Edward Snowden at Web3 Summit 2019

Prescient predictions about the censorship to come during the COVIDcrisis

ROBERT W MALONE MD, MS

JUL 11, 2023

63 11 Share

"You have to know the past to understand the present." Carl Sagan

"...everything has a past. Everything – a person, an object, a word, everything. If you don't know the past, you can't understand the present and plan properly for the future."— Chaim Potok, book Davita's Harp

"Misunderstanding of the present is the inevitable consequence of ignorance of the past. But a man may wear himself out just as fruitlessly in seeking to understand the past, if he is totally ignorant of the present...This faculty of understanding the living is, in very truth, the master quality of the historian." — Marc Bloch (French historian, medievalist, and historiographer) 1886–1944 The Historian's Craft, pg.43

Web 3 Foundation, Web 3 Summit, 2019

Speaker 1:
All right. Well, this has been an incredible past day and a half of Web 3 Summit and we are so excited to have you here today. There's a number of talent of developers and researchers and advocates building a decentralized web focused in privacy and censorship resistance. Our vision of this new web is transparency for the commons and privacy for the individual, and no one has done more to validate this need than our next speaker, Edward Snowden.

Edward Snowden:
Thank you.

Speaker 1:
Thank you so much for joining us. Thanks for joining us.

Edward Snowden:
It's my pleasure.

Speaker 1:
We have this incredible room of developers and technologists and people who are passionate to hear what you have to say so I will just let you take it away.

Edward Snowden:
Okay, cold open. First off, thank you all for bringing me to speak with you. It's tough for me to get over to Berlin these days, but I'm still hoping in the future I might be able to come in person. When I give these talks since 2013, I've been asked many different things about what's happening with journalism, about what's happening

with government, what's happening with the internet, what's happening with technology. And the funny thing is I think they're actually all centralized around similar factors, and most of you are familiar with them. Anybody who is into technology and is not simply a developer, but is also a user, anyone who's interested in privacy, anybody who's working with online financial technology, who's thinking about cryptocurrencies or could just be Bitcoin or competitors to it is seeing that increasingly there's all of these threads connecting to one another.

And it's not a single thing, but rather we have an entire ecosystem that is decaying because it's actively under threat. And the earlier half of this century or this last century, scientists and engineers were committing their lives to the pursuit of a new science, nuclear physics, and it was an incredibly passionate work. Publications went all over the world in every language, and it just energized an entire generation with the possibilities of free, nearly unlimited clean energy, advances in medical technology, advances in transportation. It was obvious how these new advances could be applied for the betterment of everyone, but it was also not long until the work of that cohort began to be applied to private needs. And this is interesting because most famously we're talking about nuclear weapons, and people don't think about that as private needs.

People think about what the government does is as the public good, but what's good for the state is very different than what's good for the people in many cases. And I think what we are seeing today is the work of our greatest minds of the last 50 years now increasingly their work being indentured to the service of the private good. Now, this isn't just the state, this is of course the corporate state that we see, the Facebooks, the Googles that are haunching on our common backbone and they're trying to insert themselves into every human transaction. And these aren't merely trade transactions, these are communications transactions and this is how we see the same thing that happened in the last century beginning to repeat again. A science that was developed in pursuit of the ideal of the common good being captured and distorted for the private benefit of certain groups. This can be a private elite corporate segment or of course, the national elite.

Now, this is the reason that I say what we're living through today is the atomic moment of computer science. This is where we really have to look at what our work has done, and I don't mean your work personally because a lot of you guys in the room, free software guys, you tend to be on the better side of a lot of these conflicts, but we all have to realize that everything that we do isn't enough. When I was sitting in 2013 and I saw what my government was doing behind closed doors without consent of the governed in the United States, without the knowledge or consent of anyone in the world, flagrant violations, both of US law, constitutional rights and more importantly, human rights around the world I really wanted to tell somebody about it because I thought it was wrong. It took me a very, very long time to decide to come forward and tell people about it, even though I was increasingly certain that this was something that was in many cases contrary to what the government can even be permitted to do if they pass a law.

But I knew that if I did, there were going to be consequences for me. It was going to be difficult for me personally. I didn't know quite how difficult, but I did have an idea. And it is this kind of natural pressure, the incentives and disincentives to a given move that a person can take in our lives, in our communities, in our societies, that I think all of us who work with systems understand very well because this is how systems work, this is how systems are regulated. And as it stands today, all of the pre-existing laws and all of the loopholes that governments use to violate the spirit of the law, even if not the letter of the law, or more importantly and directly just to violate our rights or the dignity of a given person, these are all achieved by exploiting their deep understanding of where the incentives are and the disincentives are. Primarily they can break the law without punishment because they're the ones who applied the law. So what does it mean when the greatest safeguard of human rights that we've ever had in history, the law, begins to fail?

I know some people who have thought about this a lot more deeply have been talking about it at the conference, but I think this is where we see a lot of excitement coming from technology. Recently, and particularly people who are working on these new decentralized sort of ledger based type applications, is this idea that maybe when the law fails us, our technology can catch us. The problem of course is that technology has been catching us and general members of the public, people who know don't a fraction of what some of the people in the room and harming them quite significantly. So what do we do and what are the actual problems? I think it's this identification of the problem that really helps us. Now, I think we're moving quite far along here, but the thing that keeps me up at night, the thing that I've been thinking about for years and the reason that I wrote a book about this that actually comes out in a month.

Is that when I was a child and I was in high school, even before high school because of I think you guys know the personality type, you probably struggled the same way, you have someone in authority who's telling you what to do. They don't explain why, you don't understand the system and yet the system is applied to you. You have no power within the context of the system. You are not allowed to change the rules. You're not even allowed to petition to change the rules. That's simply the way things are. And someone says, do this, and you ask why? And they say, because I said so. This is the way a lot of power relationships work today, whether it's in the United States where our electoral system is gerrymandered so much that we can't change power even if we campaign, to the operations of internet giants. Where you see everybody complaining, you see everybody trying to boycott, you see everybody pressuring them and saying bad things about them, but they only change their policies at the very smallest edges, if at all.

And the reason I think they feel so comfortable, all of these types of authorities throughout history, is they have a mastery of our fear of what happens if we break the rules. What happens if we try to change the way the system works. And when I was young, the way this worked was if you cut up in class, if you got out of line, they'd say in of course, a very concerned manner for you because it's you, they're always worried about… Not them, not their convenience, but you. You need to think about your future. You need to think about what it's going to look like if everybody else is following the rules and you're the only one breaking them. If you get out of line, if you get a bad grade, if you get a detention, if you do whatever, if you talk back, if you question everything all the time, this will go down on your permanent record and then it will follow you to high school and then it will follow you to college and then it will follow you workplace and then it'll follow you through the rest of your interactions with power.

And as a kid when you don't know anything about anything, that's actually terrifying. And over time, bit by bit as you do more and more, the threat begins to lose its power because you realize that there actually isn't a permanent record. Nobody cares what you did in elementary school. Nobody cares what you did in middle school. Nobody cared about high school or college or honestly, nobody really cares about what you do in your workplace besides your employer and then your next employer. But at best, the records have never been permanent. They've never been perfect until now. And this is the problem of the world we live in. The younger you are in this room relative to the person next to you, the more of your life is known and recorded by people you have no influence over. And these records, at least under the laws in the United States which have been unfortunately exported around the world into a kind of status quo, says that you don't own records about your private life.

These companies that created them, they're their records, not you, even if they're entirely and exclusively about you. And this is I think the central problem that we're struggling with, is all of these companies, all of these governments, everybody who has any sort of aspiration to power is recognizing that understanding as much as possible about as many as possible is the lever of influence. We see target news, we see this being used to write news, we see this being used to change politics, we see this being used to try to influence purchasing decisions. All of these things are about shaping human behavior. And all of these things, which I would argue are fundamentally anti-democratic forces, and actually I would argue these are antisocial forces, are really about shaping the behavior of other people to your benefit. And if this can be done secretly, if this can be done privately, all the better. And when I look at this and I think about my own history and I think about what's happening on the internet, I think one of the biggest vulnerabilities in our system, the vulnerability that's being exploited by all of these forces is identity.

In the modern world, we are not permitted a sense of ownership without identity. To be able to make a trade in many cases, and God, if you live in someplace like Sweden where they're trying to get rid of cash, you've got to use a card. The card is connected to your bank account. That goes on. If you're trying to buy something like property, how are they even going to register that? They need you to show your ID. They need you to get it stamped. You go to the people at the desk, the people at the desk then bless you to be able to participate in this transaction. If you want to be able to buy a bottle of water at the gas station, this has been and should be a cash transaction. It should be traceless. But now increasingly there's cards involved. Now increasingly, there's cameras involved. Now increasingly, there's Bluetooth beacons in the store that look at your phone and they see, oh, it's got its Bluetooth active because it was just connected to its car so we know it's this device. We've seen this device at this mall.

They've got license plate readers. All of these things form big constellation of richness, especially when compounded with the fact that your cell phone is constantly a 100% of the time that it's turned on screaming out into the sky here I am, here I am, registered me to the nearest tower. And then they're tracking where this goes and all of these things mean we are never anonymous. We're never just a person. We're always this specific entity. And if we are this specific entity, we can be nudged, we can be shifted, we can be shaped by all of these people because we have universally unique identifiers. Now, programmers, developers, they love universally or globally unique identifiers. They want their metrics, they want their analytics. They want to see what's happening on this app push. They want to see what's happening on this kind of device. And so they collect everything from everyone everywhere. That's no different than what the NSA does. That's no different what Facebook does. That's no different than what Google does. And they do it because it grants them increased power.

They can be better developers and I understand that. I'm sympathetic to that. But I think we need to sit back and really take a look at the fact that when we are gating access to the infrastructure that's necessary for life through this process of proving who you are rather than proving a right to use, that you paid for this, that you should be able to access to this, that you have a blinded token of some type that could belong to anyone, but it's the digital equivalent of cash that's going, look, it doesn't matter who I am, I'm allowed to be here. I'm basically supporting the infrastructure. I've done my part. That's all it should be because otherwise, we're being forced to give up ownership of our identities. We're giving up ownership of our histories, we're allowing others to control the story of our private lives. They get to shape it, they get to tell it. They get to say, this is the narrative of this person, this phone, this card, this whatever, this browser.

And when we have this pervasive collection of, or sorry, not pervasive collection, but this pervasive creation of records, what we fundamentally have is the disempowerment of the individual and we have the empowerment of the institution. And a lot of people are fans of institutions, and institutions have done a lot of good throughout history, but they've also done a lot of bad. And the question is, what happens when you have institutions that are so strong that there is no alternative? What happens when you have institutions around the world in every country and don't even answer to your country. It's like a Mark Zuckerberg who won't go and talk to UK Parliament because he doesn't care about UK Parliament. He'll just send some lackey, right? And the people of these countries they ask why? Why do you do this? How do we change this? We don't like this. And then he can simply respond, well, that's the way it is because I said so. I'm the one in charge. We need to be able to create data, move data, process data, and transact on this data without creating a history that it happened.

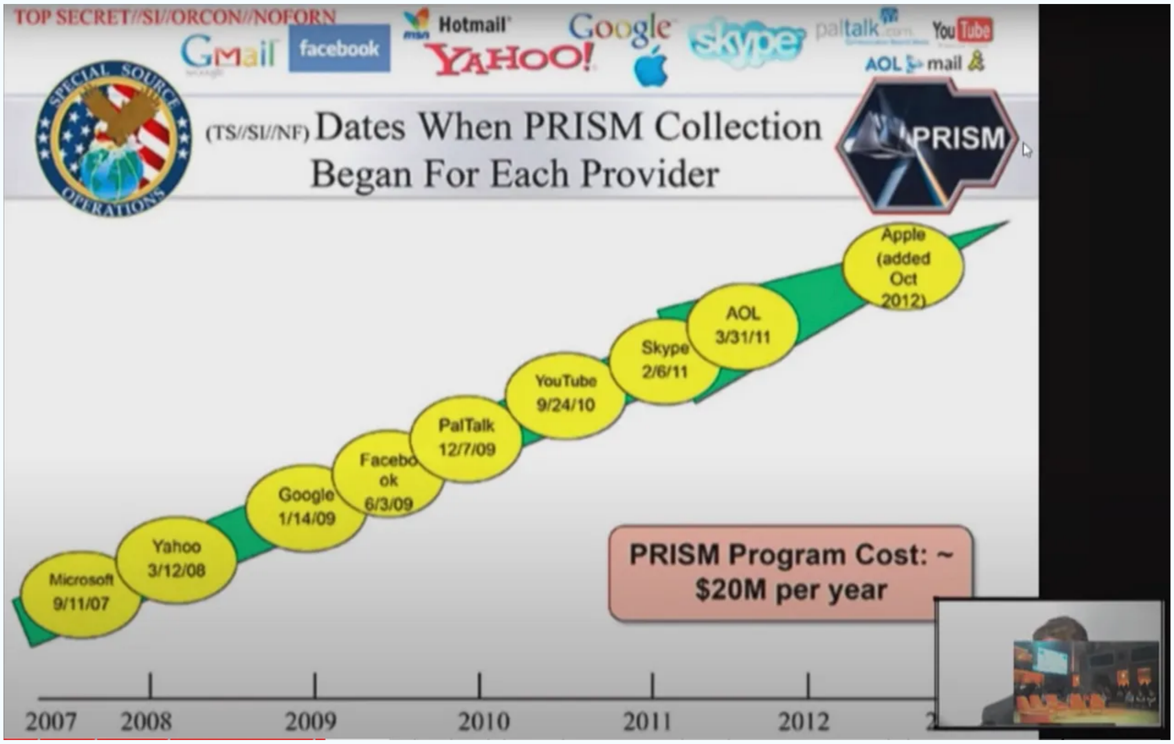
And what I mean by history that it happened is, I mean the history of you connecting the person to the thing. The transaction does not need to belong to you, the transaction belongs to itself. You can balance the books without knowing everything's connected to everyone, and I know a lot of you guys believe in this, but I'm afraid that we see a lot of people who don't believe in it enough. One of the biggest criticisms that I have of the Bitcoin blockchain today is the fact that it's not at all private. They're not even pretending to try to be private. There are arguments, and I know there are proposals that they're going to try to bring things on chain, they're going to try to integrate these enhancement proposals or improvement proposals, but they're not fast enough. We've seen this happening for years. Everybody knows the problems. We see the KYC sort of cancer spreading across the entire ecosystem where now there are no on-ramps and off-ramps of any meaningful size that will allow a normal individual, a teenager right now who doesn't even have a bank account to go, I want to buy Bitcoin.

And you guys who are working on alternatives, you can do better. And as you do better, that will pressure the bigger actors to do better because again, it's about the incentives and disincentives in the system. If you build a better model and no one else is willing to reform their own model, you become the standard model and that's a good thing for you. But even if you don't become the new unicorn, whatever, who cares, your decisions in designing these things create pressure on those incumbents to reform. Even in failing you can win for the world, for the community, even if you don't win for yourself personally. And that's what got me out of paradise in Hawaii in 2013 was I thought, look, I didn't graduate from high school guys. I'm largely self-taught and I was doing all right. I'm not going to say I'm the world's greatest anything, but I was doing all right. I was pretty good. And somehow I ended up working for the government, worked for the CIA. They put me overseas. I was undercover living as a "diplomat" in Switzerland. I went over to Japan working as a contractor for the NSA.

And each time I moved, I got more and more seniority, I got more and more pay until eventually I end up in Hawaii with the woman I love doing a job that was so ridiculously undemanding in the "office of information" sharing that I had time to do anything I wanted and that meant reading. And so what I did was I read what was going on everywhere because it was the first position I had where I could truly read without lines because in the intelligence community, there's very much this because I said so kind of worldview where there's a system called compartmentalization or compartmetation where the person in this office isn't supposed to know what the person in this office is doing. You're not supposed to be curious. You're not supposed to even ask because you don't have a need to know, right? Well, when I worked in the CIA and when I worked in the NSA previously as a technologist, as a systems administrator, I had broad access, much broader access than other people, and I could read many different things.

So I already knew a lot about what's going on relative to the average person, but when I reached the Office of Information Sharing of which I was the only employee, I was the Office of Information Sharing, now I had basically the same access to go around and read whatever I wanted as the director of the NSA. And so what did I do? I wrote some scrapers and I started to see everything that was out there, and everything got centralized in Hawaii and this was so I could share it out and create a little system that showed people, this goes here and this goes there and this might be useful for you in your office and that office, but I got to see what was going on in every office. And there weren't a lot of people in NSA who got to see this, and when I did, it started to really trouble me. Now you guys know what happened when we go back to the history. This is of course the most famous live for you guys because it's not about phones, it's about the internet.

This was where the largest internet service providers in the United States had secretly been going far beyond what the law required of them to cooperate with government and hand over in many cases without warrants the entire Google histories, Facebook histories, whatever's in your iCloud account and so on and so forth, over to the government under a system of secret court orders. This was unfortunately just where it began, and it wasn't just the internet.

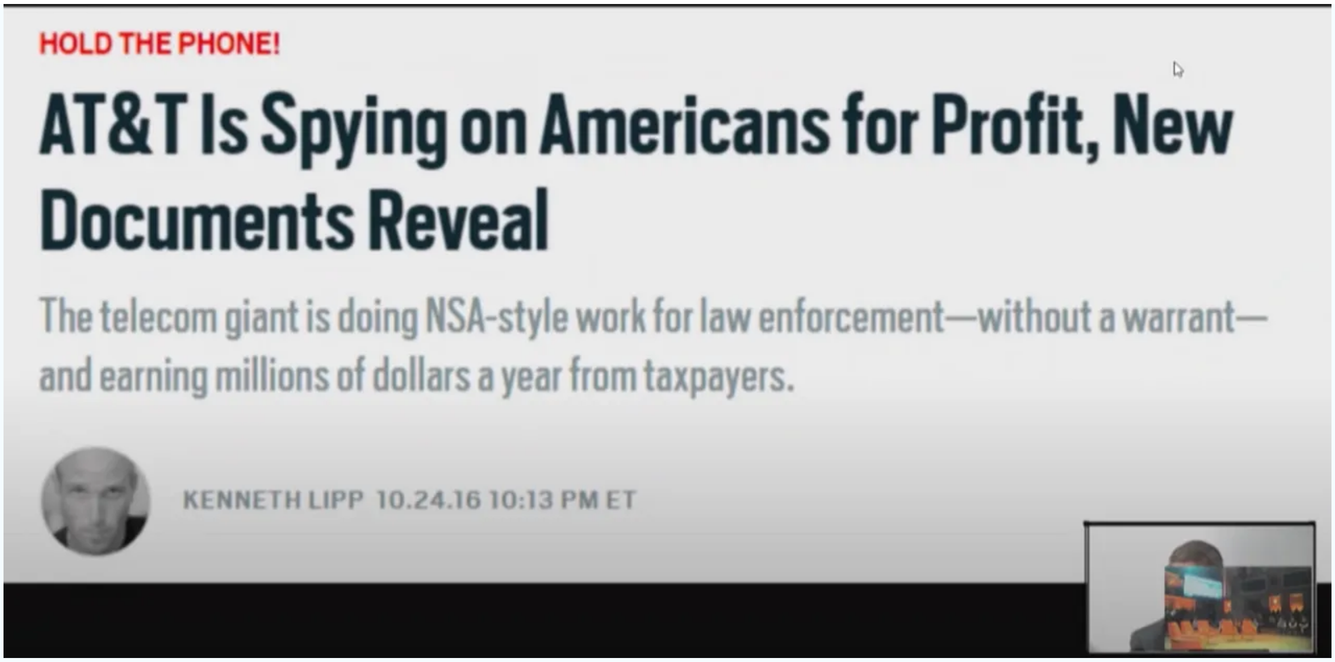


TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider

PRISM Program Cost: ~ $20M per year

There was a program that people saw that actually wasn't related to me, this was follow-up reporting that came I think actually some years later in the United States about the phone companies. AT&T is one of our largest of course phone networks, and what they found was that AT&T had been collecting the phone records of everyone who crossed their system and never getting rid of them for ages.

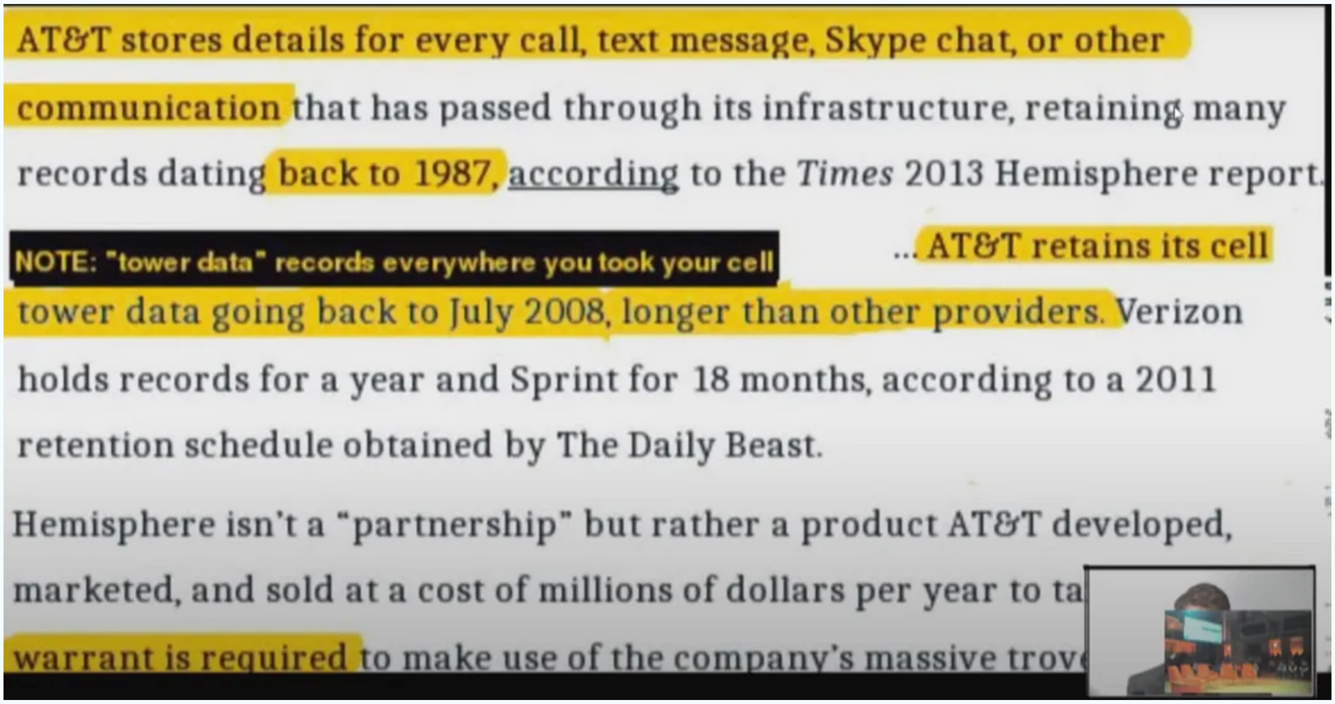


HOLD THE PHONE!

AT&T Is Spying on Americans for Profit, New Documents Reveal

The telecom giant is doing NSA-style work for law enforcement—without a warrant—and earning millions of dollars a year from taxpayers.

KENNETH LIPP 10.24.16 10:13 PM ET



AT&T stores details for every call, text message, Skype chat, or other communication that has passed through its infrastructure, retaining many records dating back to 1987, according to the *Times* 2013 Hemisphere report.

NOTE: "tower data" records everywhere you took your cell

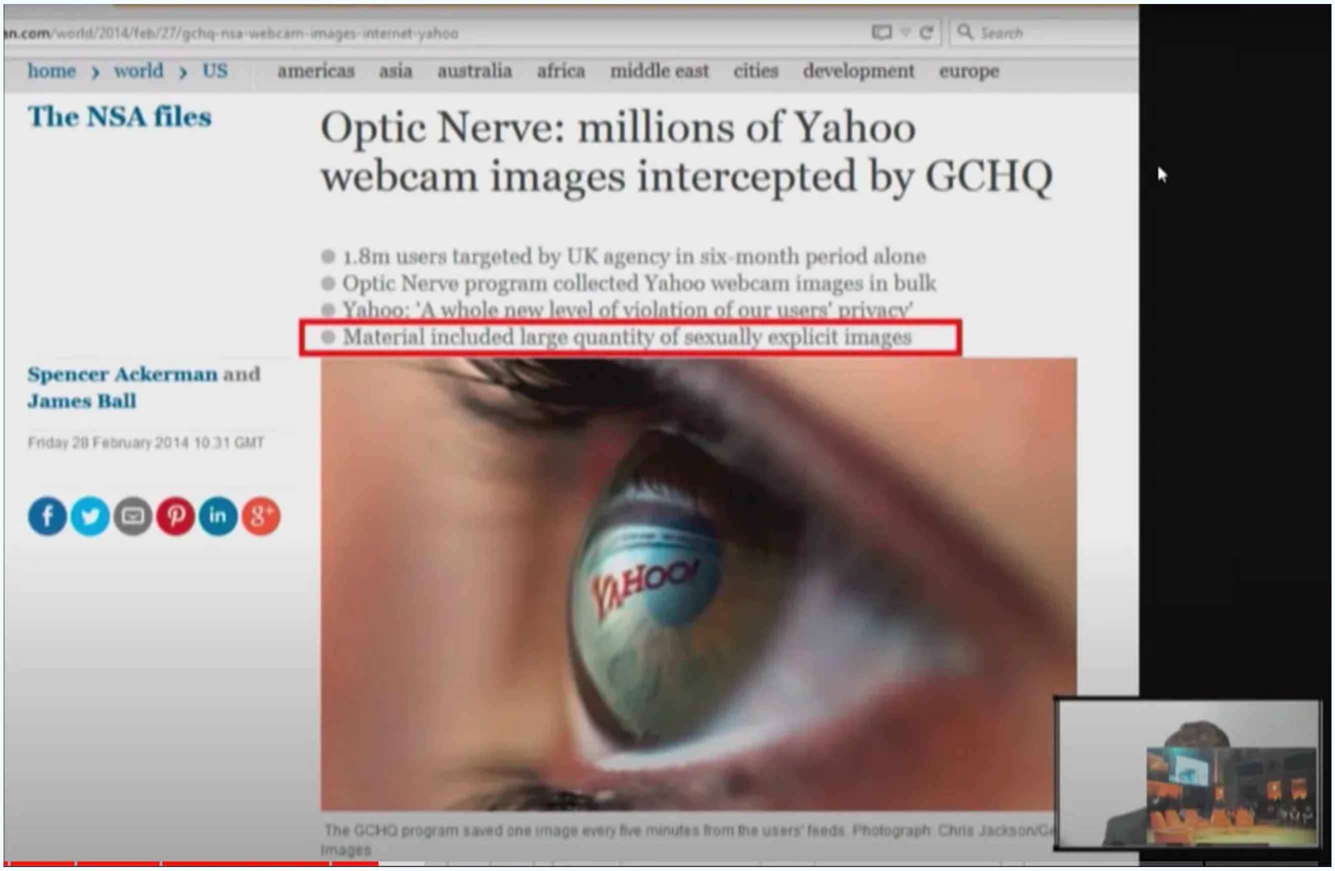
... AT&T retains its cell tower data going back to July 2008, longer than other providers. Verizon holds records for a year and Sprint for 18 months, according to a 2011 retention schedule obtained by The Daily Beast.

Hemisphere isn't a "partnership" but rather a product AT&T developed, marketed, and sold at a cost of millions of dollars per year to ta

warrant is required to make use of the company's massive trov

If you're younger, if your birthdate is after 1987 and either you're an American or you called the United States because anything that crossed their network went there too, they have every call that you ever made because that's how far their records go back.

They were keeping the tower data, which is of course the ledger of your cell phone screaming here I am, here I am, here I am going all the way back to July 2008. So they have more than a 10-year history of everyone's movements as they crossed the path of their cell phone towers. And this is the kind of thing that was just spreading and spreading and spreading everywhere on the internet because we hadn't been encrypting things by default.


n.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo
Search
home › world › US
americas asia australia africa middle east cities development europe
YAHOO!

The NSA files

Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ

- 1.8m users targeted by UK agency in six-month period alone
- Optic Nerve program collected Yahoo webcam images in bulk
- Yahoo: 'A whole new level of violation of our users' privacy'
- Material included large quantity of sexually explicit images

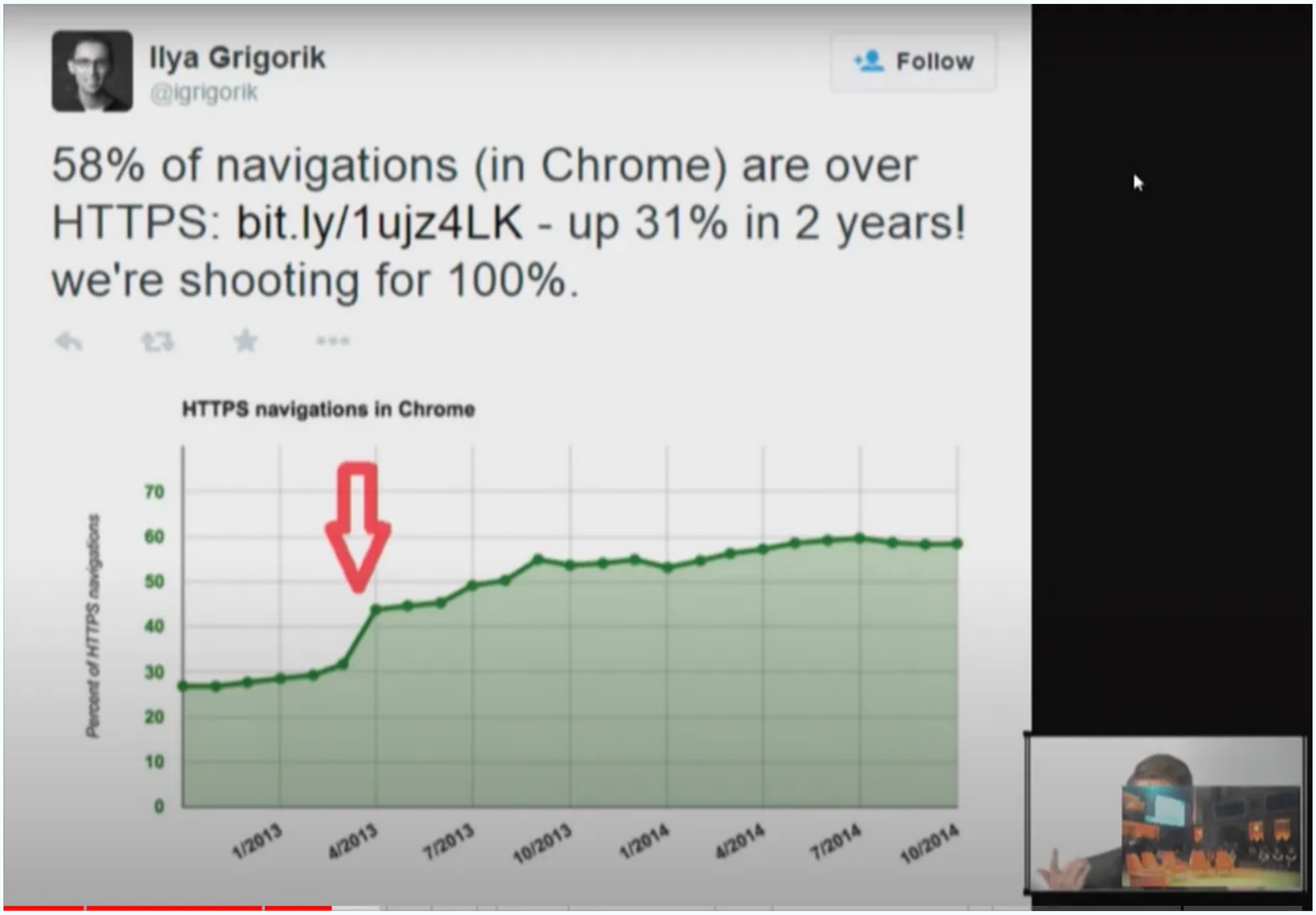
Spencer Ackerman and James Ball

Friday 28 February 2014 10.31 GMT

The GCHQ program saved one image every five minutes from the users' feeds. Photograph: Chris Jackson/Ge Images

We saw the NSA and their partners, the Five Eyes countries as they're called, that's the United States, the United Kingdom, Australia, New Zealand and Canada, the Anglophone guys, had just been looking across the backbone for anything that was even remotely interesting. And then what were they doing? They were just writing a scraper, right? They were just pulling things off the wire and then they were filing away into their little databases. And so they were getting pictures of your webcams, they were getting everything that you typed into the search box before Google finally went and encrypted it.

And then they had to ask Google for it, but Google would still hand it over all because things were not encrypted as they were in transit. Now, the thing I love about this chart, of course, is if you look at the timeline, I think this is the right one, you see there's a big spike right after June of 2013, which was the month that these revelations of mass surveillance first came forward. And this is where I want to talk about you guys as a cohort, not just as the people working on Web 3 initiatives, but as technologists. You did that. That spike is you. I didn't do that. I was on the run from the greatest manhunt that we've had in the United States in quite some time, but somebody read the news and somebody went, you know what? We're going to shift our site to HTTPS. You know what? We're going to retool our browser to prefer these kind of things. We're going to make our applications send these things. That's just in Chrome, but I can tell you from a lot of conversations that this is happening across the internet. And so what did these agencies do in response?



Ilya Grigorik
@igrigorik

58% of navigations (in Chrome) are over HTTPS: bit.ly/1ujz4LK - up 31% in 2 years! we're shooting for 100%.

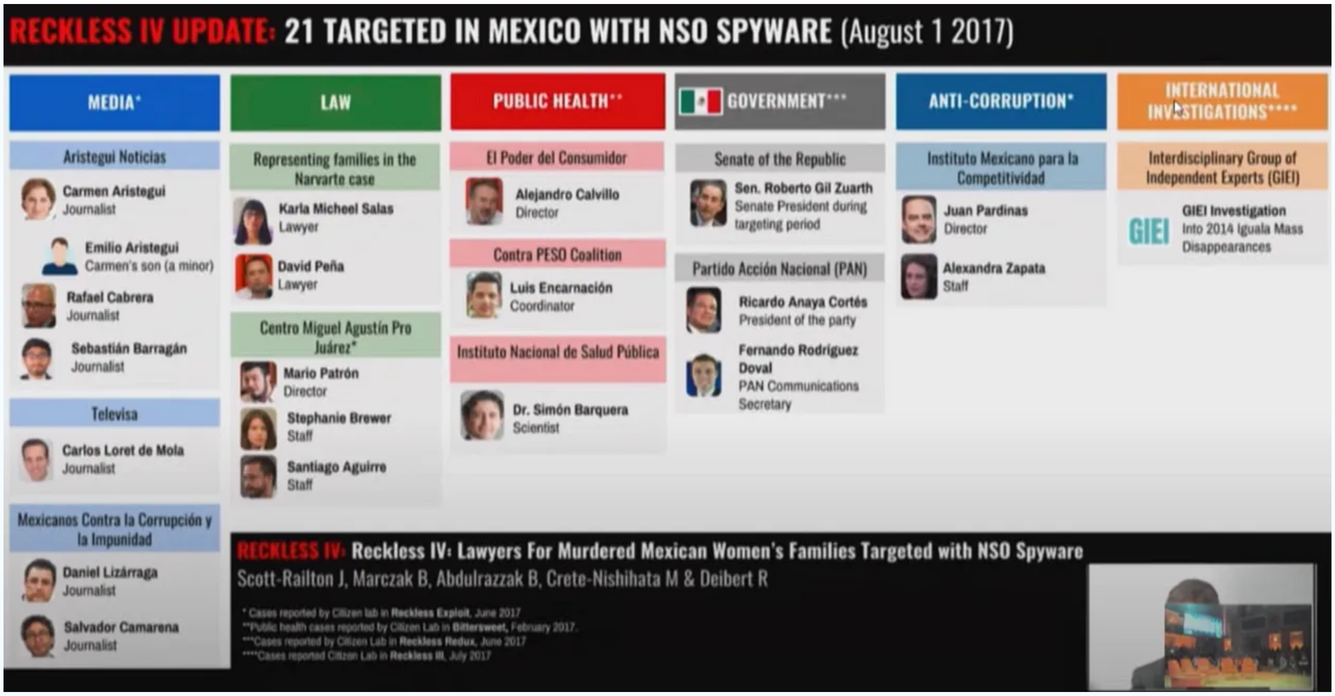
They go, oh, no, people are collecting things in transit and of course, this is the problem they've always had throughout history. They go, these people know what they're doing. They use encryption so we can't catch it in transit. Well, what can we do instead? And we see that it doesn't matter whether you're an ally or an enemy, the British version of the NSA put together a really complex operation to actually hack into Belgium's national telecommunications provider, Belgacom.

OPERATION SOCIALIST

THE INSIDE STORY OF HOW BRITISH SPIES HACKED BELGIUM'S LARGEST TELCO

Now, mind you they had legal means to get all of the information they wanted. They could use what's called a mutual legal assistance treaty to simply go right to the Belgian law enforcement agencies and go, we need this, we need that. Please provide it to them. And it would take a little time because people would have to actually check it, but then they would get it. Instead, they went, well, why don't we just let ourselves in? Then we don't have to deal with their encryption because we have their keys.

We can reroute their traffic. We can change the traffic flows to be more preferential to us to route communications of interest past our interception point. Why? Because we said so. Then as we've gone further and further away from this 2013 moment, as encryption has become more effective, as it's become more pervasive, we've seen malware and hacking attempts really explode and go beyond the government specifically into private industries.



RECKLESS IV UPDATE: 21 TARGETED IN MEXICO WITH NSO SPYWARE (August 1 2017)

MEDIA*

Aristegui Noticias

Carmen Aristegui
Journalist

Emilio Aristegui
Carmen's son (a minor)

Rafael Cabrera
Journalist

Sebastián Barragán
Journalist

Televisa

Carlos Loret de Mola
Journalist

Mexicanos Contra la Corrupción y la Impunidad

Daniel Lizárraga
Journalist

Salvador Camarena
Journalist

LAW

Representing families in the Narvarte case

Karla Micheel Salas
Lawyer

David Peña
Lawyer

Centro Miguel Agustín Pro Juárez*

Mario Patrón
Director

Stephanie Brewer
Staff

Santiago Aguirre
Staff

PUBLIC HEALTH**

El Poder del Consumidor

Alejandro Calvillo
Director

Contra PESO Coalition

Luis Encarnación
Coordinator

Instituto Nacional de Salud Pública

Dr. Simón Barquera
Scientist

GOVERNMENT***

Senate of the Republic

Sen. Roberto Gil Zuarth
Senate President during targeting period

Partido Acción Nacional (PAN)

Ricardo Anaya Cortés
President of the party

Fernando Rodriguez Doval
PAN Communications Secretary

ANTI-CORRUPTION*

Instituto Mexicano para la Competitividad

Juan Pardinas
Director

Alexandra Zapata
Staff

INTERNATIONAL INVESTIGATIONS****

Interdisciplinary Group of Independent Experts (GIEI)

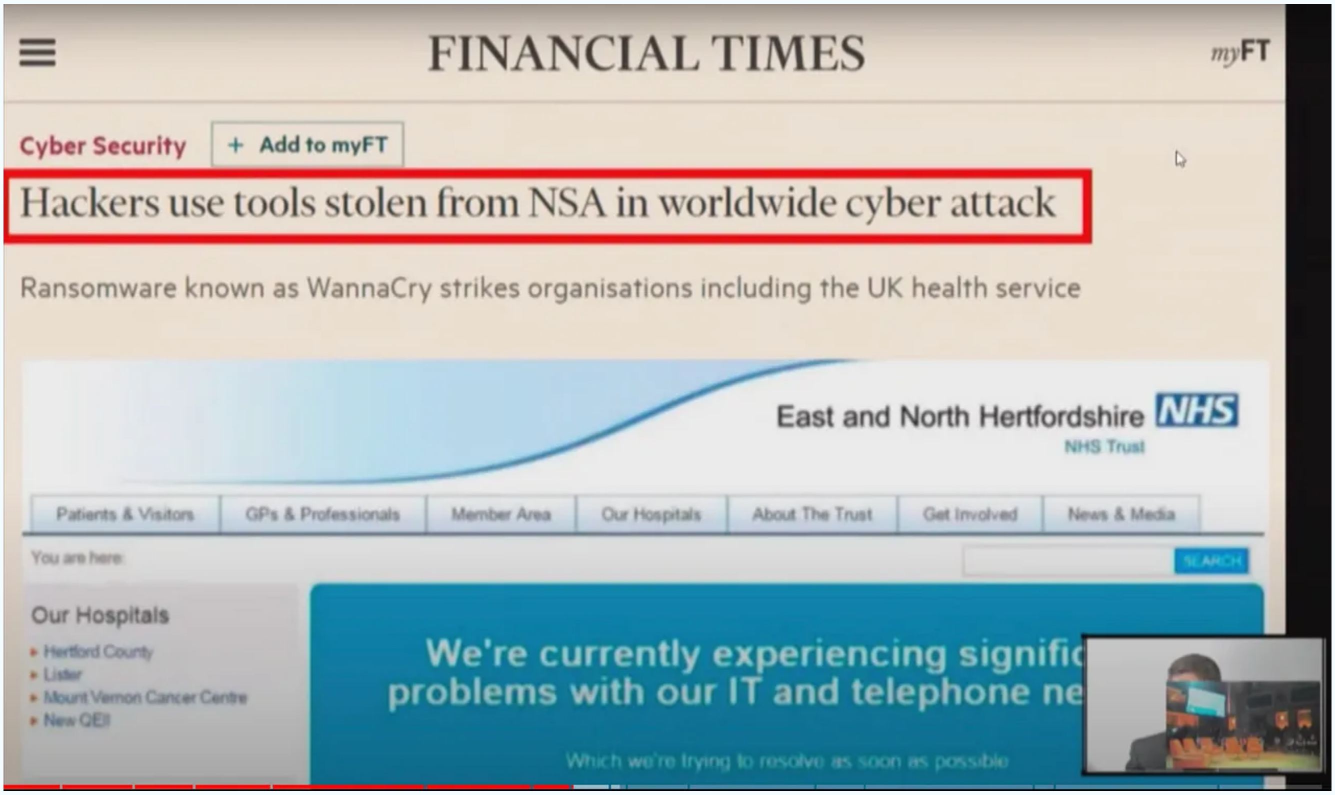
GIEI
GIEI Investigation
Into 2014 Iguala Mass Disappearances

RECKLESS IV: Reckless IV: Lawyers For Murdered Mexican Women's Families Targeted with NSO Spyware
Scott-Railton J, Marczak B, Abdulrazzak B, Crete-Nishihata M & Deibert R

* Cases reported by Citizen lab in **Reckless Exploit**, June 2017
Public health cases reported by Citizen Lab in **Bittersweet, February 2017.
***Cases reported by Citizen Lab in **Reckless Redux**, June 2017
****Cases reported Citizen Lab in **Reckless III**, July 2017

There's this Israeli company called the NSO Group, I'm sure many of you have heard about them. One of the things they really love to do is look for weaknesses in iMessage. iMessage of course, is enabled by default on every iPhone in the world. We just got some CVEs about iMessage I think out of Project Zero at Google just a couple of weeks ago. And it's great that these holes are finally being closed, but you need to think about how long they were open, how many others there are, and what's next when iMessage is finally a little bit more secure and it's just too difficult to find a fully remote bug easily. Where will they move next?

Encryption is not the answer to every problem, but encryption is the standard basis for every conversation we need to have. And this is the thing, if we have companies, NSO is valued privately at $1 billion or more right now because they were just sold for that. These guys are selling malware toolkits to governments for millions and millions of dollars. I think the Mexican government bought it for $18 million. I think the Saudis bought it for more than $50 million. 50, not 15. Again, fact check me on these because it's all public now, these records are out there, but who were they using it against? They were using against the head of their opposition domestically. They were using it against journalists that were reporting on the corruption of the president. And so this is what we start to see. We start to see corporations going, well, instead of making security safer, why don't we make it weaker? And of course, the NSA has always been doing this. They've been discovering vulnerabilities, they've been exploiting vulnerabilities, and then they've not been reporting them.



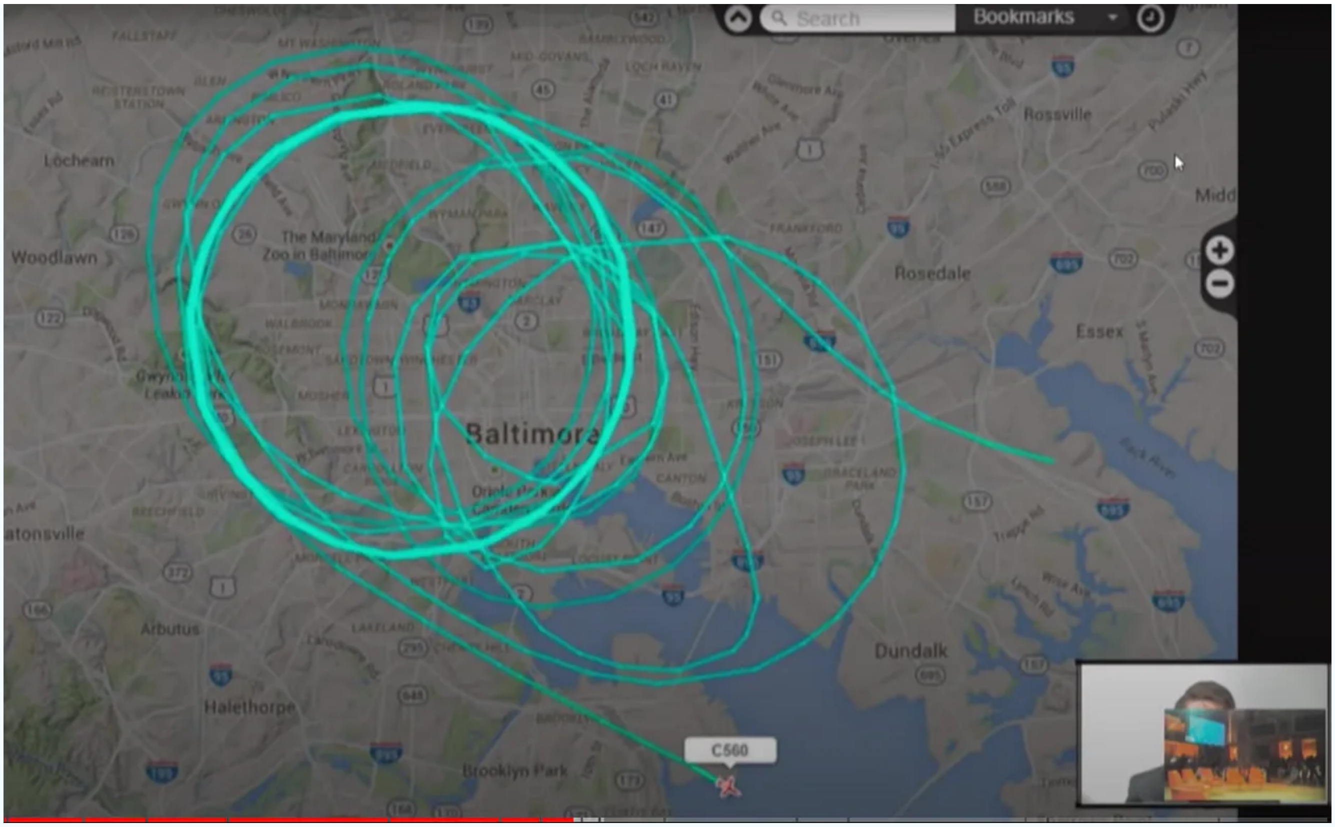
Hackers use tools stolen from NSA in worldwide cyber attack

Ransomware known as WannaCry strikes organisations including the UK health service

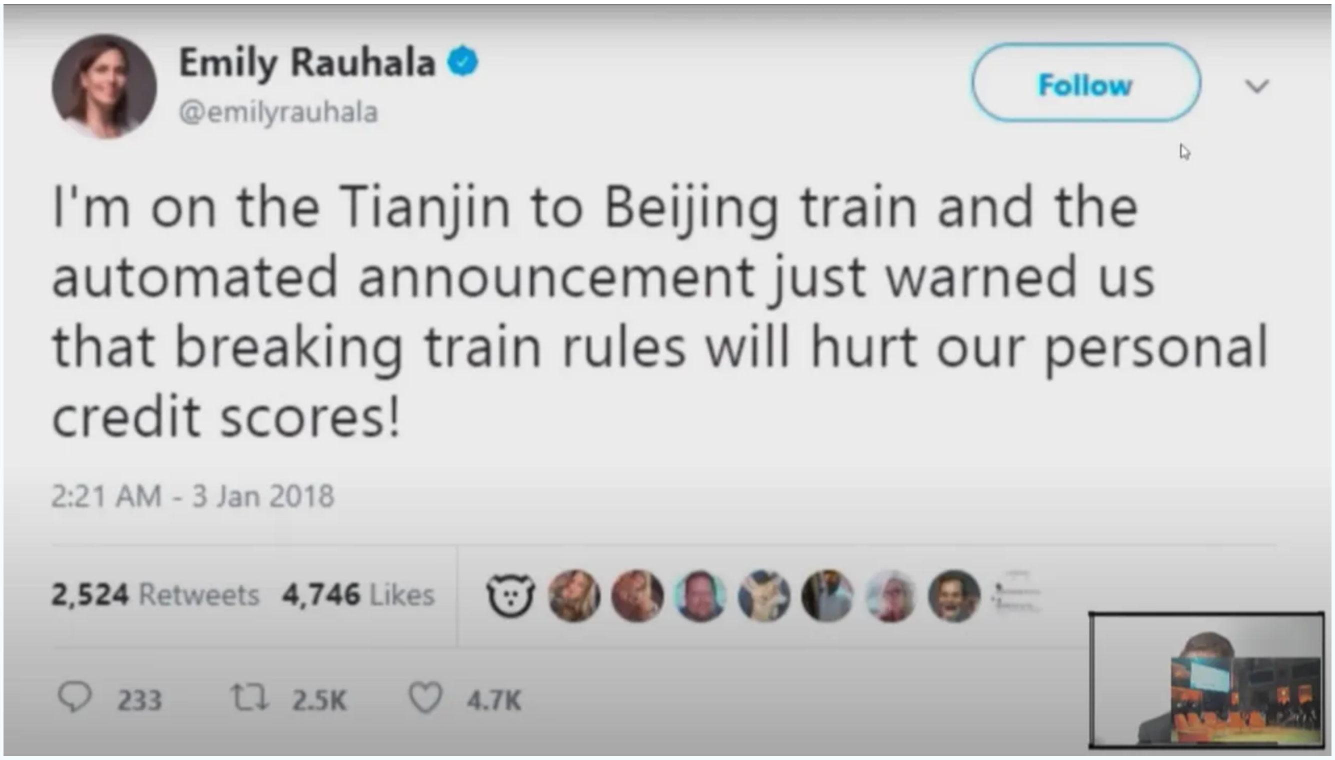
We're currently experiencing signific problems with our IT and telephone ne

Which we're trying to resolve as soon as possible

Well, the problem is those things leak too. They can't even keep their weapons safe. And then they hit us, they shut down the National Health Service in the UK. They shut down shipping around the world with Maersk. And all of these are derived from NSA bugs that should have been reported and patched years ago. Unfortunately, proprietary software you guys know how that works, but even when this doesn't happen, I want you guys to remember, look, you can make your software more secure. You can increase the security of the route as you're in transit, but we see things moving increasingly more and more to the physical layer. This is Baltimore, Maryland in the United States on the day of a Black Lives Matter protest. This is a minority protest movement against police brutality. And one of the interesting things we saw was an FBI surveillance plane during the entirety of the protest was simply doing orbits again and again and again and again.



And the only reason they do that in this kind of way is to form a census of which phones are in the area on the basis of their radio identifiers. Again, those globally unique or universally unique identifiers that are baked into hardware. And so I want you guys to constantly be thinking about where can we strip these identities out? Because now it's not on planes, right? Now it's on the cell phone tower next to you. Now it's in the gas station. Now it's at the mall at the gates and at every store. And this is something that's going to continue to get worse. And where is this going? We see in China where they really don't care about the public narratives because they can use their information control to maintain public support despite the abuses. This is not going to be theory. This is not going to be fearful conversations from paranoia acts like myself and hopefully yourself. This is going to be everyone. This is going to be your neighbors. This is going to be your family.


Emily Rauhala @emilyrauhala

I'm on the Tianjin to Beijing train and the automated announcement just warned us that breaking train rules will hurt our personal credit scores!

2:21 AM - 3 Jan 2018

2,524 Retweets 4,746 Likes

This is going to be people who don't understand politics, who don't understand technology because they don't have time. They have other obligations. They have other things they've dedicated their lives to, and they're just trying to get through the day. And if we don't do something about that, if we simply let the world continue on the same dynamic of an increasingly identified world, we are going to find that we no longer have the power to resist because we no longer have the power to coordinate, the power to collaborate because all authority has become centralized. Centralized through decentralization. And I know everybody in here sees decentralization as the holy word, and it can be good particularly when we're talking about disrupting these established orthodoxies, but what they are doing in centralizing authority through decentralizing it is they're actually just spreading what used to be quasi or fully governmental authorities to deputies that work very closely with government.

When you think about Facebook, you think centralized repository and you're absolutely right. When you think about Google and Facebook, now you're talking two central authorities. When you talk about Google and Facebook and Apple, now you're talking about three centralized authorities. And I know we've got Richard Stallman here and he's been at this a lot longer than I have, and we should all be grateful for that kind of work where they're trying to make people understand the risks of having unquestionable authorities that control your operating system, that control your decisions, that control your life. When we have a dynamic where you have great power spread very unequally around a few deputies, and these can be deputy companies, these can be deputy governments, what we ultimately find ourselves living, what we ultimately find ourselves in is a world where we're living in the midst of a net. And if we ever walk too far, we run into that kind of grid of you can't do that because I told you so.

So I know I've rambled for a while here and I don't want to go on too far, but if I could just summarize the points that I'm concerned about. The real value of, I think any kind of Web 3 movement is in making decentralization work for the public. And I don't question for a minute that is actually the intention of the people in this room. That's why I agreed to speak here. The thing is make sure you're doing enough. Whenever we start talking about identity and we're like, oh, we can prove identity and do this and that, you don't want to prove identity. Proving identity is a problem. Recording identity is a problem. That's dangerous. What you want to prove is a right of use. What you want to prove is a token for access. We need to make sure that everything we do happens encrypted by default as it goes in transit. You guys are way ahead of the game on that, and that's simply just because that's the price for entry to even a nominally private internet. But then we have to disempower ourselves.

We have to make sure that we are not replacing the old central authorities with new central authorities. And I know this gets dicey when we get into business models, I know everybody's out there and doing different things, and I know that is very much the purpose of what you guys are working on, is decentralization. But as you get bigger or as you get smaller and start to become desperate, I want you to remember the danger of temptation to succeed because we're all human and we all get hungry and we all make compromises. I compromised my values for a long number of years. I was working at the CIA, I was working at the NSA, and I was happy to do so. I was in fact proud to do so. I could defend myself a little bit by saying, well, I didn't know everything that was going on and when I did, I changed. But the reality was I knew enough that I shouldn't have been okay with it, but I was and that's because I was doing better than I ever thought I deserved to. We need to make sure that we make a world that is safe.

And we need to make sure we do more than that, we need to make sure we have a world that is free for all those people who were born after 1987. And for people to be able to make a phone call again without people making a note of it. We need people to be able to buy something, a gift for their mother without there being a record of it. We need people to be able to go to the gas station and get a sandwich and not have that left somewhere. We need someone to be able to post something truly idiotic on the internet and not have it haunt them for the rest of their life because if we can't make mistakes, we can't learn. And if we can't learn, we can't progress. And if we create this world of just an escalator of authorities where we go, yes, the old authorities were bad, we're going to create new authorities and they'll do better. And then eventually we'll realize how bad those were and somebody else will do that. We might survive, but I don't think we're actually fulfilling the promise of what we can really be.

Fundamentally, when we think about all these conversations, governments like to say, oh, security and privacy, they're different things. They're actually the same. Security is provided by privacy. When everything is known about you, you are vulnerable. Your decisions can be anticipated and you can be acted against. If the government wants to grant itself security by denying all of us privacy, that should not be reassuring. That should be concerning. And we need to think about why privacy matters, why this push for decentralization matters. You guys know, and you have people who will make the arguments better than I do, but when I think about this, I think it's really that question of when somebody tells you that's the way things are because I said so. We humanity, whether we're talking individuals, whether we're talking families, whether we're talking communities, whether we're talking nations, whether we're talking the global tribe, we need the ability to question that and we need the ability to change that.

And the only way that can happen in the face of extraordinary entrenched powers is if we can collaborate and coordinate and do this quietly. If we can talk to people that we trust, if we can sharpen our arguments, if we can find our good ideas and test and then discard our bad ideas, we can create a movement that changes the world. That sort of overturns this old regime and can hopefully in the future do away with the need for any regime. But how does that happen? That's a long way off and come on guys, we're talking about flipping bits on the internet. But those bits matter because it's a foundation. When we zoom out, when we talk about the concepts that everybody's discussing here like the failure of law, the failure of governance, the failure of all these old institutions to guarantee the rights and the freedoms that we all expected, that we all were taught in school exist in free and open societies, what then? What's our next resort? What's our last resort?

You are some of the only people in the world that can guarantee some measure of liberty for people in Russia, for people in China, for people in Iran. And if you can do it there, you can do it anywhere, and you do it by flipping bits. Let's go to questions. Thank you. Thanks.

Speaker 1:
Edward Snowden, the best dressed man at Web 3 Summit amongst. You're amongst a crowd of T-shirts and hoodies, but we appreciate you showing up today. So we're going to have some questions from the audience, but first I wanted to kick it off with a question that at Web 3 Summit we're quite curious about as we kind of look at this as a rallying call. A statement that you made in 2013, you said, "I'd rather be without a state than without a voice." So it's six years later and how do you feel about that?

Edward Snowden:
Honestly, this is one of the ideas that's the most dear to me. It's one of the ones that I get a lot of flack from actually when I speak in prominent settings on it because they're like, oh my goodness, some kind of anarchist, whatever. And the funny thing is I don't think it's about anarchism. I don't think this is a radical statement. I think it's simply order of operations. What are the things that are most essential, most vital to human liberty? What are the things that allow us to be people? Not simply to exist, not simply to survive, but to live? If we can't think, if we can't speak, if we can't express ourselves, if we can't become the person that we want to be, if we cannot disagree, if we can't have something of our own, even if it's only an idea, then we don't have anything.

It doesn't matter if we have a state, right? The state comes after. It's not the state that grants all of these things to us. It is the state that is supposed to at best protect these things for us, to act as a kind of guarantor of them. And when a state becomes contrary to these guarantees, well, I think it's time to reform it.

Speaker 1:
Hello? Yeah. All right.

Speaker 3:
So you kind of mentioned this, but I'd like for you to go further. So it's obvious that one of the largest problems we face is surveillance capitalism. It's a business model. And when you can't make money advertising, you're just going to sell personal data to the highest government bidder, and that's going to be used for social control. The bet, the fundamental bet of blockchain technologies is that there is an alternative based on tokenization as you put it. But do you think that's actually going to happen? Do you think that we could really build a sustainable alternative so that we're not all to be very frank, starving to death building free software?

Edward Snowden:
I think honestly, it's inevitable. Look, there's going to be a lot of failures, and there's going to be a lot of people who don't do this well, but think about the internet that if you are anywhere near the age I am now. I guess I'm 36, it's hard to keep track. The early internet was not commercially driven. The early internet was goofy, it was crude, it was BBSs and web forms and mailing lists. And then it moved to this thing where people are figuring out how to put up their own web servers on the new web, right? And then we get the early granted access from these guys who were trying to become the new web giants. And you remember GeoCities? You remember Angelfire? These were still big silos, they didn't have the kind of sophistication data mining that they have quite today, but the web was chaotic. It was terrible. There was no slick design, there was no great formal artistic beauty in it there, but it was beauty in a different way because it was original and because everything was driven by a purpose for a constructive sharing purpose.

And look, there's two things that we need to look at here. There is building a community. There's building a commons. There's interacting and exchanging and building a cultural identity and a commercial existence where we can survive, but then there's also the takeover the world model and I think this is where a lot of technologists are coming to conflict with their soul. When they realize they can design a service one way to get by and increase the value of human connection, but then they can make one little tweak and take over the world, and now they're a billionaire and they've got a private jet and whatever, it's difficult to resist that. What I'm saying is there's a medium where you can have something in between. And I do think a prerequisite for that in a way that protects human liberty requires a fundamentally anonymous currency. To be able to engage in private trade is one of the basic human freedoms. To be able to go, look, I painted this rock. Do you want this rock? And not to have someone at the desk deciding can you do something with this rock or not.

On the internet today you can't do that without incredible technological familiarity. This is why people have gotten on me, they're like, oh my God, he's saying all this stuff about these other fringe currencies. He's an altcoin not whatever. I don't care about any of that guys. But when you look at what's happening with zero knowledge proofs and how they're being applied and something like Zcash, when you see what the guys in Monero are doing, even though they have some pretty terrible community management on that side, when you look at all of these things where they're going, can we make things where right now it's still too hard for both of them, right? The wallets are inaccessible it. It's the stories, the narratives are not easy to understand for average people who don't understand anything about technology. The on-ramps and the off-ramps, they don't exist. But there is no reason in my mind why you shouldn't be able to go to the gas station and when you lay down cash for a bottle of water, you can lay down cash to get a bucket of internet, right?

Tokens that you can use for any service, that you can use for any product, that you can use for any anything. And then when we get beyond that, we don't even need that anymore. People can actually get paid for their labor. People can get paid directly into their economy, and then they're getting a bucket of internet for everything because why not? But this is the thing where we start running into friction with these old institutions, and you guys know that very well. You see this very well in the KYC thing. For those of you who follow the economy today and what's going on with the bond markets, what's going on with the currency markets, all of these governments they're inverting yields and they're starting to ask you to pay them for the privilege of them holding your money. The idea of what currency is, we are at the very early moment of that being called into question. I do not think currency as it has existed on paper, issued by a central authority is going to exist over the long scope of history.

But how long it takes to get there is very much an open question because you guys have no idea the kind of resistance we're going to face when the government really feels threatened. Right now, the government, every now and then you get officials out there, legislators out there who get their hackles up, they go, oh my goodness, Facebook. And Facebook's being really stupid and what they're doing now because they're too early and they're going too aggressive and they're doing it in the centralized stupid way because of course they're Facebook. But the main thing is right now, everything, what every person in this room is doing is a novelty. The state does not care because you are not a threat, but you will be. And when you will be, you need to very quickly move from being a threat to being an just completely irresistible wave that cannot be undone. Your work becomes a fait accompli. And that is the only way that this really works, but I think that actually is going to happen because there's simply too many people working on it in too many jurisdictions, in too many languages.

And ultimately when we're talking about the network, so long as we can establish those essential foundations that I talked about before, you connect from one state to a server in a completely different state and nobody knows because it's encrypted, and more importantly, the metadata is munged, right? You've got to Tor like mixnets that are preserving privacy or new technologies that I don't know about. I think we've got David Sham at this conference who's done amazing work in the past as well. We need to solve these metadata problems and we need to do this not just for money. We need to do this not just for wonky protocols on the edge. We need to do this everywhere for everything, and we need it to be invisible because the user is not going to become an expert. The user doesn't care. The user just wants to exist. They just want to live. They just want to do. They just want to be. But if you give them a voice, they will feel the value of that and they will love that, and they will be willing to defend that when it comes under attack, but only if they're able to know that it is possible, that it exists. And they're not going to know that without you.

Speaker 4:
I like that Zcash, your bucket of internet. They should really run with that. I was going to ask this, my background is an investor of journalists for The Guardian before I work for now Streamer, and I was in the newsroom when the, well what we call the

NSA revelations, but are now generally known as the Snowden revelations were revealed. And so I sat next to you and McCaskill and Luke Harding, and there was this discussion after discussion in the days that followed about where was the public reaction? Where were these riots on the streets? That was kind of the expectation. So the question is this, did you expect public outcry on the streets? But then did you also expect this, which is this room of people who are pretty well funded, fairly well funded, coming together and technologists fighting technology?

Edward Snowden:
I mean, it is a great question. It's hard to answer because so much happened in so many places. In the United States actually we did get the marches. We got protest movements. Eventually we even got our laws changed, not far enough, but we got the first substantive reforms to intelligence collection authorities in the United States since the 1970s. Sitting in the UK in London with The Guardian, it was a very different reaction, and it's interesting because the British media system, you know better than I do, is unique and unfortunately in many ways uniquely terrible. In that the government puts out denotices and the BBC and whatnot, all these competitors of The Guardian didn't do follow-up reporting. They didn't want to share the story. They didn't want to be a part of the story. Instead, they tried to just ignore it and so only The Guardian was actually out there running with this.

So readers of The Guardian were well-informed, but everybody else, broadly, socially, they didn't even realize it was happening in a meaningful way. And where they did know something was happening, they didn't know the significance of it. And that was actually an intentional strategy. Now, this is one of the challenges with the media environment around the world, because we see this sort of news distortion happening on topic after topic in country after country. It's not unique, but I did know and I did believe from the beginning that this was not likely to be the kind of thing that gets people burning down buildings. I didn't want to burn down the buildings. In that very first interview with you and McCaskill actually, I said, "I'm not trying to burn down the NSA. If I wanted to do that, I could do that in that afternoon." I had access to everything.

What I was trying to do was give people the information that had been withheld from them, that belonged to them, that they needed to know in order to actually exercise their role as citizens in a democracy. And that means a lot of things, and it's not just voting. In a democracy, the pageantry of voting is absolutely meaningless if the citizenry is not informed. The consent is not meaningful if it's not informed. And unfortunately, that's the way our governments have been operating in the long war period since 9/11, and there are arguments that that's the way it's actually always been. I'm a good friend of Daniel Ellsberg, and he told me in the 1970s during presidential elections, one of the opposition folks who was trying to win the presidency was secretly telling the Vietnamese not to end the war until after the election and all of these kind of things. Politics are a dirty, dirty thing, but when we move beyond the politics we have the individual action and we have the collective action that happens at a subnational scale.

And the unfortunate reality of a lot of surveillance, 2013 was as much about democracy as it was about surveillance, but surveillance and technology was a significant portion of this discussion. And when we look at what happens with that whole surveillance segment, it is an expert conversation. That's an unfortunate reality, right? When you start talking to an average person about metadata, they can understand it absolutely. When you start talking to them about even an exploit chain and how it works, something that's very much arcane and seeing beyond the can of the average person, you're wrong they can understand it, but it takes a lot of time. It takes a lot of explanation. And a lot of people one of the things they don't have today is a lot of free time to engage in a lot of obscure conversations. Legislators today have no idea what the actual meaningful outcomes of these surveillance economies, these global mass surveillance systems really mean. And they don't care because the systemic incentives are such that they are rewarded for turning a blind eye and they're punished for acting against it because there's a giant corporate machine behind this.

And these are the guys who ultimately in the United States will pay you directly if you don't pass a law or in other countries will work very hard to make sure you get positive coverage and opportunities to establish your continued incumbency if you do what they like. That doesn't work the same with individual technologists. That doesn't work the same with the people in this room. That doesn't work with Richard Stallman who could be a very, very rich man, but is instead sitting in this room with you over this week. And I think that is one of the things that we have to remember. When you talk about problems and conflicts that are happening on a social scale, on a human scale, elections are not your only recourse. An election is not going to be changed by a peer reviewed paper. An election is not going to be changed by the academic consensus. Unfortunately, we see this kind of thing in discussions about climate change, right? Science has settled, but political opinion is still for its own self-interest pretending that it's not.

But technology is different because when you talk about hard science, when you talk about hard math, when you talk about code as law, you can export values digitally to every jurisdiction in the world so long as your protocol can't be identified and excluded. If you make your protocol look like every other protocol, if your protocol looks like HTTPS 443, you can change the status quo not in your country, you can change the status quo in the worst of countries and that is a fundamentally powerful thing that has always given me optimism since the beginning. The one thing I will tell you about 2013 that I did not expect is I didn't think we'd still be talking about this in 2019. I thought this was very much going to be a two-week story because it was so specialist. I thought things would be very different than they are today, but rather far more to the negative than the positive.

I have been surprised and gladdened to see that contrary to what the conventional wisdom is, which is that nobody cares that nothing's changed privacy is a front page story every week all around the world today, right? Not a month goes by when you don't see some kind of legal hearing, when you don't see people talking about changing laws. It could be the GDPR in EU, it could be all of these lawsuits against Facebooks and Googles. The world is changing and public opinion is changing, and it is very much going in the favor of people who do not like what these companies are doing rather than in company's favors. The difference is the companies control the system today. The companies control the incentive today. The question is, can they maintain that control? And in all honesty, I think over the span of time the answer is no.

Speaker 5:
Hi, Edward. Thanks for the insights. There's one question that's on the back of my mind. I think as we develop the software and these technologies, we're doing so, I think you sort of mentioned it earlier, that broadly in reaction to the way that the world seems to be going. The way that the social structures that we have, the way that

the establishment seems to be behaving. The software is increasingly allowing distributed, anonymous, or very, very pseudonymous individuals to come together and perform the services that would otherwise have been very focused, very targeted by the powers that be. So you can see this with BitTorrent allowing the hosting of information that would otherwise have to have been placed on a server, run by a particular operating company that could have been taken down. So increasingly, software is moving, it's technology, it's the unstoppable force and it's going to eventually butt its head against the immovable object, which is national governments, national laws, and the establishment.

Something's going to have to give, either the laws are going to change in the same way that copyright law kind of changed a bit with the advent of VCRs or things that we take for granted today, and by that I basically mean writing software will become controlled and illegal in parts. And we already got a taste of this with crypto. In the 90s and early naughties, there was this notion of crypto being weaponized software. The US made it illegal to allow other countries to download stuff. Which way do you think it's going to go?

Edward Snowden:
Well, just a couple of comments. First was about the Bitcoin protocol or Bitcoin, sorry, BitTorrent protocol and the idea that previously these files would be stored on servers on a particular host and that could be taken down. Really that's all the BitTorrent protocol is doing, is making everyone a server. And that's the reality, everything is a server if you're brave enough. When you look at this kind of dynamic, I think that's what the promise of decentralization is all about. It is erasing the old paradigms of how we think about connection. The idea that there was one big server in many clients when instead it could be many clients who are also many servers, and when the client finishes, they become a server and then serve others. These dynamics are transformative, and when the law takes a particular paradigm into consideration of the time it's written and then that paradigm no longer exists, the law necessarily has to change, or it is no longer respected. It's no longer sort of [inaudible 01:02:01]. Excuse me, there's some construction noise here.

When we look at that future, we can't say which direction it's going to go. I can't say one way or the other with certainty, but my suspicion is that it's going to be both. The laws will change, the technologies will change, but the trend of progress over time will be in favor of liberty. It's very easy to look at the problems we have today and give up and go, the world sucks, life sucks and Donald Trump is president, but when you look over 50 years, when you look over 100 years, when you look over 500 years, we're doing very well and I think that will continue. Thank you.

Who is Robert Malone is a reader-supported publication. To receive new posts and support my work, consider becoming a free or paid subscriber.

Type your email... Subscribe