

CORA BORRADAILE ON PHONE EXTRACTION, CLONING AND KEYWORD WARRANTS

The Final Straw is a weekly anarchist and anti-authoritarian radio show bringing you voices and ideas from struggle around the world. Since 2010, we've been broadcasting from occupied Tsalagi land in Southern Appalachia (Asheville, NC).

We also frequently feature commentary (serious and humorous) by anarchist prisoner, Sean Swain.

You can send us letters at:

The Final Straw Radio
PO Box 6004
Asheville, NC 28816
USA

Email us at:

thefinalstrawradio@riseup.net
or **thefinalstrawradio@protonmail.com**

To hear our past shows for free, visit:

<https://thefinalstrawradio.noblogs.org>



The Final Straw Radio

Cora Borradaile speaks, who works around issues of tech security in movements, is an associate professor at OSU and sits on the advisory board of the Civil Liberties Defense Center. The conversation focuses on recent tactics used by law enforcement in order to access cell phone data.

Aired on November 8, 2020

Security State and The Adoption of More Secure Apps, and also is on the board of the CLDC. Thanks again for having this chat.

CB: It was wonderful talking to you, as always.

TFSR: Well are there any other things you'd like to share with the audience concerning digital tech or any insights?

CB: I did want to share one thing. You asked about them getting this data, and is this illegal search and seizure. There are still strange laws that date back to the 80's, for example e-mail can be accessed by law enforcement from somewhere like Google with just a subpoena and not a warrant, necessarily. For a law enforcement agency to get information that would otherwise be deemed illegal search and seizure, they need to get a warrant from a judge that proves probable cause for them to get that data or that physical item. But if it's email on a server held at Google then they don't need to prove probable cause and they just need a subpoena which is essentially just a 'Please can I have this information.' I think that's where these keyword searches are coming in, I'm not sure that they actually need to have a warrant for those. So that's maybe one extra detail on that front.

TFSR: In those instances it's in one centralized place, although if your doing a keyword search... Yeah I don't know- I guess I don't know how Google works on the inside and if it's just constantly categorizing what people are typing into its different services for later use and then providing that in easily digestible pills to law enforcement. If you're sending email and it's unencrypted, it's probably getting Hoovered up somewhere and fully readable anyway.

CB: Depends on who your adversary is. I don't think the Portland police department has access to a big Hoover of data on a global scale, but they certainly can ask Google for all of the emails of the activists whose email addresses they've extracted from the phones they confiscated during protests.

TFSR: Cora, thank you so much. Cora is an associate professor of Computer Science at Oregon State University with a focus on

This week on the The Final Straw you'll hear me speaking with Cora Borradaile, who sits on the advisory board of the Civil Liberties Defense Center and works around issues of tech security in movements and is an associate professor at OSU.

We discuss the use of phone cloning by US Marshall's and other law enforcement while engaging protestors in Portland, OR. We talk about UpTurn's recent report concerning widespread use of cell-phone extraction tools to copy and search the contents of cell phones captured during interactions with cops. Finally, we talk about Keyword Searches, where (often without warrants) google hands over information from peoples google searches to law enforcement.

Links to more information about these topics can be found by searching for the episode title at TheFinalStrawRadio.NoBlogs.org

TFSR: So I'm speaking with Cora Borradaile who is on the advisory board of the Civil Liberties Defense Center or CLDC and we spoke before about a range of issues in May of this year, and before the George Floyd uprising and the resulting ACAB Spring. During the uprising researchers, journalists, and activists saw that applications of new, or new to us, surveillance methods were being used by security forces against the populace in the so called US, so I was hoping to pick Cora's brain a bit about this and see, especially since upcoming months in the US also might get a little spicy with the election and all. Thank you Cora very much for taking the time to have this conversation.

Cora Borradaile: Yeah, it's great to talk to you.

TFSR: So just to list off a few things, like this summer we saw the use of military drones surveilling and sharing information with law enforcement in Minneapolis, lots of militarized gear being brought out in the streets across the US, or for late May at least protests against police violence, and collusion with para-state white supremacists have been ongoing in Portland, Oregon. In July we saw the deployment of federal officers from the Department of Homeland Security (DHS) including Customs and Border Patrol (CBP), and the Department of Justice (DOJ) sent out to fight against protesters in the streets of Portland and attack and kidnap people. Including journalists from that and other cities. the US Marshalls also had their own aerial surveillance to track crowds in Portland, it came out this summer. On the tech side of things, the public got wind, apparently from leaks within the department of homeland security, that DHS had been cloning activists' cell phones. Could you talk a little bit about this and what cell phone cloning is?

CB: Yeah, from that report there were very few details so a lot of it is guesswork as to what could possibly be going on. I could imagine two different ways in which their cloning cellphones- One which is

a new photo in the memory of your computer or cellphone, you go to the shelf and you find out 'Oh, there's supposed to be space here because according to the card catalog there's nothing stored here, so this old data must be something that I don't need anymore, now I'm going to delete that old stuff.' Right, 'I'm going to remove that book from the shelf whose existence was deemed not there anymore by the card catalog, I'll throw it away now and put my new one in.' So it's not until you use the memory again that the old information actually gets deleted.

TFSR: At least on computers there's – for instance I had to reinstall my operating system recently. And when I installed it I went to encrypt the home folder and the file system and it asked 'Do you want to overwrite everything else on the hard drive?' Is that what you're talking about?

CB: Yeah, so that would be the equivalent of actually going to all the shelves of the old library and removing all of the old books. So that's pretty common when you're setting up on a computer but I've never seen that option on a phone. I'm wondering, does a factory reset actually delete all of that information? I haven't noticed that myself.

TFSR: Microwaves. I mean I saw –

[laughter]

TFSR: Yeah, I got nothing.

CB: Drop your phone in the pool, start over.

TFSR: They invented this thing called rice though, where if you put your phone into a bag of rice it extracts the water... and the data...

[laughter]

in that Upturn article that I thought were useful. Like if someone deletes information on their phone, are they actually deleting information off of their phone, and are there appropriate or useful, good tools for actually wiping data off of phones or does it just kind of sit there?

TFSR: –MAGNETS–

CB: I don't know of a good tool. I think that if you do a factory reset of your phone that's most likely to help make that data inaccessible. Even then, is it actually getting completely deleted? It might not be. You have memory on your computer or on your cellphone, and when you delete something it just kind of takes the index away... I'm trying to use an analogy that people would remember. Do people remember libraries and card catalogs? (laughs) All of my analogies are too old.

TFSR: I think it's fair, go ahead.

CB: You think people will remember?

TFSR: I think so, or they've heard the analogy enough they'll recognize what a card catalog is.

CB: They've seen a movie with an old-timey library and card catalogs?

TFSR: Ghostbusters

CB: So, you have a big library with books on all the shelves and the way you know where to find a book is to go to the card catalog. You look up the book that you want and you find its listed location on the shelf and then you go to the shelf and you find the book. Well now, when you delete a file from a computer, really all you're deleting is the card from the card catalog. So when it comes time to put

scarier than the other. The more likely I think, is the less scary version which is if they manage to physically get your cell phone, like if you're arrested and your cell phone is confiscated from you. Even if it's confiscated temporarily, then they're copying everything from your cell phone and possibly making a new cell phone that behaves just like your cell phone. So it would allow them to intercept calls possibly receive messages that you were intended to receive.

The scarier version but probably less likely, is the ability for them to be able to do the same thing without having the need to confiscate your phone to do so. That feels unlikely to me that they were doing that. If it was some sort of remote cloning I would gather that they were just cloning the sort of network ID of your phone, and not the contents of your phone. This would still allow them to do things like intercept calls, and intercept data, but in both scenarios I think end-to-end encryption (E2E) apps that you use like Signal or Keybase or Wire, that enable E2E encryption, I think the messages you're receiving there would still be safe and that the cloned device shouldn't be able to have the keys enabled to decrypt those messages that were intended for you. And even traffic that is encrypted – if you are visiting a website on your phone that your accessing via HTTPS, where the S stands for Secure – I think that even they wouldn't be able to see the contents of that web page either because there is a key exchange that happens between you and the web server that they would have to play man in the middle on. Which is more complicated to do in a way that you wouldn't be able to tell that something was going wrong.

All that's to say, it's still scary and I think if you have poor encryption practices like keeping your phone in an unlocked form, they have access to all of your encryption keys for things like Signal and Keybase and whatever other secure messaging apps you might be using. You should do whatever you need to do to alert everyone you contact with to delete your contact from their messages, groups, and so on. And if you have a phone that is confiscated – and certain-

ly in an unlocked form – I would not trust that phone again. If your phone is confiscated but it was locked at the time and presumably you have a good password so they can't easily unlock your phone, I would still maybe do a factory reset of your phone and start fresh by installing everything over again.

TFSR: So, I'm not sure what the basis of this is, but conversations that I was having with friends when we were talking about the latter of the two instances that you were talking about- the hypothetical that remotely the cloning of the network ID or SIM connection could be done. It would be similar to you getting a new phone but having the same number, and that if Signal was installed on that device and it was connecting to the same phone number, by a Man in the Middle attack via a cloned SIM, it would appear that the interception could still be happening but that everyone would see a notation that there had been a change in safety number. Is that maybe what would happen?

CB: Yes. That is perfectly said. Right, so for them to be able to both clone your phone and intercept messages without those “safety number has changed” messages happening would be very, very difficult. So yeah, certainly if there are reports of anybody who's had a confiscated phone and then all of a sudden all of their contacts are noticing that their safety number has changed with them, that would be super interesting to find out. —

TFSR: –Or they stopped getting messages.

CB: Also horrifying.

TFSR: Yeah. You know, they noticed that they stopped getting messages, everyone notices that the safety number changed, then that means that hypothetically the cloned phone or whatever would now be in those chats.

your cellphone, if you're not guilty of this minor misdemeanor.' You know, they're just asking permission.

That's one of the things CLDC shoves down the throats of everyone at their trainings, which is don't consent to searches. Just don't do it! Even if they're going to go ahead and do the search, even if you're not consenting to it, say over and over again 'I do not consent to this search.' Have a sticker on your phone that says 'I do not consent to this search.' Because then it can't be used in the court of law at least. The other thing that we've seen over the years is, parallel reconstruction. I don't know if I've seen a well researched example of this but certainly people have hinted that this a common practice, where they'll find out something via methods that wouldn't be admissible in the court of law and then they figure out a way to reconstruct what they know using admissible methods.

TFSR: Oh like in The Wire.

CB: Yeah, exactly. So that's something that might be why they're getting information that they can't necessarily use. The other part is just general intelligence work. It's not necessarily going to be used to arrest anyone, it's not necessarily going to be used in a court of law, but they just want to know what's going on, and so are going to collect as much data as they can. Unless you find out about it and unless you prove harm in a court of law, then how are you going to stop it from happening? Which is why this report about the Google keyword searches and Google Geofencing searches is so important. If we can find out about that and we can get a case brought forth and have it deemed unconstitutional to do this kind of search then that would stop those kinds of requests from happening. Then you could put pressure on a company – even a company like Google – you could put public pressure on them to say 'Don't respond to these requests, they've been deemed illegal.'

TFSR: There are a couple of other, I guess not insights but points

CB: I would avoid Google, I definitely use DuckDuckGo. I prefer DuckDuckGo for selfish reasons, I find the personalized search aspect of Google to be somewhat infuriating. When I search for something I don't want to find what Google thinks I want to find, I want to find the documents related to my search. It's hard to avoid these tools, but I think DuckDuckGo, anything but g-mail for email please, and there are alternatives to Google Docs as well. Cryptpad seems to be getting better. Every month there are improvements. It offers collaborative online editing to documents, all E2E encrypted.

TFSR: **I am going to presume with this question that you are not a lawyer, am I correct in that?**

CB: I am not a lawyer, no.

TFSR: **It seems things like intercepting phone calls, peoples text messages, or getting deep into their cellphones and all of the information that's collected in them for arguably unrelated topics, might overstep into the realm of FISA (Foreign Intelligence Surveillance Act), or might overstep into the realm of one of those amendments that protects our rights against unfair search and seizure. That just doesn't seem to be the case? Or in these instances is it that these methods haven't been brought before courts to be challenged?**

CB: Everything I know about the law I learned from CLDC, and Law & Order in a previous lifetime. So what I do know about these from reading various news articles and conversations with CLDC is, as pointed out by Upturn, a lot of the extraction of data from cellphones was based on consent and not a warrant. It was about a 50/50 split depending on jurisdiction. So this was probably the case of intimidation by a cop to a person with a cellphone, to say 'Oh, well let us check your cellphone'. I'm not sure if they give full disclosure of what they mean by 'let me check your cellphone', right? (laughs) 'Let me copy everything there is on your cellphone off

CB: So I don't know if it's as simple as that, because when you add a new device on Signal all the other devices get a notification of that.

TFSR: **Oh I see. So if I had a desktop and at least one cell phone that was getting messages... Yeah, but if that device was no longer getting new messages because the traffic was being routed to a different device, you wouldn't like –**

CB: Right so, your contacts should at the very least get the notification saying that the safety number has changed. If it's a remote clone I think the only way in which the cloned phone would be able to read the messages in preexisting groups, for example, would be if the device was physically confiscated and copied. Because there are encryption keys that are used to start those conversations which are needed.

TFSR: **Do you mean the messages that were in loops before?**

CB: No, to continue to receive messages from conversations that had already been going on. If someone started a new conversation after the cloning then the other people in the conversation might not be able to notice, but if you were continuing a conversation that had started before the cloning I don't think you would be able to get that information without having physical access to the device and being able to copy over the encryption keys that were used to start those conversations.

TFSR: **Because they're being stored on the phone and not on the server.**

CB: That's right, yeah. So for example, when you add a new Signal device part of what happens is copying over the encryption keys needed to continue conversations. And there's a QR code that, say if you have Signal on your phone and you start using Signal on your desktop, you link those 2 devices so that both devices are able to

receive and decrypt messages that go to you as an identifier.

TFSR: If you know that if someone in your group or one of your friends has changed their number, what's a good verification?

CB: Don't message them on Signal, and ask them, right? Because who knows who's answering. Try to find a different form of communication even if it's via friend or via a regular phone call, but ideally via email or some other band that is unrelated to your phone would be perfect to ask them, 'Hey, I noticed your Signal safety number's changed, what went on?' Most of the time, or every time this has happened to me, the answer's been 'Oh, I had to reinstall my operating system on my phone' or 'I dropped my phone in a pool and had to get a new phone.' That's usually the reason for a safety number changing, but definitely what you want to do is find a different way to ask that, other than using Signal and ideally other than using the phone. Especially if we are worried about cloned phones. Because if you just use a normal SMS text message to send to your friend and your friend's phone has been cloned, then it could be the cops responding saying 'Oh, yeah I had to get a new phone.'

TFSR: I've seen some people do a thing where they ask someone in a group, when their safety number changed, 'Hey could you leave a voice memo with your name and current time that you're recording the memo and send it into the loop?' And that way everyone hears this person's voice, and it's the time when they specifically get asked to record the memo so it's outside of Enemy-Of-The-State-level NSA level operation that's probably not somebody compiling an automated voice message in that person's voice.

CB: Yeah, that's a pretty good method for doing that. As you point out, synthesizing people's voices can be done, but taking into account what your threat level is – are you someone who they're going to be throwing everything at and be able to synthesize your voice in

user accounts every year in the US. So it wouldn't surprise me if Google, instead of just getting requests saying 'Hey, I'd like to have all of the emails associated with email address thefinalstraw@gmail.com,' which seems to be the more straight forward type of request related to a specific account that might be included in a law enforcement issue... probably not though. To expand that to 'Hey, I want to know all of the information you have about people who searched for 'The Final Straw''. So that's the keyword warrant or the keyword search request that happened in this case. We've seen examples of Geofencing warrants happening for Google Maps asking for anybody who has searched for an address within a given region, that there were a few stories about over the last year. So yeah of course, the data is there why not ask for it? Google is not going to say no, why would they?

TFSR: Basically, again by collecting information based on its availability then attempting to apply it. So in this case with the arson, they asked for people who had searched for the address of the house where a car got set on fire within a certain period of time and then cross-referenced that to a Geofence of what phones were in the area within a period of time, and were able to pinpoint and place charges. And not all of the information came out from that, some of the court records are still sealed. It's kind of a frightening application of technology and as you say, a very happy-to-oblige industry.

CB: Yeah. I think the potential for false arrests and harassment of people, like say you happen to find someone in that area who you don't like for one reason or another you can arrest them and hold them for a while even if you have no evidence. Harassment arrests are used all the time by law enforcement and have been for decades, centuries probably.

TFSR: So I guess... use DuckDuckGo if you're going to be committing an – – – ?

and there's no sort of oversight of this, it seems very likely that the sorts of data that they're collecting could be used to build future cases or for building profiles on people for things they haven't actually been accused of so far.

CB: Yup. Phishing for data. Maybe they're just trying to justify the purchase of this stuff. In Oregon they spend half a million dollars on cellphone extraction technologies, Portland alone spent a quarter of a million in a period of 4-5 years. That's a lot of money to justify, right? If you're only using it 3 times a year for homicide cases then maybe you can't justify actually spending that money and you would just farm out, whenever you do need it for something like that, either to a fusion center or a pay-per-service from one of these companies. So it might just be they're partially covering their asses and saying 'Oh yeah, we use it 10 times a week'.

But we've also seen examples of law enforcement agencies that just collect so much data, almost for the purpose of just having data. The LAPD famously uses Palantir which is a horrible company, to do all sorts of data analytics for their region collecting data on pizza purchases and parking passes and all sorts of things that don't seem relevant at all to law enforcement, but it's almost a compulsion to just collect the data and see what they can do with it.

TFSR: Another thing that I had seen was Google was recently in the news when court documents were unsealed in Detroit relating to witness intimidation and arson by an associate of R. Kelly, and this in regards to keyword warrants. Are you familiar with this case and could you talk a little about keyword warrants and what they are?

CB: Yeah, so keyword warrants. I hadn't heard about them before this news story came out earlier this month, but it's not surprising. I certainly was familiar with just how many requests for data Google gets and responds to, affecting hundreds of thousands of

a very short time? For the protest movements we've seen, probably not. However if you are the leader of a protest group, hmm... If you are someone that they're really going to be going after because they think that going after this one person will completely destroy the movement – which I don't think is the kind of movement time that we are in right now which is good, to avoid those specific people who could really destroy a movement – that's a pretty good method.

TFSR: If you could speak to that prior scenario, is that actually copying the contents of a phone? I think that was the subject of the recent article by Upturn called Mass Extraction —

CB: That's right.

TFSR: If you could talk a little bit about what the findings were there. I was kind of surprised yet kind of not surprised to see the local law enforcement here in Asheville spent at least \$49,000, according to their studies, on cell phone extraction tools. But what are mobile device forensic tools, and what do you know about them, how widespread and what kind of stuff do they do?

CB: So these things have existed for a long time. We've been talking about them at CLDC for a long time but this Upturn report is really wonderful for just as you say, how widespread they are. Small police departments have them, medium police departments spend hundred of thousands of dollars on access to this over the course of 5 years, and some of the capabilities were actually, I suppose, not really surprising. But reading them all in one place and knowing how low cost access to that technology is was sobering.

So these cell phone extraction devices, they come in different forms but the kind that is most popularly seen is a small stand alone device that you plug a cell phone into and that stand alone device either tries to break into that phone if it's locked or otherwise just copies all of the content of that phone for later analysis. Some of the

things that were surprising to me was how much was available even when the phone was locked and encrypted. There's a lot of data that is existing in an unencrypted form on your phone.

For example say your phone is locked, you receive a phone call and the name of your contact still shows up, right? It's not the name that your contact is sending you, its not metadata associated with that contact. if your mother is calling you, it probably shows up "Mom" in your phone, and the reason it says that is because your address book has an entry with that phone number and the name "Mom" attached to it. So your address book entries are existing in an unencrypted state, for example.

Some of the other things that were sort of surprising that were pointed out, that exist in this unencrypted state even though your phone was in a locked condition, were Telegram files and Discord files, and files associated with Google mail. I think a lot of this stuff could just be from bad decisions that the app developer made. Like Telegram is not necessarily focused on security, and so for convenience or speed they may just not be hiding that information behind the device encryption.

There was definitely some reporting in that Upturn report about being able to brute force guess passwords and so there are some things that you can do to protect yourself from that, which is to have a long enough password. Or if you have an Apple device you can enable your phone to self-wipe if you have 10 incorrect guesses, for example. Which if you have a small child at home maybe you don't want to do because I almost guarantee you will end up with a wiped phone by the end of the week.

TFSR: With encrypted files, if there are messages or what-have-you that are saved in an encrypted section on the phone would that just get copied and saved, and tested against decryption later? Is that the idea?

CB: I think what's happening in most cases is they're taking a copy of encrypted information, possibly in the hopes that they could decrypt it later or in the hopes that they would be able to get the unlock password from you by other means, like a court order for example. You know, they did point to instances where they were still able to bypass security features like encryption because of security flaws, which is very common. If your phone is badly out of date and you haven't been keeping up with installing security updates, always install your security updates. That's a common thing in computer security, that there are flaws that can be taken advantage of that can allow bad actors to break through otherwise strong encryption. But I think if you're keeping an up-to-date phone, I think that's the best that any of us can do.

TFSR: Another point that was interesting in the article, and I'm glad that they pointed it out, was the sorts of instances when this is being applied to people. You hear about Apple being pressed to give up encrypted information or give a back door when there's a mass shooting, or a sort of incident that may involve multiple conspirators and the loss of life – something very serious. But in the Upturn article they talk about how through their research and requesting of records it showed that a lot of law enforcement agencies, even local law enforcement agencies, are attempting either to pressure people whose devices they get a hold of or apply for warrants to copy peoples' contents of their phones for minor things that they're being accused of.

Like if it's something like shoplifting or graffiti or public intoxication, petty drug charges, sex work, these are a few of the examples that they give. Considering the way that policing works in the United States, and this shouldn't surprise anyone in the listening audience, police tend to focus their attention on poor and racialized parts of the population. So if law enforcement gets people's data, whether by asking for it and pressuring people into it or by using devices, and then saves it for a later investigation