precise picture of a customer's driving behavior, enabling agents to write more appropriate policies and offer rewards or lower rates for safer driving.

© 2014 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.

- One of the most intriguing areas in which wireless companies are working with third parties involves auto insurance.
- This may explain why AT&T conducted such extensive research into subscribers' mobility habits. Sprint recently established the Integrated Insurance Solutions unit offering "usage-based insurance" data.
- Sprint is working with Allstate's unit, Esurance, on a pilot program in Arizona and Texas. It offers insurance companies a turnkey tracking solution, including the on-board car tracking device, the wireless connectivity to capture, send and record the data, and the program to evaluate the driver's performance.



Have I Been Pwned?

From Wikipedia, the free encyclopedia

Have I Been Pwned? (**HIBP**) is a website that allows internet users to check if their personal data has been compromised by data breaches. The service collects and analyzes dozens of database dumps and pastes containing information about hundreds of millions of leaked accounts, and allows users to search for their own information by entering their username or email address. Users can also sign up to be notified if their email address appears in future dumps. The site has been widely touted as a valuable resource for internet users wishing to protect their own security and privacy.[1][2] Have I Been Pwned? was created by security expert Troy Hunt on 4 December 2013.

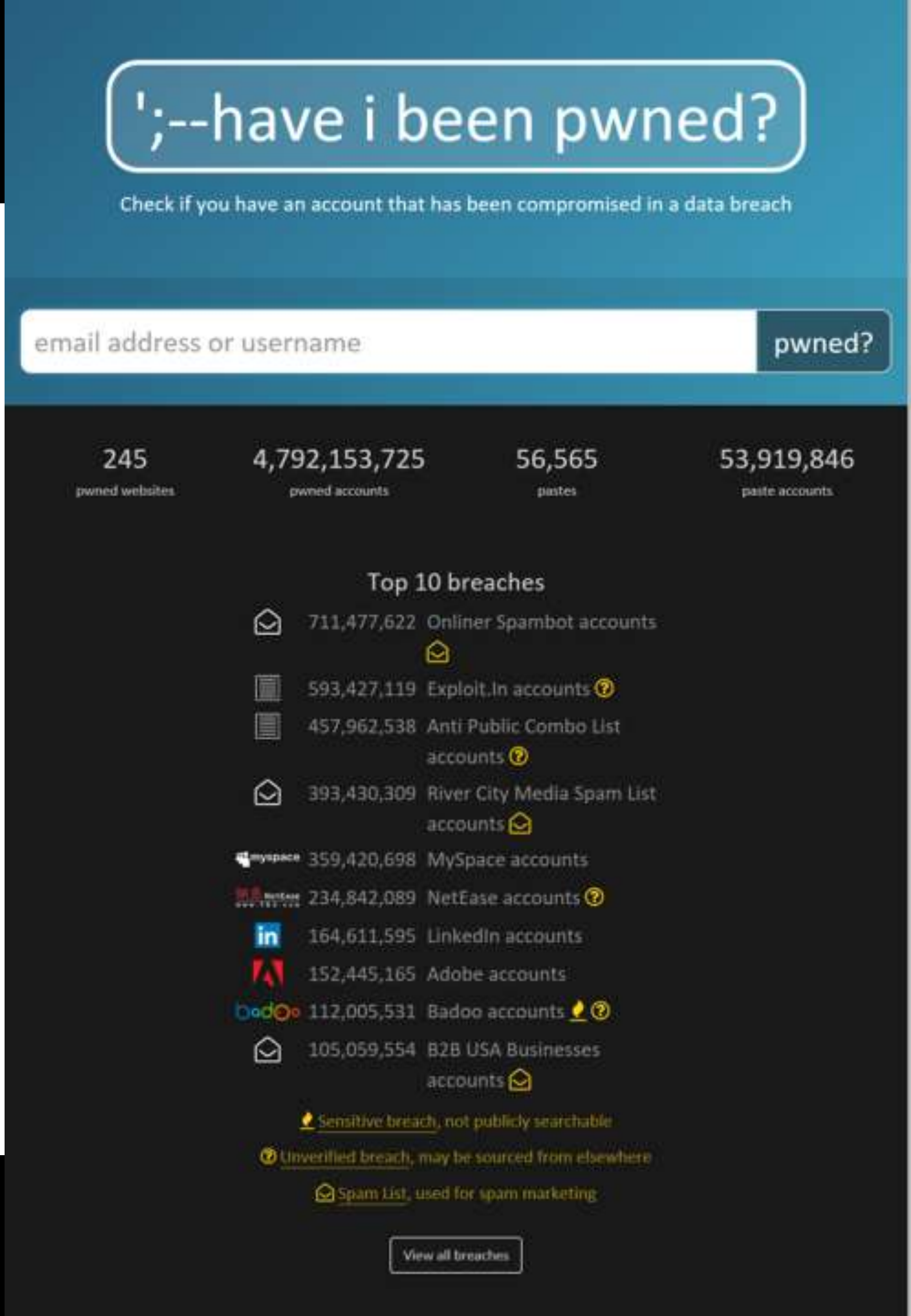
As of March 2016, Have I Been Pwned? receives around ten thousand daily visitors.[3] As of February 2017, the site has over 1 million active email subscribers and contains records of over 3.9 billion accounts from over 227 data breaches.[4][5]

Have I Been Pwned?

';--have i been pwned?

Screenshot [show]

Type of site	Internet security
Created by	Troy Hunt
Website	haveibeenpwned.com
Alexa rank	▲ 12,389 (Global 10/2017)
Commercial	No
Registration	Optional
Users	1,000,000 email subscribers
Launched	4 December 2013; 3 years ago
Current status	Online



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username | pwned?

245	4,792,153,725	56,565	53,919,846
pwned websites	pwned accounts	pastes	paste accounts

Top 10 breaches

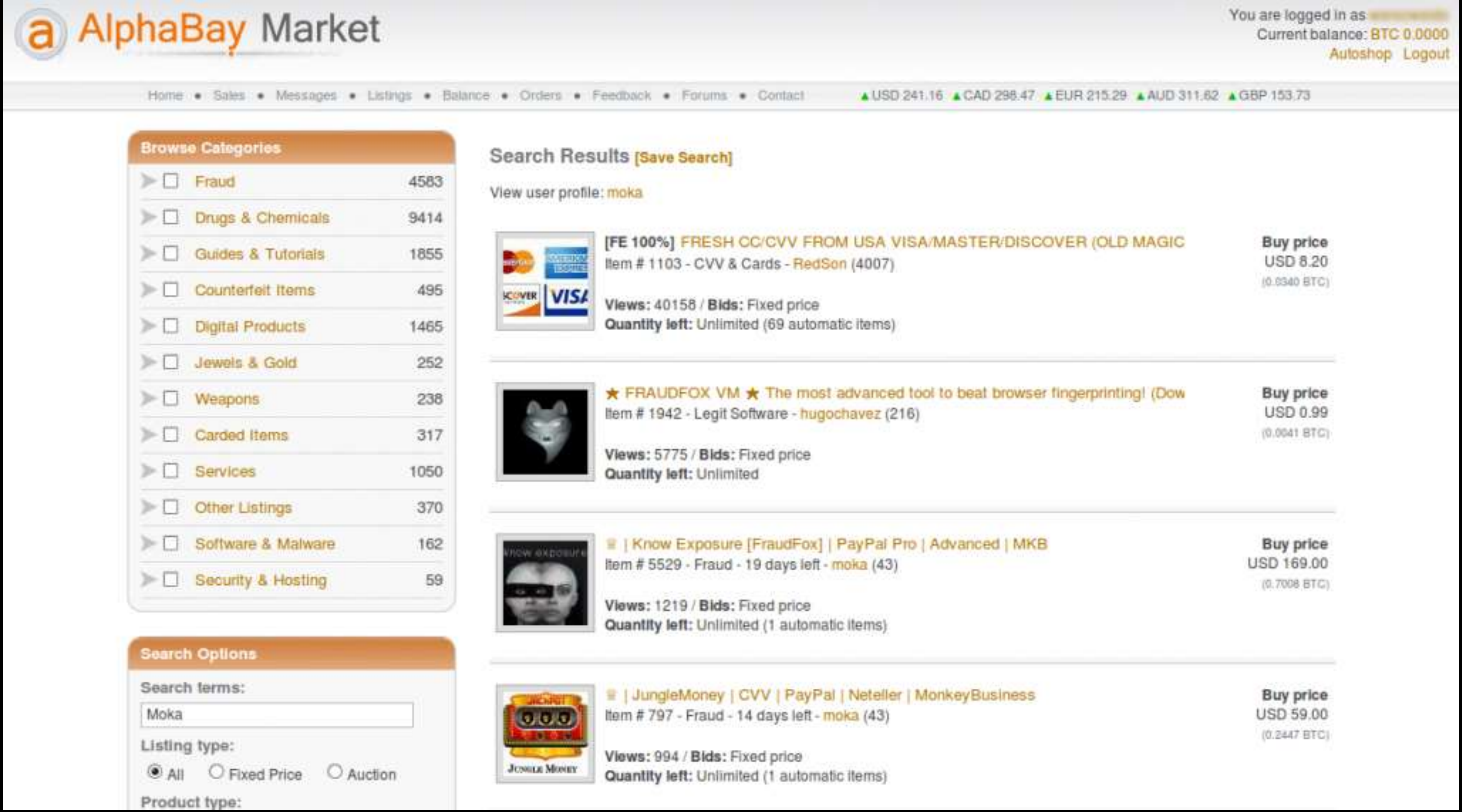
✉	711,477,622	Onliner Spambot accounts ✉
▤	593,427,119	Exploit.In accounts ?
▤	457,962,538	Anti Public Combo List accounts ?
✉	393,430,309	River City Media Spam List accounts ✉
myspace	359,420,698	MySpace accounts
NetEase	234,842,089	NetEase accounts ?
in	164,611,595	LinkedIn accounts
A	152,445,165	Adobe accounts
badoo	112,005,531	Badoo accounts 💧 ?
✉	105,059,554	B2B USA Businesses accounts ✉

💧 Sensitive breach, not publicly searchable

? Unverified breach, may be sourced from elsewhere

✉ Spam List, used for spam marketing

View all breaches



AlphaBay Market

You are logged in as [redacted]
Current balance: BTC 0.0000
Autoshop Logout

Home • Sales • Messages • Listings • Balance • Orders • Feedback • Forums • Contact ▲USD 241.16 ▲CAD 298.47 ▲EUR 215.29 ▲AUD 311.62 ▲GBP 153.73

Browse Categories

□ Fraud	4583
□ Drugs & Chemicals	9414
□ Guides & Tutorials	1855
□ Counterfeit Items	495
□ Digital Products	1465
□ Jewels & Gold	252
□ Weapons	238
□ Carded Items	317
□ Services	1050
□ Other Listings	370
□ Software & Malware	162
□ Security & Hosting	59

Search Options

Search terms: Moka

Listing type:
● All ○ Fixed Price ○ Auction

Product type:

Search Results [Save Search]

View user profile: moka

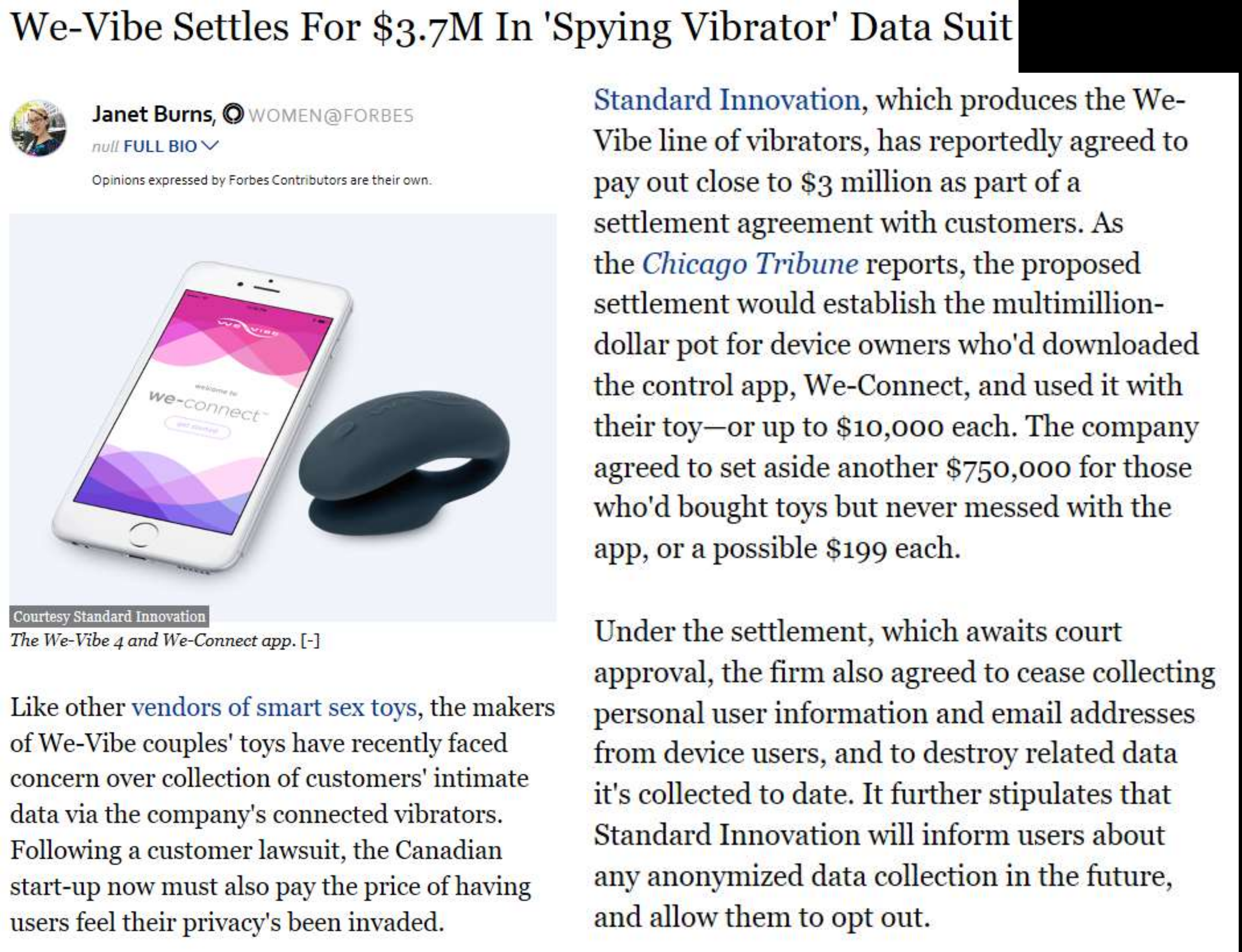
[FE 100%] FRESH CC/CVV FROM USA VISA/MASTER/DISCOVER (OLD MAGIC
Item # 1103 - CVV & Cards - RedSon (4007)
Views: 40158 / **Bids:** Fixed price
Quantity left: Unlimited (69 automatic items)
Buy price USD 8.20 (0.0340 BTC)

★ FRAUDFOX VM ★ The most advanced tool to beat browser fingerprinting! (Dow
Item # 1942 - Legit Software - hugochavez (216)
Views: 5775 / **Bids:** Fixed price
Quantity left: Unlimited
Buy price USD 0.99 (0.0041 BTC)

| Know Exposure [FraudFox] | PayPal Pro | Advanced | MKB
Item # 5529 - Fraud - 19 days left - moka (43)
Views: 1219 / **Bids:** Fixed price
Quantity left: Unlimited (1 automatic items)
Buy price USD 169.00 (0.7008 BTC)

| JungleMoney | CVV | PayPal | Neteller | MonkeyBusiness
Item # 797 - Fraud - 14 days left - moka (43)
Views: 994 / **Bids:** Fixed price
Quantity left: Unlimited (1 automatic items)
Buy price USD 59.00 (0.2447 BTC)

Compromised Data is Bought and Sold on the Dark Web



We-Vibe Settles For $3.7M In 'Spying Vibrator' Data Suit

Janet Burns, WOMEN@FORBES

null FULL BIO

Opinions expressed by Forbes Contributors are their own.

Courtesy Standard Innovation

The We-Vibe 4 and We-Connect app. [-]

Like other vendors of smart sex toys, the makers of We-Vibe couples' toys have recently faced concern over collection of customers' intimate data via the company's connected vibrators. Following a customer lawsuit, the Canadian start-up now must also pay the price of having users feel their privacy's been invaded.

Standard Innovation, which produces the We-Vibe line of vibrators, has reportedly agreed to pay out close to $3 million as part of a settlement agreement with customers. As the *Chicago Tribune* reports, the proposed settlement would establish the multimillion-dollar pot for device owners who'd downloaded the control app, We-Connect, and used it with their toy—or up to $10,000 each. The company agreed to set aside another $750,000 for those who'd bought toys but never messed with the app, or a possible $199 each.

Under the settlement, which awaits court approval, the firm also agreed to cease collecting personal user information and email addresses from device users, and to destroy related data it's collected to date. It further stipulates that Standard Innovation will inform users about any anonymized data collection in the future, and allow them to opt out.

"It [the data] gives us a general sense of users' [vibration] intensity levels, steadiness of mode, and whether we're marketing to the right people."

roughly 300,000 have bought We-Vibe devices that are covered by the settlement, while closer to 100,000 downloaded and used the company's corresponding app.

S.2986 -International Communications Privacy Act

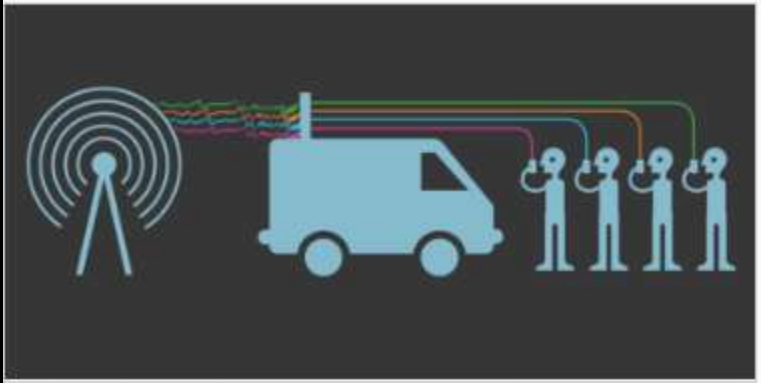
Introduced in Senate (05/25/2016)
Latest Action:
Senate - 05/25/2016 Read twice and referred to the Committee on the Judiciary

This bill amends the federal criminal code by **allowing a governmental entity to require providers of electronic communication services or remote computing services to disclose the contents of communications in electronic storage (e.g., the cloud), regardless of where those communications are located.** Thus, a governmental entity may obtain a warrant for electronic communications stored outside of the United States if certain conditions for obtaining the warrant are met.

The bill allows a governmental entity to obtain those communications only if a court finds that the governmental entity has taken all reasonable steps to establish the nationality and location of the subscriber or customer whose communications are sought and that there are reasonable grounds to believe that such subscriber or customer is a U.S. person, a person physically located within the United States, or a national of a foreign country that has a law enforcement cooperation agreement with the United States.

The Department of Justice must: (1) establish a process for foreign governments to file mutual legal assistance treaty requests for obtaining access to electronic communications, and (2) publish annually information concerning those requests.

The StingRay is an IMSI-catcher, a controversial cellular phone surveillance device, manufactured by Harris Corporation.[2] Initially developed for the military and intelligence community, the StingRay and similar Harris devices are in widespread use by local and state law enforcement agencies across Canada,[3] the United States,[4][5] and in the United Kingdom.[6][7] Stingray has also become a generic name to describe these kinds of devices.[



When operating in active mode, the Stingray device mimics a wireless carrier cell tower in order to force all nearby mobile phones and other cellular data devices to connect to it.

A Stingray device in 2013, in Harris's trademark submission.[1]

6/5/2017 – The Supreme Court will review United States v. Carpenter, a case involving long-term, retrospective tracking of a person’s movements using information generated by his cell phone. This is very exciting news in the world of digital privacy. With Carpenter, the Court has an opportunity to continue its recent pattern of applying Fourth Amendment protections to sensitive digital data. It may also limit or even reevaluate the so-called “Third Party Doctrine,” which the government relies on to justify warrantless tracking and surveillance in a variety of contexts. EFF filed an amicus brief urging the Supreme Court to take Carpenter and a related case, so we’re hopeful the Court will rule in favor of strong constitutional protections.

Blockchain Technology - TL;DR

Blockchain is a ledger of transactions that everyone owns and contributes to.

Bitcoin is a digital currency with a fixed supply built on blockchain technology, and has a few nice features that people like so they give it value.

Ethereum is a platform that lets anyone build "decentralized applications" on top of their blockchain technology, and runs on its own currency called Ether.

A "block" is just a bundle of transactions. A "hash function" is an algorithm that takes any data of any size, and spits out a constant length seemingly random alphanumeric string. It is a one way function (it is easy to get the hash from the data, but you can't go backwards from the hash to find out the data), and it is unpredictable (changing the input data even slightly, changes the hash completely). Bitcoin miners take the data comprised of a whole bunch of transactions and run the hashing function trillions of times a second to find the hash that is below a target value (they add a random number called a nonce at every attempt, to get a different hash). Once the right hash value is found, the block is added to the blockchain. Each block includes the hash of the previous block in its data, along with the bundle of transactions, and that is the way blocks are chained together. So to change a block, you would have to re-calculate the the hash of every subsequent block, which is very computationally intensive and becomes impossible once you are a few blocks deep.

Bitcoins are long hashes of random numbers and letters that computers try to guess. These computers are called miners. **Miners** will guess hashes to mine blocks of Bitcoins. **Blocks** consist of 50 Bitcoins, as well as recent transactions that occur between wallets. The blocks are collectively known as the blockchain. The **blockchain** contains the entire, detailed history of every transaction that has occurred in the bitcoin network between wallets, since its creation. **Wallets** send and recieve Bitcoins, and look like this 19UJAQMPqxDqhkppwzd1YFtfTbLiX3rjJ9
The entire network of Bitcoin miners set the **difficulty**, or how hard it is for a miner to guess a hash correctly, to ensure that blocks are created predictably (about every 10 minutes). Each subsequent creation of blocks **confirms** the last block, so as to prevent double spending. A transaction of Bitcoins between wallets needs 6 confirmations in order to be considered valid. A block of 50 Bitcoins needs 120 confirmations in order to be considered valid.
They have value just like anything else would. They are a thing, and there is demand for them. For example, a group of people start collecting shiny rocks and exchanging them for goods. There is a demand for shiny rocks, and they now have a price.

Blockchain Applications

- Distributed Cloud Storage
- Decentralized Notary
- Digital Voting
- Smart Contracts
  - 3p ‘Oracles’
- Digital Identity
  - Passports
  - E-Residency
  - Birth Certificates
  - Wedding Certificates
  - IDs

Oracles

Some smart contracts systems, including the one built into Bitcoin, are strictly deterministic. In order to interact with the real world, these systems rely on cryptographic signatures submitted by outside systems called "oracles."

Oracles are trusted entities which sign claims about the state of the world. Since the verification of signatures can be done deterministically, it allows deterministic smart contracts to react to the (non-deterministic) outside world.

Benefits:

Limit Personal Liability

Good Luck Serving a Subpoena on a Smart Piece of Code!

Oracle contracts:

- The main limitations to what can be done with smart contracts is that a computer program cannot easily and reliably tell what is happening in the physical world or who is telling the truth. Checking whether a bitcoin payment has been made is a simple task which is suitable for a computer program to do, but most real-world contracts and situations (for example: was a product really delivered to someone? Did a freelancer deliver work that met the company's stated requirements?) are much harder for a computer program to evaluate.
- A smart contract's execution is only as good as the inputs it takes in, and it may be difficult to find inputs which are sufficient to the job which both parties trust. One solution to this is to have oracles – online services providers whose job is to broadcast data which can be used as inputs by smart contract makers.
- For example, an oracle may broadcast new entires on the government registry of deaths, to be used by contracts executing wills, or the results of a football match, to be used in settling gambling bets. This method is used by Ripple's Codius smart contracting platform

September 12, 2017 **Yelp alleges Google Broke Promise Made to FTC to not Scrape its content as part of Anti Trust Settlement**

The assertion intensifies Yelp's criticism that Google unfairly uses its influence to stifle competition

Yelp Inc. said in a letter to Federal Trade Commission Chairwoman Maureen Ohlhausen that Google is using Yelp photos for local-business listings in its search results, despite Yelp's formal request that Google not pull such content from its site.

As part of a December 2012 settlement to end an FTC investigation into Google, the tech giant agreed to not use content, including photos and user reviews, from third-party sites that opted out of such scraping. Google's commitment lasts through 2017 and applies to a variety of its products, including its local-business listings.

The FTC has said that it would penalize the company if it doesn't comply with the 2012 settlement

In 2013, the European Union fined Microsoft Corp. $731 million for breaking its promise to regulators there to offer consumers a choice of web browsers.

Browser Fingerprinting

Resource: https://amiunique.org/

What is browser fingerprinting?

Device fingerprinting or browser fingerprinting is the systematic collection of information about a remote device, for identification purposes. Client-side scripting languages allow the development of procedures to collect very rich fingerprints: browser and operating system type and version, screen resolution, architecture type, lists of fonts, plugins, microphone, camera, etc.

- On this site, we collect:
- the User agent header
- the Accept header
- the Connection header
- the Encoding header
- the Language header
- the list of plugins
- the platform
- the cookies preferences (allowed or not)
- the Do Not Track preferences (yes, no or not communicated)
- the timezone
- the screen resolution and its color depth
- the use of local storage
- the use of session storage
- a picture rendered with the HTML Canvas element
- a picture rendered with WebGL
- the presence of AdBlock
- the list of fonts

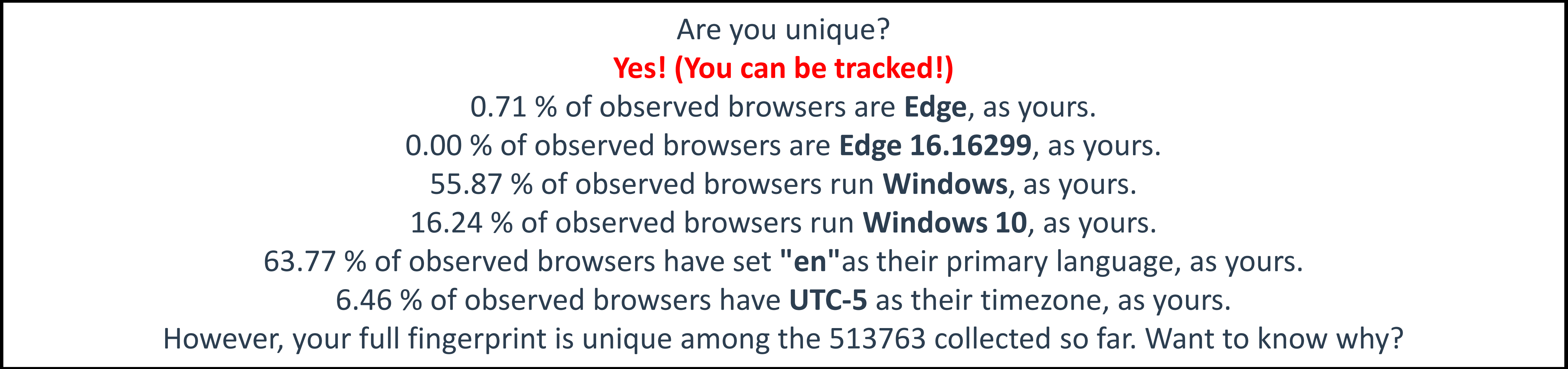
How are the fingerprints exploited?

Like all tracking technology, it is a double-edge sword.

Fingerprints can be used in a constructive way to combat fraud or credential hijacking, by checking that a user who logs into a specific site is likely the legitimate user.

Fingerprints can also be used in more questionable way, in order to track users across web sites and collect information about their habits and their tastes without the users knowing about it. - this type of digital forensics may be used to link a suspect to a crime

Fingerprints can even be used in a destructive way: if attackers know which software modules (specific browser version, plugins, etc.) are installed on a specific device, they can deliver exploits that are tailored for these specific modules or combination of modules.



Are you unique?

Yes! (You can be tracked!)

0.71 % of observed browsers are **Edge**, as yours.

0.00 % of observed browsers are **Edge 16.16299**, as yours.

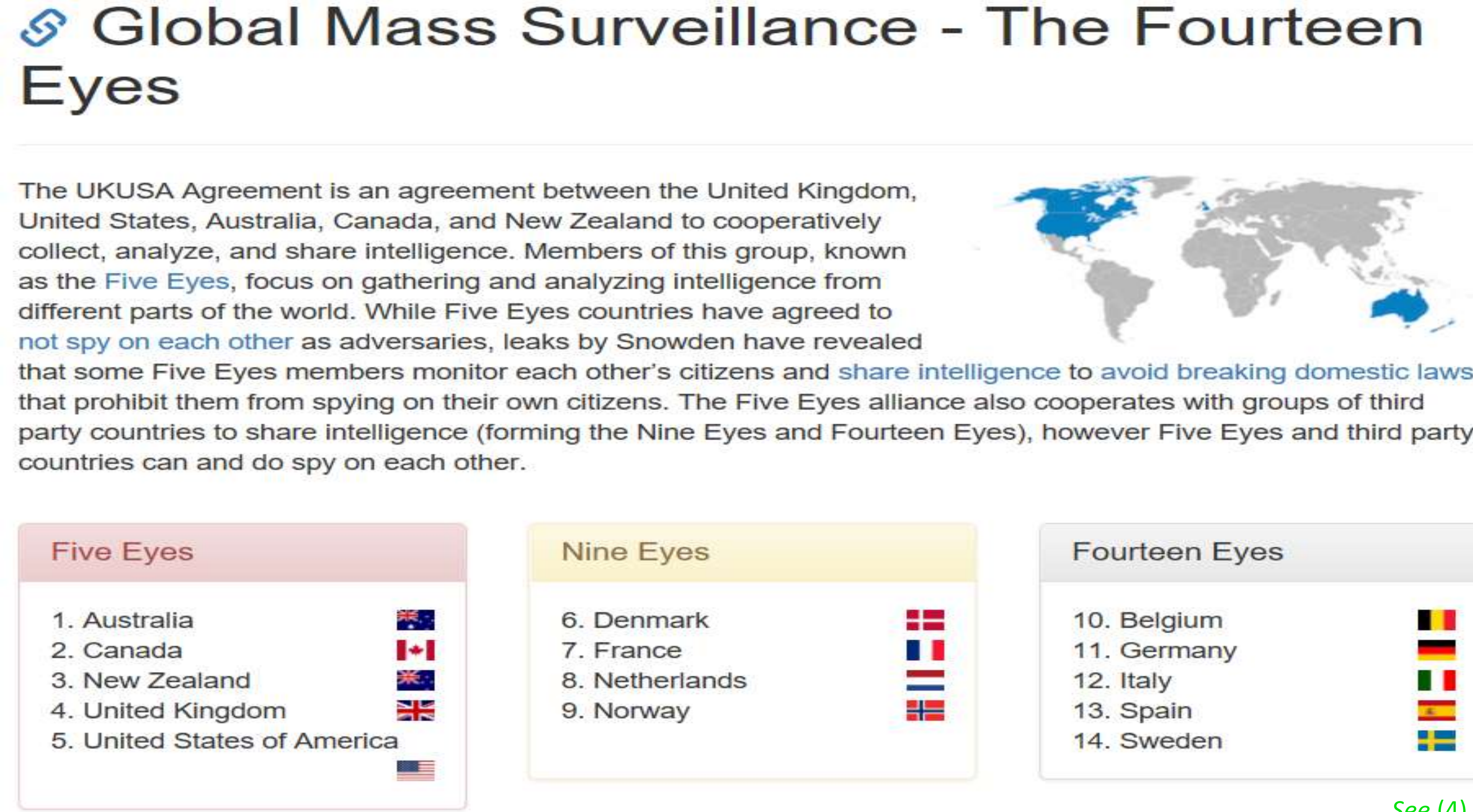
55.87 % of observed browsers run **Windows**, as yours.

16.24 % of observed browsers run **Windows 10**, as yours.

63.77 % of observed browsers have set **"en"**as their primary language, as yours.

6.46 % of observed browsers have **UTC-5** as their timezone, as yours.

However, your full fingerprint is unique among the 513763 collected so far. Want to know why?



Global Mass Surveillance - The Fourteen Eyes

The UKUSA Agreement is an agreement between the United Kingdom, United States, Australia, Canada, and New Zealand to cooperatively collect, analyze, and share intelligence. Members of this group, known as the Five Eyes, focus on gathering and analyzing intelligence from different parts of the world. While Five Eyes countries have agreed to not spy on each other as adversaries, leaks by Snowden have revealed that some Five Eyes members monitor each other's citizens and share intelligence to avoid breaking domestic laws that prohibit them from spying on their own citizens. The Five Eyes alliance also cooperates with groups of third party countries to share intelligence (forming the Nine Eyes and Fourteen Eyes), however Five Eyes and third party countries can and do spy on each other.

Five Eyes

1. Australia
2. Canada
3. New Zealand
4. United Kingdom
5. United States of America

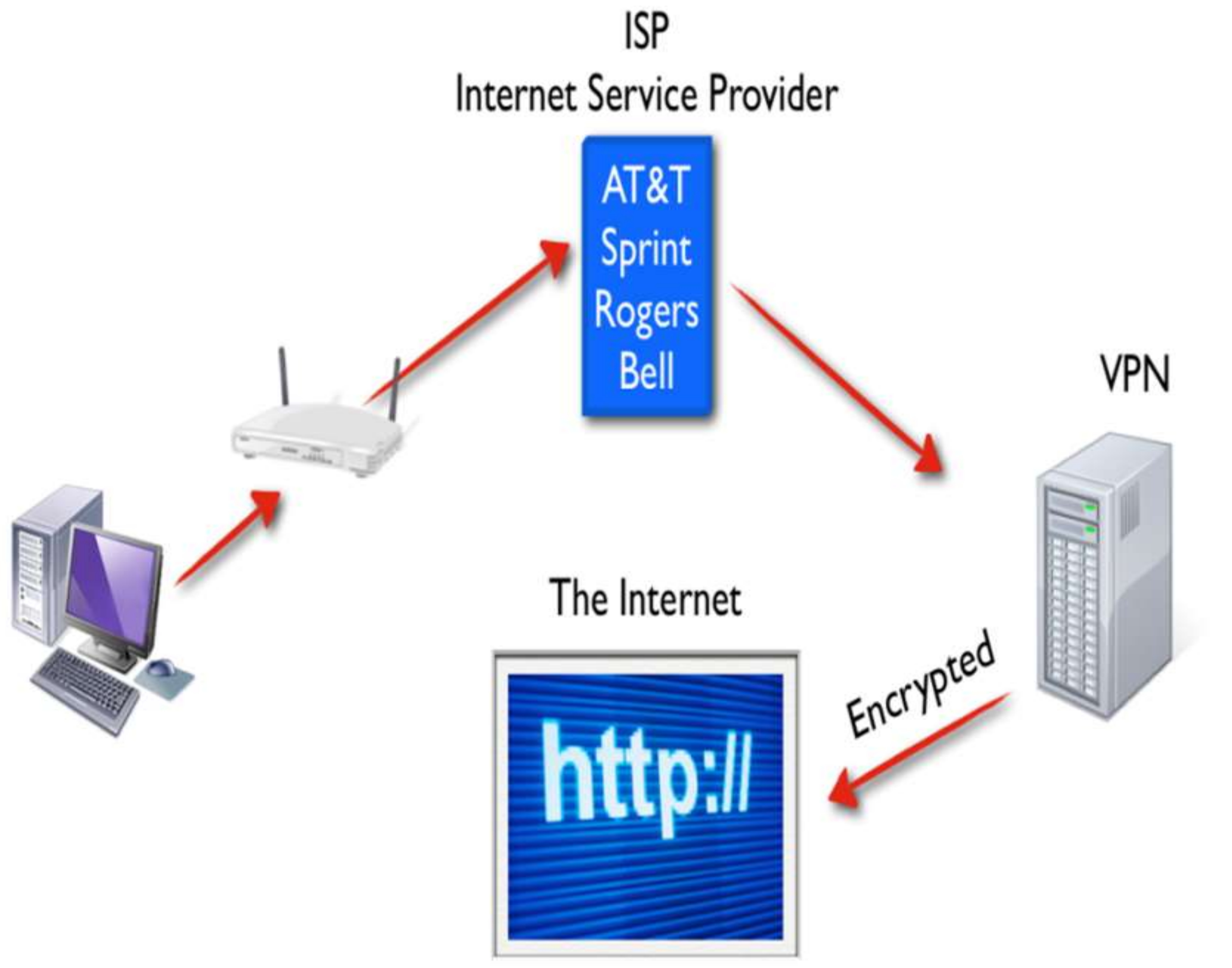
Nine Eyes

6. Denmark
7. France
8. Netherlands
9. Norway

Fourteen Eyes

10. Belgium
11. Germany
12. Italy
13. Spain
14. Sweden

See (4)



Solution:

Virtual Private Network

VNP Explained (as if you were a child):

You don't want the FBI to know you're talking to Billy, so you talk to John, who talks to Billy for you. When the FBI watches you, they see you talking to John. When they watch Billy, they see John talking to him. Since they never see you talking to Billy, they don't know you ever talked to him. Replace the people with computers, and that's how a VPN works.

Why is it not recommended to choose a US based service?

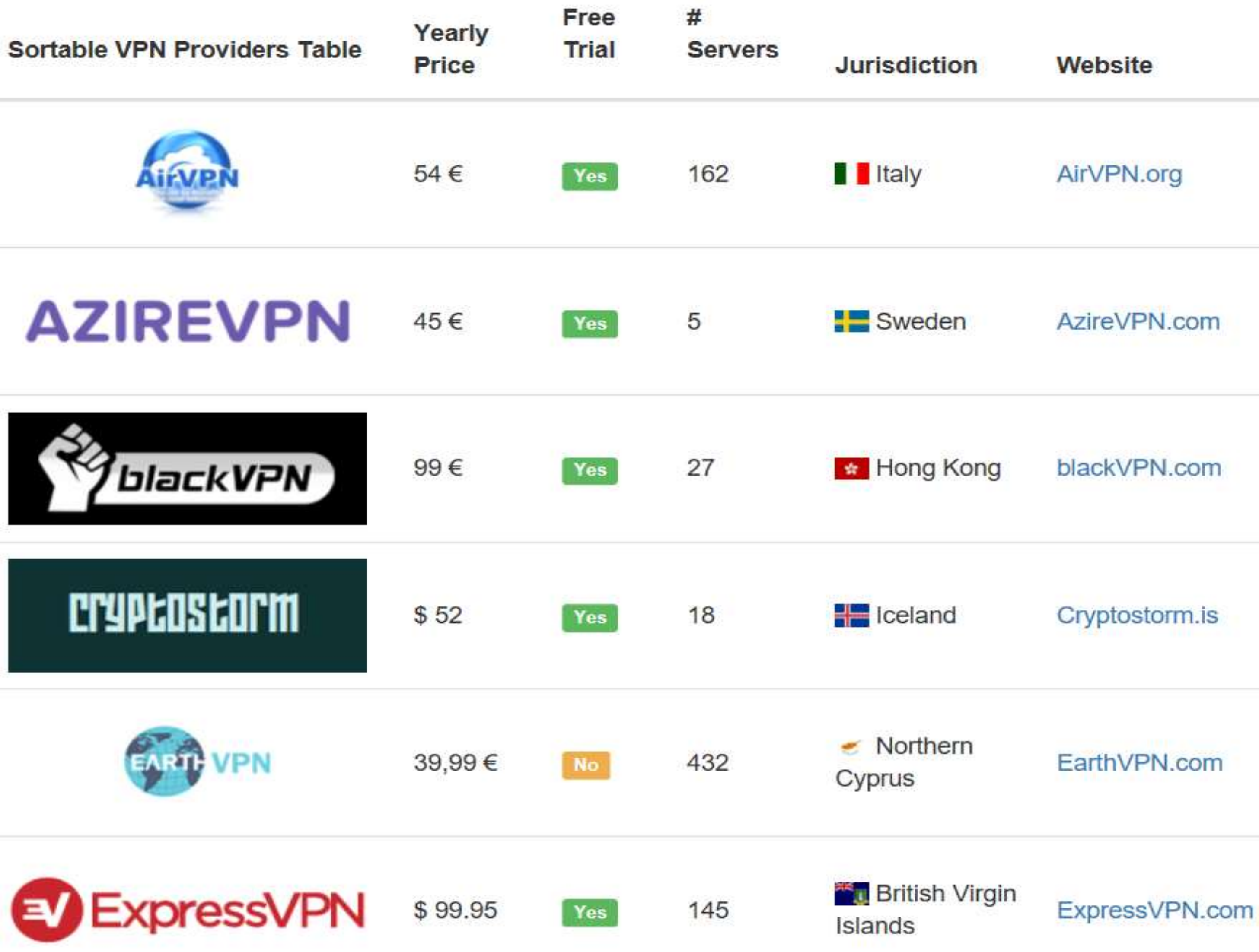
Services based in the United States are not recommended because of the country's surveillance programs, use of National Security Letters (NSLs) and accompanying gag orders, which forbid the recipient from talking about the request. This combination allows the government to secretly force companies to grant complete access to customer data and transform the service into a tool of mass surveillance.

An example of this is Lavabit – a discontinued secure email service created by Ladar Levison. The FBI requested Snowden's records after finding out that he used the service. Since Lavabit did not keep logs and email content was stored encrypted, the FBI served a subpoena (with a gag order) for the service's SSL keys. Having the SSL keys would allow them to access communications (both metadata and unencrypted content) in real time for all of Lavabit's customers, not just Snowden's.

Ultimately, Levison turned over the SSL keys and shut down the service at the same time. The US government then threatened Levison with arrest, saying that shutting down the service was a violation of the court order.

Our VPN Provider Criteria

- Operating outside the USA or other Five Eyes countries.
  More: Avoid all US and UK based services.
- OpenVPN software support.
- Accepts Bitcoin, cash, debit cards or cash cards as a payment method.
- No personal information is required to create an account. Only username, password and 🔗 Email.



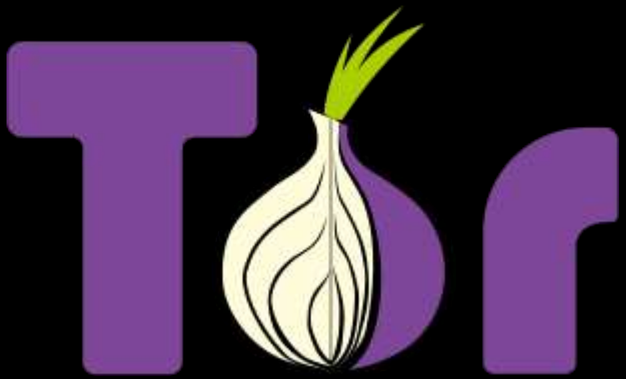
Sortable VPN Providers Table	Yearly Price	Free Trial	# Servers	Jurisdiction	Website
AirVPN	54 €	Yes	162	Italy	AirVPN.org
AZIREVPN	45 €	Yes	5	Sweden	AzireVPN.com
blackVPN	99 €	Yes	27	Hong Kong	blackVPN.com
cryptostorm	$ 52	Yes	18	Iceland	Cryptostorm.is
EARTH VPN	39,99 €	No	432	Northern Cyprus	EarthVPN.com
ExpressVPN	$ 99.95	Yes	145	British Virgin Islands	ExpressVPN.com

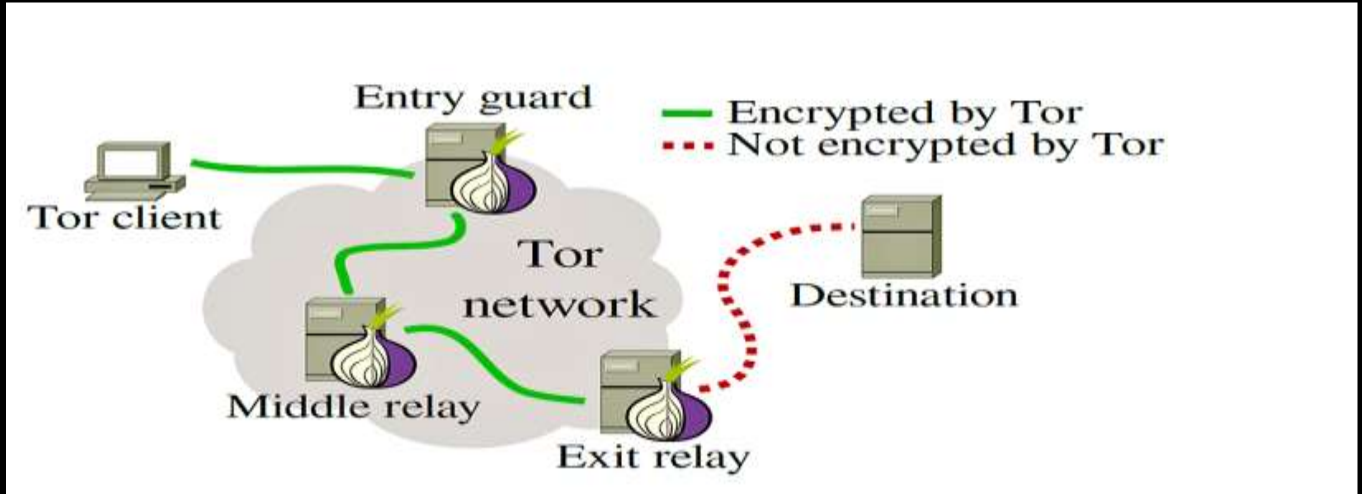
Onion routing is the method that is used by **Tor**, which is a program. It's named that because it has layers. Like an onion.

So how does it work? Let's say I want to access the website that's located at this server. My computer connects to another computer in the Tor network, which connects to another, and so on. Eventually, one of them will connect to the server, which can send back information using this pattern. However, none of the computers in the Tor network know who is getting what. The computer that you connect to isn't the same as the one that connected to the server, so it's very anonymous.

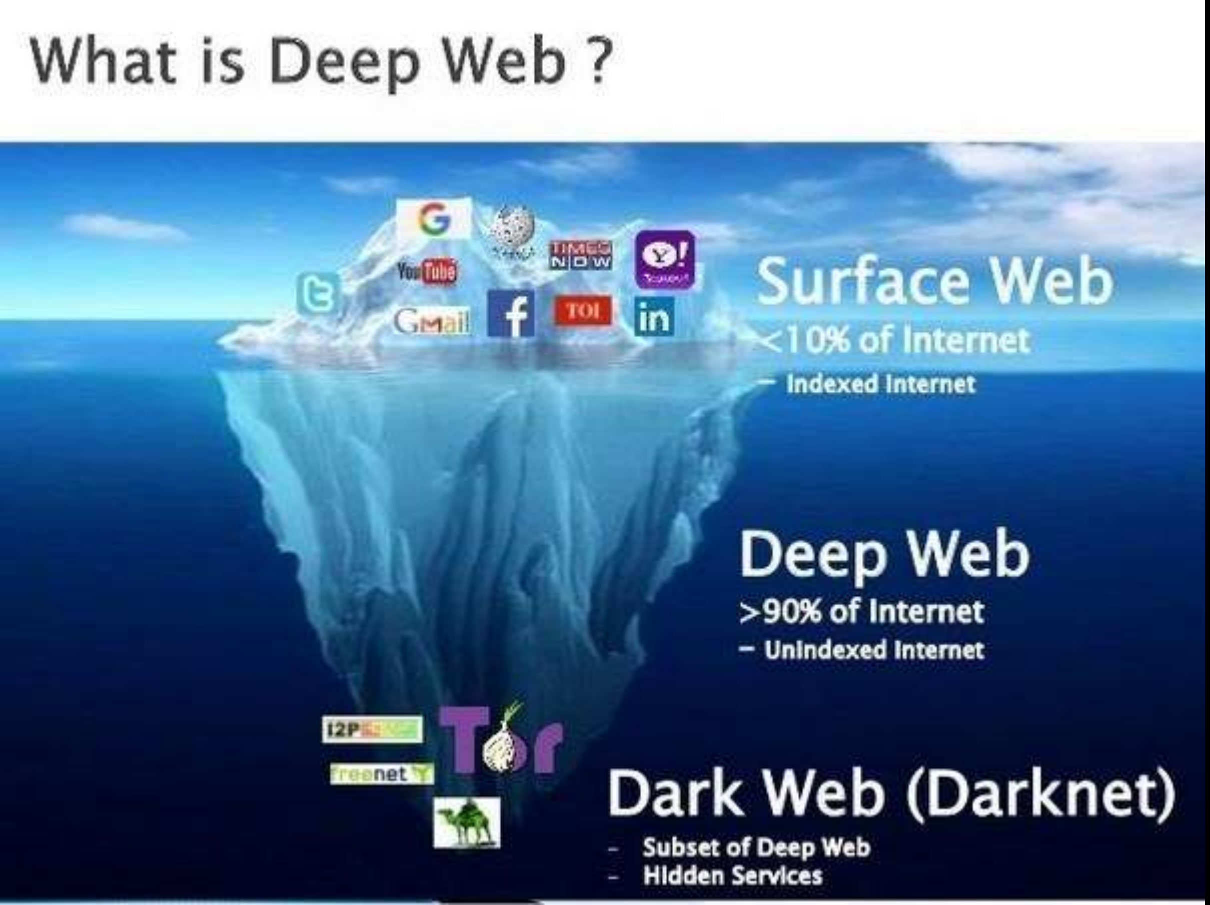
Another key feature is that the path of nodes used differs each time. The first time I visit a site, it might connect to computer B, then computer A, then computer J before connecting to the server. The next time, it might connect to computer F, then computer B, then computer L before getting the server. As a result, not only do none of the computers know who is viewing what, but the computers used change from time to time (about every ten minutes).

So why use Tor and onion routing? Simply because it's very, very anonymous. All the connections are encrypted and it would be nearly impossible to trace a user. It is, however, much slower than regular browsing, since we have to connect to all these computers in series.





The deep web refers to sites that aren't accessible via search engines. Since you couldn't find it via, say, Google normally, the site is as good as hidden from the eyes of normal people. This could mean that it's simply not linked to. Search engines follow links. If nothing links to a site, it as good as doesn't exist. There's also sites that instruct search engines specifically to not index them. Search engines have to follow a text file called "robots.txt", which tells what can and can't be indexed.



Much of the deep web is perfectly safe. Things like your facebook page might be hidden from search engines if you're underage or specified you didn't want it indexed. Likewise, most websites have deep web sections that are meant for administration, and thus not accessible by regular users. The dangerous part of the deep web include child pornography and black market services.

These sites use Tor as a hidden service, meaning they are a server connected to a Tor network, allowing them the same anonymity. Instead of hiding a user, the Tor network is now hiding a server

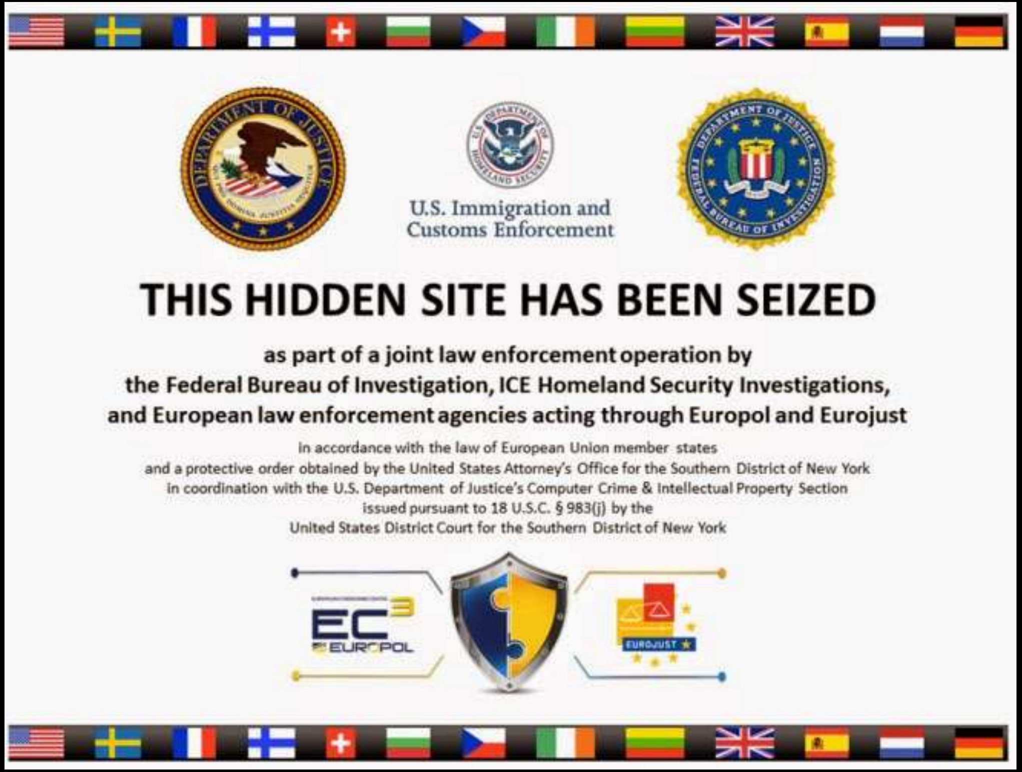
USA v. Jay Michaud

The Department of Justice filed a motion in Washington State federal court on Friday to dismiss its indictment against a child porn site. It wasn't for lack of evidence; it was because the FBI didn't want to disclose details of a hacking tool to the defense as part of discovery. Evidence in United States v. Jay Michaud hinged at least in part on information federal investigators had gathered by exploiting a vulnerability in the Tor anonymity network.

"Because the government remains unwilling to disclose certain discovery related to the FBI’s deployment of a 'Network Investigative Technique' ('NIT') as part of its investigation into the Playpen child pornography site, the government has no choice but to seek dismissal of the indictment," federal prosecutor Annette Hayes wrote in the court filing on Friday.

She noted that the DoJ's work to resist disclosing the NIT was part of "an effort to balance the many competing interests that are at play when sensitive law enforcement technology becomes the subject of a request for criminal discovery."

In other words, the feds are letting an alleged child pornographer free so that officials can potentially catch other dark-web using criminals in the future. *See* (9)



THIS HIDDEN SITE HAS BEEN SEIZED

as part of a joint law enforcement operation by
the Federal Bureau of Investigation, ICE Homeland Security Investigations,
and European law enforcement agencies acting through Europol and Eurojust

in accordance with the law of European Union member states
and a protective order obtained by the United States Attorney’s Office for the Southern District of New York
in coordination with the U.S. Department of Justice’s Computer Crime & Intellectual Property Section
issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

Michaud was listed as a special education teacher at Gaiser Middle School in Vancouver.

Allegedly, Michaud first signed on to an unidentified, hidden website in October 2014 under the username 'Pewter,' and viewed numerous threads containing child pornography.

Federal agents obtained a search warrant for Michaud's Vancouver home and confiscated a thumb drive that allegedly contained multiple images of child porn.

08.09.17 - Lawsuit claims Disney illegally collected data in kids apps

The suit names 42 apps that allegedly tracked and sold personal information.

The class action suit, brought forth by a California woman, claims that Disney and three software companies involved in the development of 42 youth-aimed apps have used software to track the apps' users online activity, which was subsequently sold to advertisers without consent of the parents.

The lawsuit points to a violation of the Children's Online Privacy Protection Act (COPPA) -- a 1999 law that requires parental consent before apps aimed at children under the age of 13 can collect personal data. Companies like Path, Yelp, Genesis Toys and even a Disney subsidiary have come under fire for violating COPPA laws.

In a statement Disney said, "Disney has a robust COPPA compliance program, and we maintain strict data collection and use policies for Disney apps created for children and families. The complaint is based on a fundamental misunderstanding of COPPA principles, and we look forward to defending this action in court.“

The plaintiffs in the case are seeking actual and statutory damages and punitive damages, which will be determined at trial, along with all trial-associated costs. They're also requesting an injunction of the practices and for the companies to sequester any illegally obtained data.

See (5)

30 Aug 2017 - **Francis Rawls**, a former sergeant in the Philadelphia police department, has spent nearly two years in prison for contempt of court after refusing to provide the passcode for two hard drives that were taken from his house in 2015 during an investigation into child abuse images.

Rawls claims he can't remember the passcode for the two drives, encrypted using Apple's FileVault system. The government says that he's stalling because he fears that the contents could see him in serious trouble with his former employers.

The ex-cop has twice appealed the decision to detain him, once in federal court and once in the 3rd US Circuit Court of Appeals. His lawyers argue that holding him breaches his Fifth Amendment right to not incriminate himself.

Both have turned him down, in the latter case because an examination of the drives showed that they had been used in a computer that had visited child abuse sites and claimed they contained files with the same hash values as known child pornography files.

See (6)

The Defense argues that Rawls' stay in prison had already exceeded the maximum 18-month sentence under the 28 USC § 1826 statute for failure to comply with an order to testify or provide other information in federal judicial proceedings.

The Prosecution Argues that Rawls should stay in prison until he coughs up his encryption keys, noting that Rawls isn't being held under 28 USC § 1826, but rather the All Writs Act – the archaic legislation the FBI tried to use against Apple.

It says that they are not asking him for his decryption keys per se – they're simply saying he needs to perform the physical act of decrypting the drives and he's free to go.

The government is also arguing that, as Rawls didn't use his Fifth Amendment rights in his initial appeal he can't try to use that defense now.

It points out that in other cases, people have been held for contempt of court for nearly seven years, and cites the appeals court verdict that "no temporal limitation on the amount of time that a contemnor can be confined for civil contempt when it is undisputed that the contemnor has the ability to comply with the underlying order."

The government points out that if the drives do contain child abuse images then Rawls is looking at over 20 years in prison, and there is no statute of limitations for crimes against children. It asks that Rawls should be given another chance to decrypt the drives, and if he refuses, he should stay in prison.

Jewel v NSA

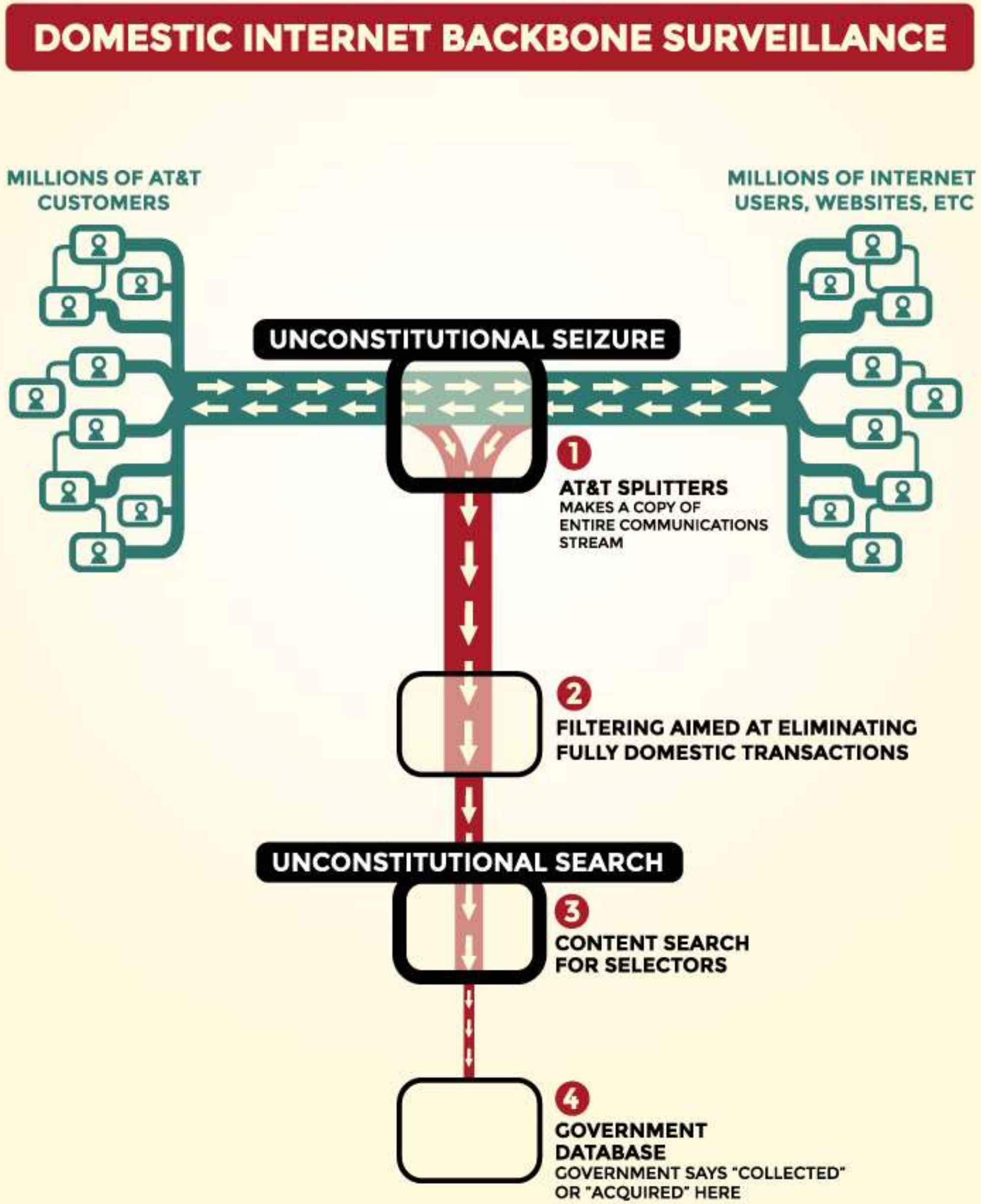
Secret government documents, published by the media in 2013, confirm the NSA obtains full copies of everything that is carried along major domestic fiber optic cable networks.

Currently, EFF is representing victims of the illegal surveillance program in *Jewel v. NSA*, a lawsuit filed in September 2008 seeking to stop the warrantless wiretapping and hold the government and government officials behind the program accountable.

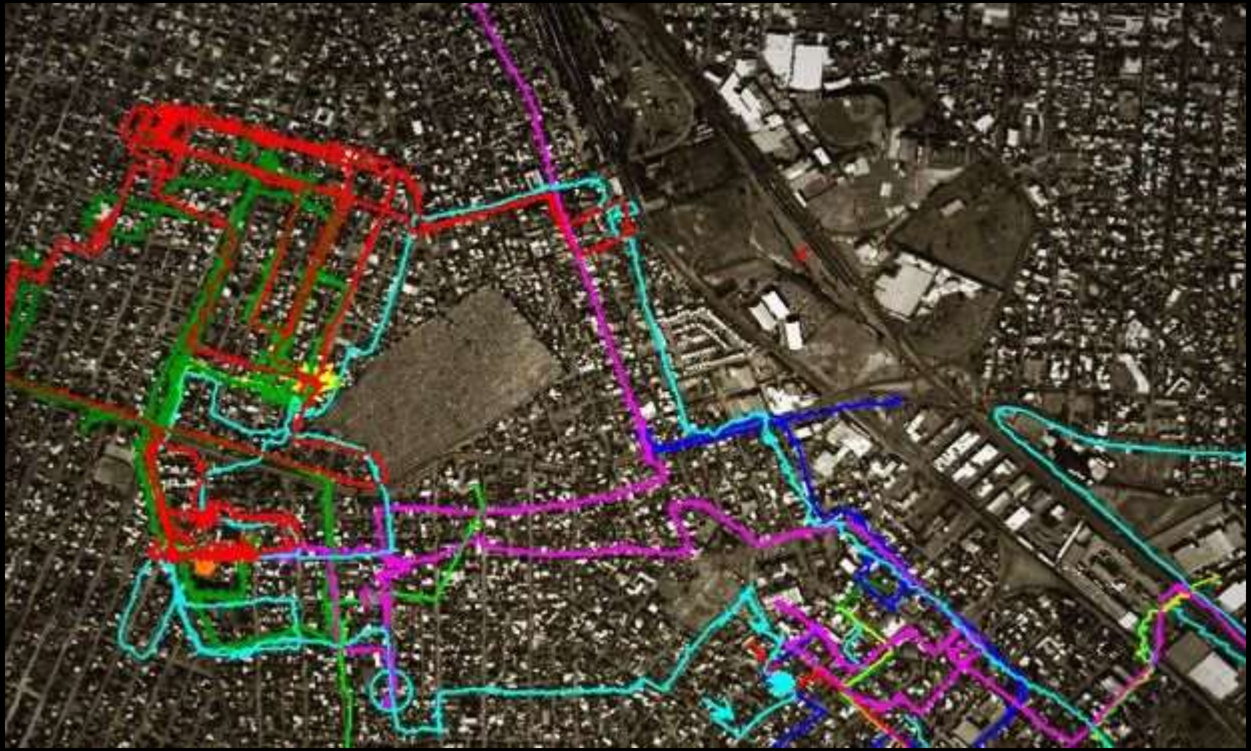
On February 10, 2015, however, the court granted summary judgment to the government on the Plaintiffs' allegations of Fourth Amendment violations based on the NSA's copying of Internet traffic from the Internet backbone. The court ruled that the publicly available information did not paint a complete picture of how the NSA collects Internet traffic, so the court could not rule on the program without looking at information that could constitute "state secrets."

The court did not rule that the NSA's activities are legal, nor did it rule on the other claims in Jewel, and the case will go forward on those claims.This case is being heard in conjunction with *Shubert v. Obama*, which raises similar claims. *See* (7)

Note – advances in quantum computing may enable full copies of encrypted data to be decrypted


DOMESTIC INTERNET BACKBONE SURVEILLANCE
MILLIONS OF AT&T CUSTOMERS
MILLIONS OF INTERNET USERS, WEBSITES, ETC
UNCONSTITUTIONAL SEIZURE
1
AT&T SPLITTERS
MAKES A COPY OF ENTIRE COMMUNICATIONS STREAM
2
FILTERING AIMED AT ELIMINATING FULLY DOMESTIC TRANSACTIONS
UNCONSTITUTIONAL SEARCH
3
CONTENT SEARCH FOR SELECTORS
4
GOVERNMENT DATABASE
GOVERNMENT SAYS "COLLECTED" OR "ACQUIRED" HERE

Eye in the Sky

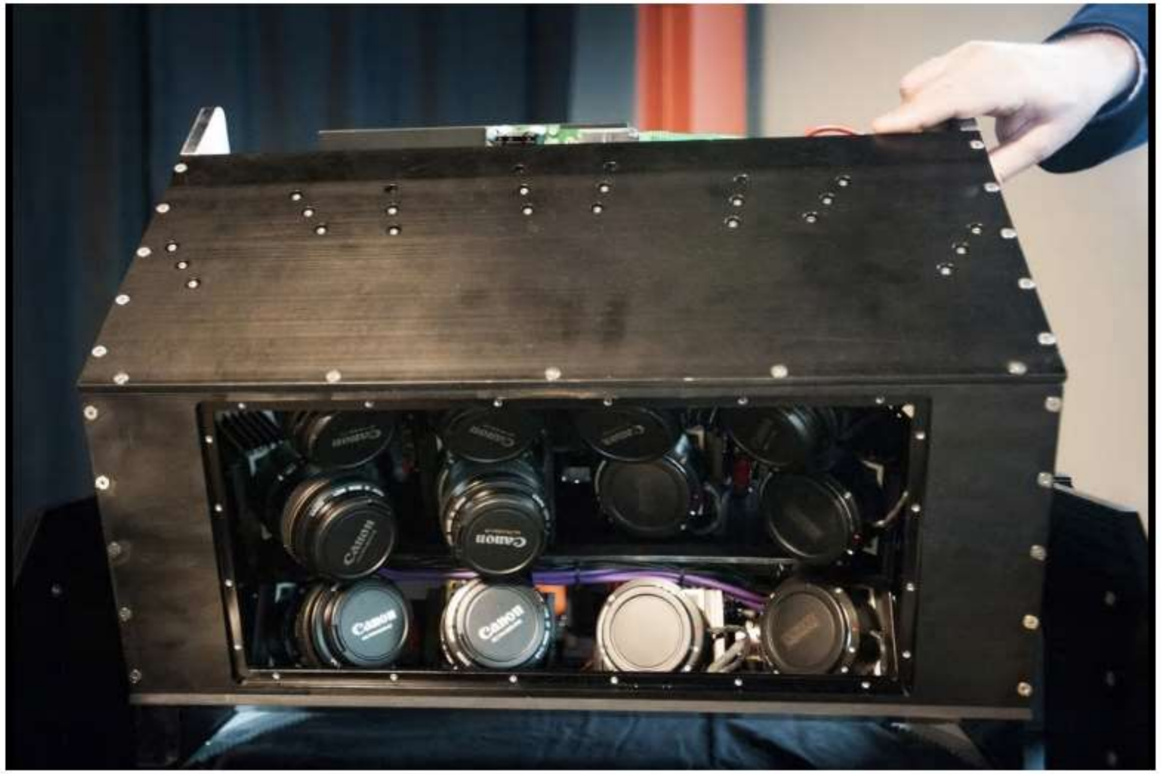


In 2004, when casualties in Iraq were rising due to roadside bombs, Ross McNutt and his team came up with an idea.

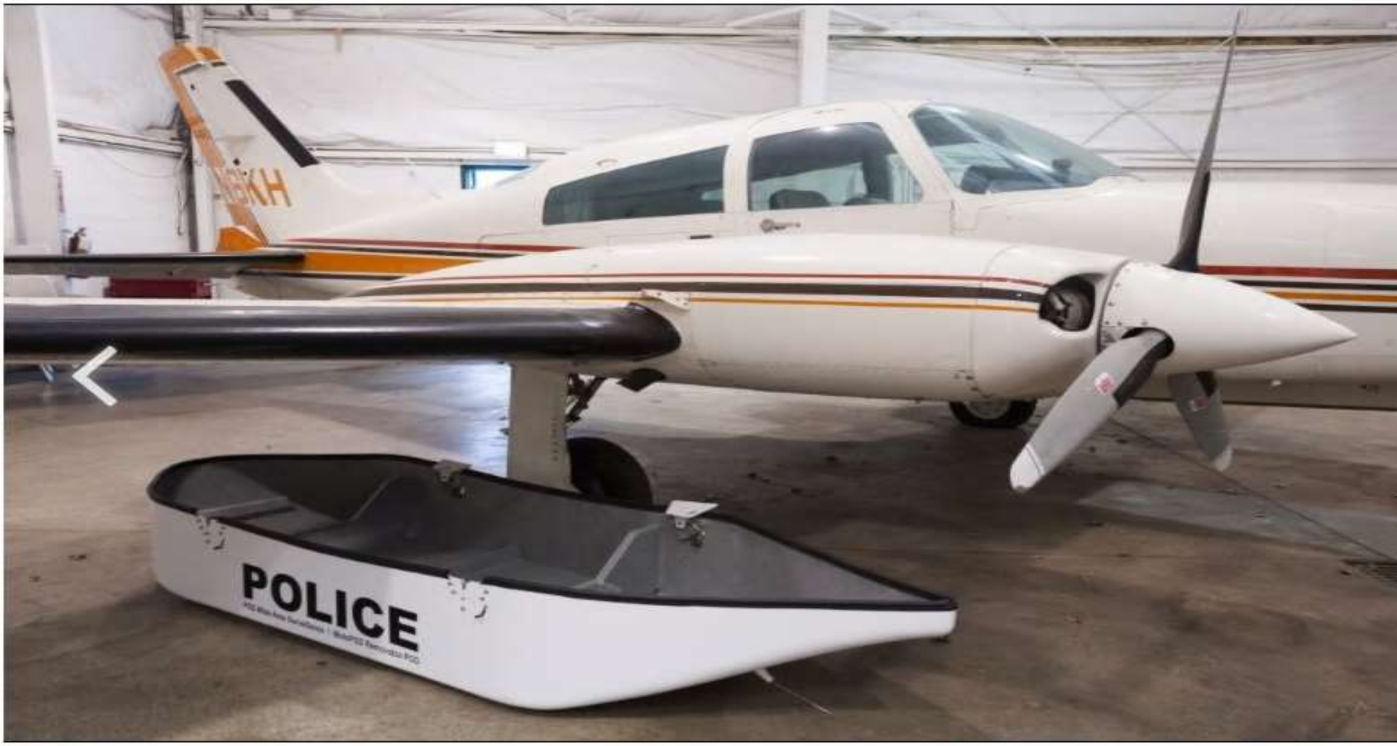
With a small plane and a 44 mega-pixel camera, they figured out how to watch an entire city all at once, all day long. Whenever a bomb detonated, they could zoom onto that spot and then, because this eye in the sky had been there all along, they could scroll back in time and see - literally see - who planted it.

After the war, Ross McNutt retired from the airforce, and brought this technology back home with him.]This technology has been implemented in cities from Juarez, Mexico to Dayton, Ohio.

02-05-14: Ohio-based *Persistent Surveillance Systems* is trying to convince cities across the country that its surveillance technology can help reduce crime. *See* (8)



Twelve Canon 50mm lenses are used as the optical elements that make up a composite image of the Hawk Eye II camera. (Ty Wright/For The Washington Post)



The Hawk Eye II surveillance camera is transported in a pod underneath this plane. When such cameras have flown over Ciudad Juárez, Mexico, they have captured evidence of 34 murders, the company says. (Ty Wright/For The Washington Post)

Elizabeth Dils, a Persistent Surveillance Systems analyst, studies traffic patterns. The company's cameras have been used for traffic studies and security at NASCAR races. (Ty Wright/For The Washington Post)

Different-colored circles highlight a group of cars on a monitor at the command center. While Persistent Surveillance Systems hopes to reduce crime across the country, it has sparked privacy concerns amid a wave of revelations about the National Security Agency's surveillance. (Ty Wright/For The Washington Post)

FINISHED FIRST SEMESTER OF SOFTWARE ENGINEERING
"I'M A HACKER, LIKE ANONYMOUS."

Lessons Learned:

If you want to keep something digital private – USE GOOD ENCRYPTION

- What's Old is New Again. -> Nothing Beats Pencil & Paper (hello shredding parties)
- Script Kidde <>= Hacker
- There is always someone more 1337 than you!
- Blockchain – That's What's Up
- AI > You
- Quantum Computing Changes Everything
- Spokeo: a Must Have Research tool For Lawyers
- "Know Yourself Know Your Enemy"
- "Use data to gain insights that give you leverage in negotiating your position"
- "Divide and Conquer"
- REPUTATION IS EVERYTHING – *See Harvey Weinstein*

List of Data Brokers :
https://www.privacyrights.org/data-brokers

WHAT HAS BEEN SEEN
Cannot be un-seen...

SOURCES

1. http://searchsecurity.techtarget.com/definition/digital-signature
2. *See generally,* www.productivity501.com/digital-signatures-encryption/4710/
3. https://www.wsj.com/articles/google-rival-yelp-claims-search-giant-broke-promise-made-to-regulators-1505167498
4. https://www.privacytools.io/
5. https://www.engadget.com/2017/08/09/disney-illegally-collected-data-kids-apps/
6. https://www.theregister.co.uk/2017/08/30/ex_cop_jailed_for_not_decrypting_data/
7. https://www.eff.org/cases/jewel
8. https://www.washingtonpost.com/business/technology/new-surveillance-technology-can-track-everyone-in-an-area-for-several-hours-at-a-time/2014/02/05/82f1556e-876f-11e3-a5bd-844629433ba3_story.html
9. https://www.wired.com/2017/03/feds-rather-drop-child-porn-case-give-exploit/