www.freeroman.org

Roman Sterlingov

An Innocent Man Behind Bars

TABLE OF CONTENTS

1. The Story

1.1. Roman Sterlingov's Story

Roman Sterlingov was born in Voronezh, Russia to Tatiana and Michael Sterlingov. His childhood was marked by the trauma and insecurity that characterized the collapse of the Soviet Union. Violence, food scarcity and family turmoil were common. His main reprieve from the destitute world around him came from his grandfather's computer, which he mastered at an early age. When he was 14, Roman and his mother immigrated to Sweden, settling in Gothenburg where he lived until his arrest.

Roman and his mother, Tatiana.

Roman Sterlingov's Bitcoin journey begins in 2011 when he arranged to buy roughly 2000 Euros worth of Bitcoin in a peer-to-peer ("P2P") transaction from another Bitcoin enthusiast at a bar in Gothenburg. In January 2011, the price per Bitcoin was roughly 30 cents. As interest in the new P2P electronic cash system grew, Bitcoin meetups began popping up, bringing together people interested in the new currency. Roman attended many of these meetups in Scandinavia and the Baltics. He helped onboard people to Bitcoin, assisting them in setting up their first wallets and funding those wallets with P2P transactions in return for cash. Roman conducted hundreds of these P2P transactions with individuals he barely knew. At this time, there were no exchanges, so the exchange rates had to be agreed upon based on forum posts and general consensus. During a P2P transaction at one of these meetups, Roman's counterparty informed him that the blockchain is public and that with the transaction ID, he could look up Roman's wallet address and view the total value it held. By this time, the price of Bitcoin had increased astronomically and Roman had accumulated a substantial amount of Bitcoin. This individual recommended that Roman use a Bitcoin mixer to obfuscate the originating source wallet so as not to draw unwanted attention or expose himself to the possibility of a wrench attack where attackers physically threaten you and force you to give up your private keys.

Roman tried several mixing services, ultimately settling on Bitcoin Fog as his favorite. He was attracted to it because he could easily make a new account each time he wanted to send Bitcoin through the mixer, and none of his personal details were required to use the service. Roman

ultimately used Bitcoin Fog to transfer Bitcoin from his older wallets to newer exchanges so that he could more easily spend the profits.

Roman has described his early Bitcoin wallets as “magical” because “they kept increasing in value no matter how much [he] spent”. As Bitcoin continued its global ascent, many new products and services became available. Roman was an early user of Mt. Gox and set up Kraken and Local Bitcoin accounts when they became available. By all measures, Roman was a law-abiding Bitcoiner. He followed KYC protocols, uploading his IDs to these new services. He never sold illegal goods on any dark net market and he tried his best to navigate the patchwork regulatory environment. Never did it occur to him that the FBI had already targeted him and was collecting all of the information he submitted to these platforms.

From 2014 to 2020, Roman attempted a series of business ventures, including a recording studio, a mental health coaching practice, and a VPN service, all of which failed. By 2021, Roman decided to pursue a career as a commercial pilot. He registered for a training program in California and hopped on a plane to Los Angeles. April 27, 2021 turned out to be the last day Roman lived a free life. Upon the plane landing at LAX, Roman was arrested for the operation and administration of Bitcoin Fog and has been imprisoned ever since.

No Direct Evidence

When Roman was arrested at LAX, the Government seized all of his electronic devices – laptops, phones, e-readers, SIM cards, hard drives etc. – none of which contained any evidence linking Roman to the operation of Bitcoin Fog.

The Government’s case was entirely circumstantial. No direct evidence came in at trial of Roman operating Bitcoin Fog. No servers, no logs, no private keys, no communications, no notes, no source code – NOTHING.

1.2. The Government’s Story

Careerism, self-interest, and financial motivations permeate this case in ways that expose internal failings at the Department of Justice. The Government’s investigation began in 2014 at the Russia Desk of the Philadelphia FBI offices. A young FBI analyst named Catherine Pelker distributed an internal memo requesting assistance with investigating Bitcoin Fog. The memo contained cursory analysis and identified Roman Sterlingov as the mixer’s potential operator based on blockchain tracing done by government contractor Chainalysis, Inc. From that point on, the Government’s entire investigation focused on establishing Roman as Bitcoin Fog’s operator, despite never discovering any direct evidence of his involvement. This Government even put Roman under heavy visual and electronic surveillance during his 2017 trip to Miami – turning up nothing.

Two of the original prosecutors on the case, Youli Lee and Zia Farouqi left DOJ not long after this case began. Chainalysis hired Youli Lee to head their Legal Department. Zia Faruqui became a magistrate judge in the District of Columbia issuing decisions favorable to Chainalysis. They were replaced by Chris Brown, and none other than Catherine Pelker. During the pendency of the

government's investigation, Catherine Pelker graduated from law school at Georgetown University and became a federal prosecutor with Washington DC DOJ office. She then became the lead prosecutor on the case.

Until his arrest, Roman had never been to Washington, DC, and didn't know anyone there. This posed a problem for the prosecution. In an effort to manufacture jurisdiction in Washington DC, IRS agents in DC sent some Bitcoin through Bitcoin Fog. This is the sole basis for venue in DC.

The Bitcoin Fog Logo

Upon Roman's arrest, DOJ ran a press release thanking the many individuals and organizations who participated in the investigation. Above all the prosecutors and agencies involved, DOJ highlighted work done by a previously unknown company that appeared nowhere in evidence called Excygent, LLC. Excygent was owned by Aaron Bice, a contractor who the IRS contracted to work as a criminal investigator. WIRED Magazine also ran an article about Roman's arrest before the DOJ publicly announced it, quoting a Chainalysis executive saying that the arrest proved that their type of blockchain tracing worked. Shortly after the arrest, Chainalysis bought Excygent for an undisclosed sum, and initiated a Series E funding round. To date, it is unclear what Excygent contributed to the investigation.

The Government chose not to pursue leads, and from the day Catherine Pelker distributed the internal memo, focused their investigation on establishing Roman as the operator of Bitcoin Fog, rather than discovering who its real creator was. As with many other cases, the Government was motivated in securing a conviction rather than discovering who the true culprit was.

During the trail, the Government manufactured evidence, misattributed statements, drew inaccurate conclusions from circumstantial evidence, and repeatedly linked the operation of Bitcoin Fog to unrelated criminal activity – all of which is on the record. The Court allowed the government to introduce expert testimony that had no scientific basis nor known error rates, allowing it in purely on the basis of self-serving anecdotal statements from law enforcement. The Defense was denied full access to Chainalysis Reactor, the blockchain surveillance tracing software used in the investigation. The judge accepted every expert proffered by the Government while repeatedly denying the Defense the use of experts who are in the top of their fields. Upon receiving a verdict in their favor, the Government sought a sentence of no less than thirty years in prison – an astonishingly harsh sentence for a non-violent crime.

Chainalysis, after initially implying in the press that their blockchain tracing led to Roman, explicitly denied making any attribution to Roman both in their expert report and in trial testimony. Since the conclusion of trial, Chainalysis has admitted to substantial inaccuracies in their digital forensics. In December 2024, Chainalysis confessed that they overstated the amounts stolen by North Korean hackers by over 33% or roughly 340 million dollars.

1.3 What Really Happened

Roman was likely set up as a patsy. Best we can tell, Roman conducted P2P transactions at those early meetups with the individual or individuals who set up Bitcoin Fog. Whoever set up Bitcoin Fog had a comprehensive understanding of the blockchain's ability to be surveilled and traced. It is unlikely whoever set up Bitcoin Fog would have KYC'd accounts directly linked to subsequent transactions. Considering his activity in the meetup scene, it is likely that Roman was targeted as a source of 'clean' Bitcoin that could not be traced back to the actual culprits.

It is likely the Government zeroed in on Roman because he was the only KYC'd address they could find. Chainalysis' forensics skip over multiple non-KYC'd BTC addresses and identify Roman's KYC'd Mt. Gox address as the root source of funds used to set up a clearnet website marketing Bitcoin Fog.

Roman (bottom right) out for dinner with his friends.

2. WHY THIS MATTERS

Roman could be any of us. Anybody who has done a P2P transaction with BTC could end up like Roman under the Government's unique and novel prosecutorial theories.

2.1. IP Overlap Analysis

The Government relied on a unique and novel IP overlap analysis method that had never been done before by the Government's expert. This FBI analyst stated that she believed Roman was in control of a particular email address related to Bitcoin Fog because the Bitcoin Fog email address used a VPN server within a few minutes of Roman using the same server for his email. The IP address in question was linked to a European VPN service that had thousands, if not tens of thousands of other users on it, any of which could have been identified as the operator of Bitcoin Fog under the Government's imprecise IP Overlap Analysis. This analysis was done without any server logs.

DOWNSTREAM LIABILITY HYPOTHETICAL

Imagine an individual pays for a coffee with a $20 bill. That bill is then handed to a third party as change for a later purchase at the coffeeshop. This third party then uses the same bill to tip a busboy at a hotel. The bill then changes hands 19 more times. Later that night, the same bill is used to purchase a gun that is used in a murder. The individual who bought the coffee had nothing to do with the murder, but if you use the tracing theories applied by the Government in Roman's case, that individual would be facing trial for a crime they didn't commit - just like Roman.

Downstream liability is not applied when it comes to the cash. It should not be applied to cryptocurrencies for the same reason. But that's what's happened here.

To present a particular Bitcoin address as belonging to a particular individual, the Government should have to establish ownership through that individual's possession of the private keys to that address. No private key came into evidence in this case.

2.2. Inaccurate Forensics

Chainalysis's inaccurate digital forensics directly led to the wrongful conviction of Roman Sterlingov. There are no standards in the field of blockchain forensics. This is something that needs to be changed. Despite never having conducted an inquiry into the accuracy of their forensic techniques, having no idea as to the false positive rates or false negative rates of their clustering methodologies, and presenting no peer-reviewed papers attesting to their forensics' accuracy, Chainalysis was permitted to present tracing evidence in this case.

2.3. Manufactured Venue

Anyone who operates a website anywhere in the world is at risk of being hailed into an American court of the Government's choosing under the jurisdictional theory used in this case. If the Government can acquire venue simply by interacting with a website, they can establish venue in favorable jurisdictions, as happened here.

Roman posing on a cannon while on a family trip.

2.4. Downstream Liability

The Government's blockchain tracing strategies as applied against Roman risk imposing downstream liability upon anyone who uses digital assets. All links on the blockchain between Roman and the operation of Bitcoin Fog were separated by multiple unknown Bitcoin addresses, but the Government attributed all wallet addresses to him despite not having any private keys.

2.5. P2P Rights

This case is at the forefront of the assault on P2P rights. The Bitcoin whitepaper was titled "Bitcoin: A Peer-to-Peer Electronic Cash System". Bitcoin, and all following cryptocurrencies are based on the premise that the asset can easily be traded P2P. Everyone in the United States has a right to participate in commerce peer-to-peer. Yet, throughout the trial, the Government emphasized P2P transactions as suspicious because they could not be identified, attempting to taint them as inherently criminal.

2.6. Financial Privacy

There are many statutes in the United States that protect an individual's right to financial privacy. The transparent, public and decentralized nature of the Bitcoin blockchain allows governments and bad actors the capabilities to view financial information that would not be accessible in the fiat system. Privacy on the blockchain has been a contentious issue since the early days of Bitcoin. Privacy services like Bitcoin Fog, Tornado Cash and Samourai Wallet grew to meet the demand for privacy on the blockchain.

3. Transcript Quotes

3.1. Does the Blockchain have an Administrator?

> Judge Moss: I'm sorry. Is there -- I'm going to convey my ignorance on the topic. Is there an administrator for Bitcoin that maintains the blockchain? Who maintains that?
>
> Daubert Hearing Tr.
> 52:18-21 (Jun. 23, 2023)

After locking Roman up pretrial for the better part of three years based on the weight and credibility of the evidence, Judge Moss asked if there was an administrator to the blockchain. The Bitcoin blockchain is a decentralized ledger that is not controlled by any particular entity. There is no administrator to a decentralized ledger.

3.2 Chainalysis Never Attributed Bitcoin Fog to Roman

> Mr. Ekeland: …Now, if I recall your testimony correctly, you've made no attributions regarding Mr. Sterlingov anywhere in your expert report, correct?
> Ms. Bisbee: Correct
> Mr. Ekeland: And the only place that Mr. Sterlingov's name appears on your expert report is on the title page, correct?
> Ms. Bisbee: Correct.
>
> Daubert Hearing Tr.
> pp. 120:21-21:2 (Jun. 23, 2023).

Chainalysis expert witness Elizabeth Bisbee, testified that Chainalysis made no attribution regarding Roman anywhere in their expert report. No direct evidence was ever presented of Roman operating Bitcoin Fog.

3.3 No Peer-Review of Chainalysis' Tracing Methods

> Mr. Ekeland: As you sit here today, can you point or direct me to or cite any scientific paper or any kind of peer-reviewed paper or any kind of independent analysis that discusses the accuracy rate of Chainalysis Reactor's coinjoin identification methodology?
> Ms. Bisbee: No.
> Mr. Ekeland: As a matter of fact, in your entire expert report, you don't cite to a single scientific peer-reviewed paper attesting to the accuracy of Chainalysis Reactor, do you?
> Ms. Bisbee: No.
>
> Daubert Hearing Tr.
> pp. 122:17-23:1 (Jun. 23, 2023).

Elizabeth Bisbee admitted in pretrial *Daubert* Hearings that Chainalysis' methodologies and Reactor tracing software had never been peer-reviewed and that no independent inquiry had ever analyzed the accuracy of their software.

3.4 No Inquiry into Chainalysis Reactor's Accuracy

> Mr. Ekeland: Is it your testimony that Chainalysis Reactor is 100% accurate?
> Ms. Bisbee: No.
> Mr. Ekeland: And are you aware of any internal analysis at Chainalysis of the error rates for Chainalysis Reactor?
> Ms. Bisbee: No
>
> Daubert Hearing Tr.
> pp. 139:19-24 (Jun. 23, 2023).

Despite this testimony, Judge Moss allowed Elizabeth Bisbee to testify at trial and allowed in evidence from Chainalysis Reactor.

3.5 The New Hard Drive

> Ms. Pelker: CS Mazarin, could you explain what the significance, if any, is of all of this being completely zeroed out?
> Ms. Mazars: Having a drive have only zeros and no other information, that's generally something a user has to do to a drive. If you take a hard drive new, out of the box, and look at what all the bytes are, sometimes they do have some data, although not actual files, here and there. To get a drive to look like that, you have to do what's known as zeroing it out, or wiping it. This is, for example, what I do with any drive I'm about to use for forensics. I overwrite it with all zeros.
>
> Trial Tr. (Ms. Mazars Direct) 93:14-23 (Feb. 28, 2024)

FBI Investigator Ms. Mazars' testimony was littered with misattributions and misrepresentations. At one point in the trial, she testified that a hard drive on the server Roman used for his VPN company had been wiped, and that she could tell it had been wiped because the hard drive had all zeros. The Government used this testimony to argue that Roman must have had a kill switch that zeroed out this server when he was arrested, and that the drive must have been part of the hardware facilitating the operation of Bitcoin Fog. Even though Roman's VPN server was under surveillance for months, there was no evidence of any Bitcoin Fog traffic.

The model of hard drive in question contains all zeros when it is bought new, like a lot of hard drives. Roman testified that his VPN company never required use of the second server blade, and the Government did not find any kill switch, or anything related to Bitcoin Fog on Roman's devices.

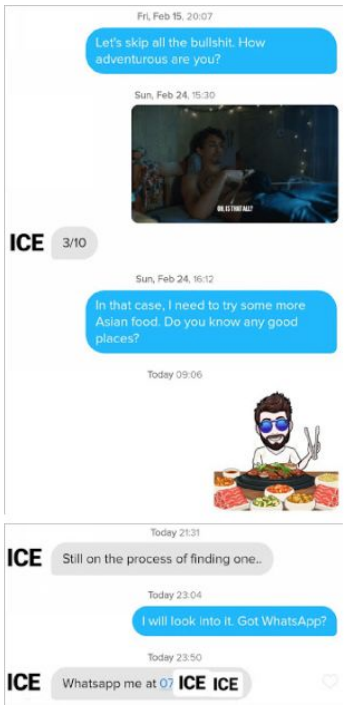
3.6 The e-Book Image

Government Exhibit #721: Tinder chat mentioning money laundering. Misattributed to Roman by FBI investigator Ms. Mazars.

Ms. Pelker: When the government was reviewing the table extraction, did Exhibit 721 appear to you to be part of a dating ebook?
Ms. Mazars: No.
Ms. Pelker You have now heard the defendant's testimony. Do you have any reason to doubt that it was originally part of a dating ebook?
Ms. Mazars: I have no reason to doubt that.
Ms. Pelker And not drafted by the defendant?
Ms. Mazars: That is correct.
Ms. Pelker If you had seen that it was part of an ebook, would you have testified to this exhibit in that way?
Ms. Mazars: Not at all.
Ms. Pelker The government moves to withdraw Exhibit 721 and passes the witness.

Trial Tr. (Ms. Mazars Re-Direct) p. 60:4-17 (Mar. 7, 2024).

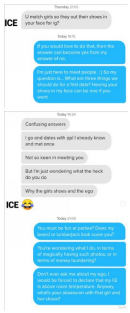
FBI Investigator Ms. Mazars, the same individual who performed the questionable IP Overlap Analysis, misattributed this Tinder chat to Roman. She testified that the above image was a screenshot from Roman's devices in which he discussed money laundering. The image in fact came from an e-book on Roman's e-reader that was seized by the Government. The book was titled "The Message Game" by a pick-up-artist named Ice White. The Government appears to have manipulated the PDF, cutting out the books text and watermarks to make it look like a Tinder chat. Roman never even had a Tinder account.



Still no response, another bump sent.

Her communication is almost useless.

However, I got it.



Tinder

She opened. Interesting but weird question referring to one of my photos on Instagram, inspired by a scene in The Wolf Of Wall Street where Jordan Belfort is tempted by his wife taking her panties off.

Well, she's a mean one.

Page 115 of "The Message Game" by Ice White.
Note the Tinder chat in the bottom left of the page, and the author's watermarks.

3.7 No Direct Evidence

Mr. Ekeland: When you searched Mr. Sterlingov's devices, you didn't find any of the private keys to the Bitcoin Fog cluster?
Ms. Mazars: No.
Mr. Ekeland: And you didn't find any of those private keys to the Bitcoin Fog cluster in any of Mr. Sterlingov's private notes?
Ms. Mazars: No.
Mr. Ekeland: And you didn't find any administrator passwords to Bitcoin Fog in his decrypted password vault?
Ms. Mazars: Not labeled as such, no.
Mr. Ekeland: And you didn't find any log-in credentials to the Bitcoin Fog servers in any of Mr. Sterlingov's devices?
Ms. Mazars: There were a lot of log-in credentials, but none of them were labeled for Bitcoin Fog.
Mr. Ekeland: And as far as you were aware, none of them were to Bitcoin Fog?
Ms. Mazars: Not that I am aware, no.
Mr. Ekeland: And the phrase Bitcoin Fog doesn't appear anywhere in any of his devices?
Ms. Mazars: Not that I saw, no.
…
Mr. Ekeland: And the phrase Bitcoin Fog doesn't appear anywhere in his notes?
Ms. Mazars: No, not that I saw.

Trial Tr. (Ms. Mazars Cross-Examination) 5:24-6:20 (Feb. 29, 2024)

The Government found no direct evidence of Roman operating Bitcoin Fog. This is, in part, what makes this case so infuriating. Roman is innocent. The Government found no private keys to any of the wallets associated with Bitcoin Fog, no admin passwords, no log-in credentials, no mention of Bitcoin Fog anywhere on any of his devices, no communications about the operation of Bitcoin Fog. Nothing! The evidence is entirely consistent with him being innocent because he is.

3.8 No Trace of Bitcoin Fog on Any of Roman's Devices

> Mr. Ekeland: And in relation to the clearnet website www.BitcoinFog.com, you didn't find a trace of that on any of his devices, did you?
> Ms. Mazars: No.
>
> Trial Tr. (Ms. Mazars Cross-Examination 7:5-8(Feb. 29, 2024)

The clearnet website that the bulk of the Government's inaccurate blockchain tracing relates too was a key piece of evidence for the Government. However, Ms. Mazars testified that there was no trace of that website on any of Roman's devices.

3.9 The Government Never Acquired Bitcoin Fog's Ledgers or Source Code

> Mr. Ekeland: The government doesn't have the Bitcoin Fog ledgers, do they?
> Ms. Mazars: No.
> Mr. Ekeland: And you haven't examined any of the source code to Bitcoin Fog, have you?
> Ms. Mazars: No, not that I am aware.
>
> Trial Tr. (Ms. Mazars Cross Examination 8:9-14 (Feb. 29, 2024)

Perhaps most importantly, the Government never identified or seized the Bitcoin Fog ledgers or source code. The ledgers and source code would have constituted substantial direct evidence of the operation of Bitcoin Fog, but the Government never found them. If Roman had been the operator of Bitcoin Fog, he would have been in possession of the ledgers and Bitcoin Fog source code. The Government couldn't find them in Roman's devices because they got the wrong guy!

4. News Articles

Law360 – January 28, 2025
Silk Road Pardon Sparks Hope for More Crypto Clemency
https://www.law360.com/articles/2287486/silk-road-pardon-sparks-hope-for-more-crypto-clemency

Bitcoin Magazine – January 23, 2025
Ross Is Free, But This Is Far From Over
https://bitcoinmagazine.com/takes/ross-is-free-but-this-is-far-from-over

Bloomberg – November 8, 2024
Crypto 'Mixer' Gets 150 Months for Bitcoin Fog Money Laundering
https://www.bloomberg.com/news/articles/2024-11-08/crypto-mixer-gets-150-months-for-bitcoin-fog-money-laundering

The Crypto Times – August 17, 2024
Bitcoin Fog Founder Begs Mercy Post Money Laundering Conviction
https://www.cryptotimes.io/2024/08/17/bitcoin-fog-founder-begs-mercy-post-money-laundering-conviction/

Cointelegraph – August 16, 2024
Crypto mixer founder argues 30-year prison sentence is 'unwarranted'
https://cointelegraph.com/news/bitcoin-fog-crypto-mixer-prison-sentence-unwarranted

Bloomberg – March 27, 2024
The Science of Crypto Forensics Survives a Court Battle- for Now
https://www.wired.com/story/the-science-of-crypto-forensics-court-battle/

CoinDesk – March 13, 2024
How a Bitcoin Mixer Laundering Conviction Might Be Appealed
https://www.coindesk.com/opinion/2024/03/13/how-a-bitcoin-mixer-laundering-conviction-might-be-appealed/

Cointelegraph – March 12, 2024
Bad Blockchain Forensics Convict the User of a Bitcoin Mixer – As its Operator
https://cointelegraph.com/news/bad-blockchain-forensics-convict-roman-sterlingov

Bloomberg – March 12, 2024
Crypto 'Mixer' Convicted of Money Laundering on Bitcoin Fog
https://www.bloomberg.com/news/articles/2024-03-12/crypto-mixer-convicted-of-money-laundering-on-bitcoin-fog

Unchained Crypto – March 12, 2024
Bitcoin Fog Operator Found Guilty of Conspiracy, Money Laundering for Darknet Markets
https://unchainedcrypto.com/bitcoin-fog-operator-found-guilty-of-conspiracy-money-laundering-for-darknet-markets/

Bloomberg – February 27, 2024
He Laundered $4.5 Billion in Bitcoin. Now He's a US Government Witness
https://www.bloomberg.com/news/articles/2024-02-27/crypto-heist-mastermind-ilya-lichtenstein-turned-us-cooperating-witness

Crypto Slate – February 27, 2024
Bitfinex Hacker Testifies in Bitcoin Fog Trial as Government Witness
https://cryptoslate.com/bitfinex-hacker-testifies-in-bitcoin-fog-trial-as-government-witness/

Bloomberg – February 13, 2024
Crypto Launderer Kept Identity 'Hidden in the Fog,' US Alleges
https://www.bloomberg.com/news/articles/2024-02-13/crypto-launderer-kept-identity-hidden-in-the-fog-us-alleges

Cryptopolitan - September 16, 2023
How Trustworthy Is Chainalysis Data, or is it Junk Science?
https://www.cryptopolitan.com/how-trustworthy-is-chainalysis-data/

Bitcoin Magazine – September 15, 2023
Bloomberg Calls Questioning of Chainalysis 'Smear Campaign', Raises Questions of Media Integrity
https://bitcoinmagazine.com/culture/bloomberg-calls-questioning-of-chainalysis-smear-campaign-raises-questions-of-media-integrity

Be(in)Crypto - September 15, 2023
Lawyers Labled Chainalysis Data Unreliable "Junk Science"
https://beincrypto.com/lawyers-labeled-chainalysis-data-unreliable-junk-science/

Bloomberg - September 14, 2023
Wall Street-Backed Crypto Tracer Faces 'Junk Science' Attack
https://www.bloomberg.com/news/articles/2023-09-14/bitcoin-fog-case-puts-spotlight-on-chainalysis-crypto-tracing

Bitcoin Magazine - August 31, 2023
Chainalysis, The Theranos of Blockchain Forensics?
https://bitcoinmagazine.com/technical/chainalysis-the-theranos-of-blockchain-forensics

Bitcoin Magazine - August 28, 2023
Chainalysis Investigations Lead in 'Unaware' of Scientific Evidence The Surveillance Software Works
https://bitcoinmagazine.com/technical/chainalysis-investigations-lead-is-unaware-of-scientific-evidence

Bitcoin Magazine - August 15, 2023
Your Financial Privacy is Under Attack: How State-Sponsored Attacks on Bitcoin are Growing
https://bitcoinmagazine.com/culture/state-sponsored-attacks-on-bitcoin-privacy-are-growing

Cointelegraph - August 9, 2023
CipherTrace Expert says Chainalysis Data Contributed to 'Wrongful Arrest' of Alleged Bitcoin Fog Founder
https://cointelegraph.com/news/cipher-trace-expert-says-chainalysis-data-contributed-wrongful-arrest-alleged-bitcoin-fog-founder

CoinDesk - July 24, 2023
Chainalysis Testimony Raises the Question: Do We Know How Well Any Such Software Works?
https://www.coindesk.com/consensus-magazine/2023/07/24/chainalysis-investigations-lead-is-unaware-of-scientific-evidence-the-surveillance-software-works/

WIRED - August 2, 2022
Bitcoin Fog Case Could Put Cryptocurrency Tracing on Trial
https://www.wired.com/story/bitcoin-fog-roman-sterlingov-blockchain-analysis/

5. Podcasts & Keynotes

MoneroTopia Conference – Mexico City – November 16, 2024
The Criminalization of Privacy: Ongoing Efforts by DOJ to Clamp Down on Privacy

Bitcoin Conference Hong Kong – Hong Kong, China – May 10, 2024
Blockchain Surveillance State: The Disturbing Prosecution of Roman Sterlingov
https://www.youtube.com/watch?si=AlWUAu1L_Bhg-Atk&v=Ue8RyPVYxtg&feature=youtu.be

MoneroTalk Podcast – Dallas Texas – March 16, 2024
#304: Roman Sterlingov's Bitcoin Fog Conviction Based on Chain Analysis Sets Dangerous Precedent
https://www.monerotalk.live/monerotalk-304

Finney Forum – Dallas, Texas – March 16, 2024
Blockchain Surveillance State: The Disturbing Prosecution of Roman Sterlingov
https://finneyforum.com/

PubKey Bitcoin Lightning Meetup – January 25, 2024
Update on the Bitcoin Fog Trial

What Bitcoin Did with Peter McCormack – May 24, 2023
WBC #662: The Case of Roman Sterlingov with Tor Ekeland and Mike Hassard
https://www.whatbitcoindid.com/podcast/the-case-of-roman-sterlingov

Bitcoin Conference 2023 – Miami, Florida – May 20, 2023
The Disturbing Bitcoin Prosecution of Roman Sterlingov
https://www.youtube.com/watch?v=x8neTHW3BdU&pp=ygUfcm9tYW4gc3RlcmxpbmdvdiAgYml0Y29pbiBtaWFtaQ%3D%3D

The Swiss Road to Crypto with Didier Boreal – Zurich, Switzerland – May 7, 2023
Roman Sterlingov – Profits over Justice – Disturbing ChainAnalysis Based Prosecution
https://podcasts.apple.com/us/podcast/roman-sterlingov-profits-over-justice-disturbing-chainanalysis/id1494483658?i=1000612040995

MoneroTopia Conference – Mexico City, Mexico – May 7, 2023
Chainalysis Panel Discussion with ArticMine, Peter Todd, Tor Ekeland and Mike Hassard
https://www.monerotalk.live/chain-alysis-panel-monerotopia23

MoneroTopia Conference – Mexico City – May 5, 2023
Profits Over Justice: The Disturbing Prosecution of Roman Sterlingov
https://www.monerotalk.live/profits-over-justice-the-disturbing-crypto-prosecution-of-roman-sterling-monerotopia23

Vonu Podcast – April 29, 2023
TVP #184: ChainAnalysis Coercion & Quack Science: The Troubling Case of Roman Sterlingov with Tor Ekelend, Mike Hassard, & SW from Samourai Wallet
https://vonupodcast.com/tvp-184-chainanalysis-coercion-quack-science-the-troubling-case-of-roman-sterlingov-with-tor-ekelend-mike-hassard-sw-from-samourai-wallet/

Bitcoin im Ländle Conference – Stuttgart, Germany- April 28, 2023
Profits Over Justice: The Disturbing Prosecution of Roman Sterlingov

Café Holzmarketperle Bitcoin Meetup – Berlin, Germany – April 25, 2023
Profits Over Justice: The Disturbing Prosecution of Roman Sterlingov

Stemmerhof Studios Bitcoin Meetup – Munich, Germany - April 23, 2023
Profits Over Justice: The Disturbing Prosecution of Roman Sterlingov

Volkshaus Theatersaal Keynote Presentation – Zurich, Switzerland - April 19, 2023
Profits Over Justice: The Disturbing Prosecution of Roman Sterlingov
https://www.youtube.com/watch?app=desktop&si=LokNetH7ez1X3nB0&v=nUrwPb4sTVk&feature=youtu.be

Citadel Dispatch – April 13, 2023
CD#100: The Disturbing Chainalysis Led Prosecution of Roman Sterlingov with Mike Hassard and Tor Ekeland
https://www.fountain.fm/episode/kx4hjej0NwYtpjEQrqN1

MoneroTalk Podcast - January 30, 2023
The Bitcoin Fog Mixer Case Puts the Blockchain Analytics Ecosystem on Trial
https://open.spotify.com/episode/6OUxBvN3ARWHHnFTSJhdEr?si=kZMkWvliSEioB6hzi6A4TQ

Roman waiting for a flight.

6. How to Help

DONATIONS TO ROMAN STERLINGOV'S LEGAL DEFENSE FUND

We cannot do this without you. Appeals to the Federal Circuit Court of Appeals are costly, involving significant attorney fees, court filing costs, and other legal expenses. Every dollar raised brings us one step closer to overturning this unjust conviction. All donations are final, no refunds, and will be used at the sole discretion of the Appellate team for Roman's Appeal.

This is a pivotal moment not just for Roman but for everyone who values financial privacy and fairness in the legal system. Together, we can fight back against this injustice and ensure a brighter, freer future for all cryptocurrency users.

Thank you for standing with Roman Sterlingov.

Bitcoin (BTC) Donation Address

bc1qqqv8xemhhpdw2h0dpah7z5kvqzy6awnhh6ccnz

Monero (XMR) Donation Address

84yR8q98HBVPQRsoF1rcqQ5eu3FbLhAaYTSM3XMa3Q1eWH6BunADyHKE8CssJabJvcNdrD
VT1efJwFYRfJtwAiZNFXud2yU

7. Contact Information

Tor Ekeland

Tor is a trial and appellate lawyer. He's best known for representing hackers and white-collar defendants in federal criminal court and on appeal. Tor also counsels businesses and individuals under investigation by the United States Department of Justice, and those needing counseling on U.S. and international computer laws.

Prior to starting the Firm, Tor was a complex commercial and securities litigator with the New York City office of Sidley Austin, LLP. At Sidley, he gained in depth experience representing individuals and business entities under government investigation by the United States Department of Justice for violations of the Foreign Corrupt Businesses Act, the SEC for securities fraud, as well as working on litigation involving complex financial derivatives. Businesses often turn to Tor for counseling on virtual currencies such as Bitcoin, ICO's, and the intersection of U.S. securities and computer laws.

Email: tor@torekeland.com
Twitter/X: @TorEkelandPLLC

Michael Hassard

Michael Hassard is a Senior Associate at Tor Ekeland Law, based in New York. He represents computer hackers, Bitcoiners, and white-collar defendants in federal courts across the United States, focusing on cryptocurrency-related cases. A strong advocate for financial privacy, net neutrality, and sound digital forensics, Michael frequently speaks on these topics at conferences and on podcasts.

In addition to trial and appellate work, Michael advises cryptocurrency businesses and decentralized financial organizations on compliance matters and regulatory approvals in the United States.

Email: Michael@torekeland.com
Twitter/X: @mikehassard