ISOJ 2021: Day 2, Workshop

How to develop secure communication with sources and a drop box for whistleblowers

---

Harlo Holmes, Freedom of the Press Foundation

Mallary Tenore Hello and welcome, everyone. We're so glad that you're here today, and we hope that you're enjoying ISOJ so far. I want to give a special thanks to the Knight Foundation and Google News Initiative for sponsoring ISOJ, which is in its twenty-second year. Before we jump into today's workshop, I want to remind everyone that we're providing simultaneous interpretations into Spanish thanks to support from Univision Noticias. If you click on the globe icon at the bottom right hand corner of your Zoom screen and you select the Spanish channel, you can access this workshop and all the other ISOJ sessions in Spanish. And if you're tuning in via Zoom and have technical issues at any point, you can always tune in via YouTube instead in both Spanish and in English. And we'll post those YouTube links in the chat for you.

So now I want to turn to our workshop, which will be led by Harlo Holmes, who is the director of digital security at the Freedom of the Press Foundation. Harlo is going to teach you how to use SecureDrop, an open source whistleblowing platform that enables journalists to secure their communication with sources. And she's also going to explore how you can use other tools like Signal, WhatsApp, and Onion Share to enhance your investigations. During the workshop, you can feel free to post questions for Harlo in the chat, and we'll get to as many of them as we can at the end of the workshop. And you can also post highlights from this workshop on social media using the hashtag #ISOJ2021. And now, without further ado, I'd like to introduce Harlo Holmes. Thanks so much for being here with us today, Harlo.

Harlo Holmes Hello, everyone. Great to to see you. And it's really, really great to be at ISOJ, albeit from home. I really, really miss you. Welcome to our workshop. And I believe my screen is being shared, and people will let me know if that is not the case. But let's get right to it. We have a lot of stuff to do today, and I want to make sure that we pack in as much as possible. OK, so first and foremost, a little bit of an introduction. Once again, Freedom of the Press Foundation develops a product, it's called a newsroom appliance that is called SecureDrop. It's a little bit intensive and a little bit expensive, and we'll get into the nuances about that. But it connects sources and members of the public at large to newsrooms. And it's currently installed in upwards of 70 newsrooms across the entire globe. This is just a subset of some of the organizations that we work with. And it would be remiss if I didn't mention the other two components of our organization that we're really proud of, such as the US Press Freedom Tracker, which is our main advocacy wing, that documents where members of the press have had the right to report infringed upon. So please do check check this out. This is a really excellent project that we do in conjunction with CPJ and other organizations that are on our steering committee. And my part of the organization is the digital security wing, where we provide training, consultation, security, auditing, et cetera, for newsrooms, large and small, freelancers and documentarians across the globe.

OK, so first off, actually, let's talk about some terminology as we talk about source communications. First and foremost, there is the content of your communications, which is what's being said. But then there's also the metadata, which if we're going to talk about the journalist parlance, it's the who, the when, the where and the how of attributes of a conversation. And so from our perspective, this includes things like people's names, their handles, their phone numbers, things like that. But also as far as computers are concerned, because most of our communications are entirely digital. This includes things like IP addresses and sometimes even location data, timestamps, et cetera, and we're going to get into that a little bit later. So some more vocabulary. When looking at communication strategies, no matter what it is, and we're going to talk about these strategies in just a moment, there are a couple of terms that I want you to think about that are incredibly important when making decisions. So there's encryption in transit, which is roughly like why we have that little lock in the corner of our address bar in our Web browsers. It's the ability to scramble the content of Internet communications as it travels over to its destination. So that's why our encryption with Google is so strong, with our email, hopefully, et cetera. But then there's also encryption at rest, which is similar but different. It's important because files that we have at rest, whether those are like Word documents or the folder that holds all of your communications in Signal desktop or whatever, all of those local files on your computer or on your phone are pretty much illegible when that device is powered down. And just want to emphasize the fact that communications can live at rest at a number of different places, so it can live at rest on your computer. It can live at rest on Google servers, on Facebook servers, et cetera. So we never really have control of the entire picture. Then there is a really cool term that I'm sure you've heard thrown about wildly end to end encryption, which means combining multiple types of ways to encrypt in order to ensure that the content of your conversations cannot be decrypted by anyone other than the devices that are party to this conversation. We're going to get more into that when we talk about Signal and WhatsApp very shortly.

There's also properties that are really important nowadays as far as like maintaining the confidentiality of a conversation. One is called perfect forward secrecy, which means that only a limited subset of a conversation can be decrypted if somebody did for some reason get the key to do that. And so that means that actually makes things ephemeral. So that's where disappearing messages come from. And sometimes disappearing messages actually do work because they apply this principle of perfect forward secrecy like we see in Signal, and in WhatsApp, and Wire and a couple of other things that we're going to talk about. But sometimes it's just a parlor trick, and it's not actually true, like Snapchat. So like Snapchat will totally say that the messages expire after a certain amount of time. But quite frankly, they don't actually apply perfect forward secrecy, and they're still sitting on all of your snaps in their servers, where you're just reliant upon their having encryption at rest, properly applied. And also you're relying on them not to get subpoenaed for snaps that you sent like two months ago. Finally, there's plausible deniability, which is a cryptographic attribute. That means that while you may know who you're talking to, the system itself, if they're holding on to any of your data, they actually don't have the ability to do so.

OK, so let's talk about some of the tools, because we have a lot to do in the hour that we have. I would absolutely love to introduce you to SecureDrop. SecureDrop is, once again, a newsroom appliance that allows people to communicate with newsrooms, with technological anonymity by leveraging the Tor network. It is a portal where you just you use the Tor browser, and we'll talk about Tor throughout here. You use the Tor browser, which is a mimic of Firefox, in order to properly access a portal that a newsroom might host. And then you start communicating with journalists, you exchange files, you communicate whatever it is that you need to do in order to get an investigation done.

Really quickly, I'd like to introduce people to the Tor network as being kind of like what this photo is right here. This is the parking lot in Virginia where Deep Throat met with Bernstein in order to discuss the Pentagon Papers. And actually, Tor is built technologically similar to that. If you're not sure about what Tor actually works like, there are what's called circuits that pretty much bring you to a rendezvous point that is known by you and the service that you're reaching. So like you and The New York Times, but ultimately, like you go through several what we like to call "hops" on the circuit in order to obfuscate exactly where you're coming from. So once you meet at this rendezvous point and you exchange your information, once you go away, no one in this particular conversation knows how or where that person goes at the end of the day.

Here's a little bit of a diagram of how SecureDrop typically works, if you are using it currently. We have a couple of servers and what's called a firewall that sit safely, physically and from a networking perspective, safely within a particular office, let's say. And then the source uses the Tor browser, communicates with these servers over the Tor network as represented by the onion. Traditionally SecureDrop has worked over an operating system which is called Tails. Tails is the amnesiac incognito operating system, and what it does is it protects you from two things. One, all of the networking is routed entirely also over the Tor network, which means that you can provide that anonymity, that kind of parking lot style anonymity, but also it protects you from malware. So if you ever did receive a document from a source that you obviously cannot trust upon first contact, then once you shut down that session, that operating system and the computer that you're running it on will clean itself. So none of those bad things possibly persist. That said, the journalist does connect to the Internet to look at what we like to call the journalist's workstation. This is a very simple portal where similar to an email inbox, the journalist can view submissions. And it's a little bit tiny right now. But you might notice that in this image of our journalist's workstation, the source that they're talking to actually comes up as what we like to call a code name. This keeps their anonymity, but it also keeps a little bit of persistence of identity. So you can definitely say that like Risen Crowbar is the person who I'm communicating with about this particular issue and continue that correspondence with that source based off of that particular code name. This is where it gets complicated. So I mentioned the idea of malware and also the idea that malware is capable of a lot of things. And we're going to talk about that a little bit more as we go through other options. But what we have to do in SecureDrop land is we have to after downloading those encrypted submissions, we have to put them on a USB stick. We call this the transfer device and then bring it over to what we like to call the secure viewing station or the SVS. This is an example of an air gap. It is a computer that has been physically removed of all of its capabilities of connecting to the Internet. And the reason why is if there is malware or if there is something that is like a booby trapped file that sends metadata like your location or your IP address or something like that, we want to prevent that as much as possible. And we want to protect the newsroom environment from any thing that could attack its network rather than attacking the particular journalist who has unwittingly opened these things. And so it's a very complicated dance.

There is actually a sneaker at the bottom of this particular slide, and that is another term that I'll introduce to you. It's called a sneaker net, which means pretty much taking something that is online and vulnerable and bringing it to whatever means is necessary, in this case, a USB stick, to an air gap where it is no longer capable of harming people. Once we get to our air gap, we are able to then decrypt the submission because all of the submissions are inevitably encrypted so as to protect the newsroom server from any threats having to do with people poking at the server. A subpoena, literally like a law enforcement kicking down your door and physically removing the server, in order to protect

that, all of these submissions are encrypted by a key that only that air gap has in order to decrypt those submissions where the journalist reads them and then does what they need to do with it, whether that is to make safer copies of it and distribute it to other people in their newsroom, like editors or other people on the investigative team, or print it out or whatever in order to complete that cycle.

But you can see from this diagram that it's a little bit complicated, and we're looking to make this type of hypersensitive security more accessible and perhaps less daunting for people typically working in newsrooms. So, yeah, as I had said, to recap, that secure viewing station is kept offline at all times, and we train newsroom teams that are participating in SecureDrop about exactly how to do that, which includes, once again, physically removing a Wi-Fi card and a Bluetooth card. Sometimes it literally includes like gumming up or taping over the Ethernet port so people don't mistakenly plug it into the Internet. Yeah, it's a lot to do, but that's security.

So I'll talk about some of the pluses and also some of the caveats to using SecureDrop and also really like an appeal to all of you, if you're interested in getting your newsroom, no matter the size unboarded with SecureDrop, please do reach out to us. But ultimately, this is a system that has proven to have, and we're proud to say, to have moved a lot of contemporary history. I really, really would say so. We do not at Freedom of the Press Foundation, have any access to any of the submissions that come in through anyone's secure portal. But those news organizations who do share their triumphs with us definitely do make us incredibly proud. The feedback that we've gotten is that it's an excellent way to ensure that sources can communicate bi-directionally as freely and as candidly as possible while maintaining the utmost of technical confidentiality. When submissions come in that are worthwhile, it's really an excellent environment to facilitate cross-team coordination. And the Tails operating system by default, this is totally separate from SecureDrop, but we do work very closely with the Tails operating system team, they have created an environment that is perfect for doing things like redacting documents, redacting the metadata that is contained in those documents, and tools to even prepare stories securely in an environment that's comfortable for the journalists. It comes with things like Audacity for audio reduction. It comes with a modest video editor. It has the suite of LibreOffice tools that are very, very similar to the Microsoft Office environment. And it's all open source, and it's all made by people who have developed these projects in order to protect the rights of privacy and security for human rights defenders, journalists and do gooders across the world.

Caveats, though. The air gap workflow. It is incredibly complicated. We have heard that it's especially cumbersome. No matter what you use for a confidential tip line, you are ultimately working with members of the public that are anonymous and unknown to you. And so you open yourself up to a certain amount of not necessarily abuse, but a high signal to noise ratio, where people might attempt to spam you, to waste your time, to troll you, to lead you to dead ends. And so when you have a workflow that includes using like several computers, using these weird operating systems that are definitely not what you're used to in an office environment and literally walking with your feet to perhaps even another room where there is an air gapped computer, and then you decrypt something, and you open it up and it's just like troll face or whatever, that might make people a little bit reticent to engage in this type of investigative tool. So one of the confessions that I will say as a digital security professional is that security folks are always looking for ways to temper people's expectations of ease of use and efficiency with what they need to protect themselves. And so we're going to talk about other ways with working within a variety of

price points and other resources and threat models to get what you need for an investigation as efficiently as possible.

One thing that we've done at Freedom of the Press Foundation is we have started to work with a brand new operating system called Qubes. This doesn't replace Tails. You still have to use Tails, but it's called the Qubes Operating System in order to create what we like to call the SecureDrop workstation, which combines all of those journalist facing steps into just one simple experience. These are some screenshots of it. Currently, this is a pilot program. And if you're already a SecureDrop user and you're interested in getting bootstrapped onto the the SecureDrop workstation, please do let us know. Yeah, it's not as resource intensive. So what we have here is a Linux based operating system that if you are a SecureDrop user already, you probably will already be accustomed to. But there's just some key differences. We have one computer, no more, several computers, just one computer that you can have in your home. You can put it on whatever network you want to. There's no mutilation of its networking properties. It doesn't feel like a James Bond toy or anything like that. Where you simply log in using our SecureDrop app, and then you're presented with what looks to be like an email inbox. It looks exactly like Outlook. Our designers actually worked really, really hard about that after a lot of feedback. So you have a basic inbox interface where you can immediately establish correspondence with your sources. The encryption is still there, so we still have that encryption at rest and encryption in transit. We still have end to end encryption. And so all of our technical terminology checkboxes are totally ticked off. But there you go. You can just immediately start chatting with people as simple as you were using email, or Signal, or something like that. Also, you have the ability to easily export or print out any of these documents without having to take it to the air gap, and without possibly making decisions about how you're going to coordinate that within your team.

I'm not going to belabor this point too much because we have so much to talk about. But I do want to pinpoint that this particular operating system, Qubes, is special in that it actually does allow you to create air gaps on the fly. So in this screenshot where you see that's Groovy Bantamweight, we still have those code names, has sent a document, it's a JPEG in this particular instance. That green-bordered window where we are looking at that JPEG that was sent in is entirely separated, from a technical sense and a verifiable sense, from the rest of the environment on the computer. So what we're dealing with in our yellow-bordered window, which is that app that is our inbox, is entirely separated from this green-bordered air gap, where you can have a very safe space to do potentially risky things. Because at this point, we don't necessarily know who Groovy Bantamweight is and what their motivation is in sending us this particular picture. And then once you close that window, it's entirely gone from your computer. And so we are maintaining that amnesiac property, which is also super duper important when you are working with untrusted stuff.

OK, there is going to be Q&A, but feel free to pile those questions up. I will definitely get to them a little bit later on. But in the interest of time, I'm going to move on to some tools that we can use in order to kind of have the same effect. But if you don't have access to everything that SecureDrop requires. I will be entirely honest. SecureDrop is not trivial. It takes a lot of investment of time and of money. To source all of these all of the equipment required, you're probably looking at $5,000 at minimum. And so we get at Freedom of the Press Foundation a lot of questions from journalists, especially from smaller newsrooms, about what options they might have when they're not quite ready to get to SecureDrop. Although once you are ready, we're here for you, but we're also here for you if your price point doesn't allow. So I'd like to recommend, first and foremost, OnionShare.

OnionShare is a really, really awesome tool by a friend of ours and also a member of our board, Micah Lee, who is the head of security at not only the Intercept, but at First Look Media. OnionShare is a very, very simple app that comes on all of the desktop platforms that you want, so Mac, Windows, Linux. And what it does is it allows you to once again leverage the Tor network, which is great for our anonymity, so you can maintain the same technological respect as far as confidentiality is concerned to share and receive files. Also it hosts, like an entire website to do chats, to have anonymous chat. So there are four functions within OnionShare. This is a little bit of an old screenshot. I apologize. But ultimately what it does is you say, "I want to go into share mode," or "I want to go into receive mode," or "I want to go into chat mode," or "I want to just host a website," or whatever. You click that particular button, you receive an Onion address, which are addresses that are only available on the Tor network, in that parking lot metaphor that I was discussing beforehand. And from then you're off to the races. You can once again send files, receive files, host a website, or start chatting. The only thing that you have to do over another trusted third-party channel is to communicate that like weird Onion address. They're incredibly long. I think they're like, what, 54 or 52 characters. I forget off the top of my head, and they all end in .Onion, which means that they're only accessible over Tor, and you have to find a way to communicate that. And you might take that to Signal, or depending on what your purpose is for hosting this particular thing, you could totally put that on the commons of the Internet. And we'll talk about contact pages in just a moment.

One cool thing about OnionShare, actually, is that have a look at Micah's blog. If any of you are technically minded and want to torture yourself with a really cool weekend project, you can actually run these type of services on some like very, very small, low-cost computing device, like a Raspberry Pi that you put wherever you feel comfortable putting it. So a Raspberry Pi for those of you who are not familiar is kind of a toy computer. It costs about $30. It's impressively really fast and robust. Teenagers love them. Nerds love them. They're really fun to play with, and ultimately with instruction, you can learn how to take this like $35 box that you get from your local Best Buy, or hobby nerd shop, or order off of Amazon, run OnionShare on it and plug it into your router, and you could conceivably, if you're comfortable with it, run an anonymous SecureDrop-like portal for people to send you files, or communicate with you, or however you feel like using your particular OnionShare.

So before we move on, I'll talk about the caveats, because once again, it's always like, is it security or is it ease of use? Also, we're throwing in the mix like the resources we have. So one of the plusses to SecureDrop is that our security architecture definitely accounts for things like firewalls, which are for those of you who are not in the newsroom technology, but maybe more on the journalism side, I'll tell you that the firewall is pretty much what keeps your organization safe for anything that you accidentally click on. We all accidentally click on things, all of us, no matter how tech savvy you are. We all accidentally click on things. And so usually in enterprise environments and office environments, you have dedicated staff that knows how to use this particular appliance called the firewall to keep you all safe for the inevitable event when somebody clicks on a thing. In our home, especially in the COVID era, nobody's really administering their router in the way that like an office I.T. staff would. And so if you are going to have a Raspberry Pi where you literally tell everybody, send me anything, I promise I'll click on it. You might want to think twice or do it in a situation where you feel comfortable. And actually in Micah's post, he does have recommendations for the considerations that you need to take into account. Unlike SecureDrop, also using OnionShare is rad, it's awesome, but unlike SecureDrop, there isn't an end to end encryption out of the box. There's definitely encryption in that you're using the Tor network. You're meeting in the parking lot, like you're exchanging the stuff in

the parking lot, which is awesome, but you do not have end to end encryption out of the box. And so if someone raided your apartment and took your Raspberry Pi, that data that was on that Raspberry Pi would definitely be open and available to anybody who observes it. So that's just one consideration. But that said, it's still like incredibly efficient and also, like, really, really fun and really easy, and way quicker to spin up than SecureDrop.

OK, so let's talk about some of the trends that I've been seeing as far as just sourced communications are concerned. One just has to do with the fact that we're all on the phone. We're all on the phone all the time. And once again, when we come back to that toss up between what's efficient, what's going to keep you moving, because we all move at the clock of newsprint, we move at the speed of the press, and also what is affordable. We're definitely on our mobile phones. So before we get into the nuances of why the choices that we use on our phone matter, I do want to talk about just end to end encryption, and why it's important. So no matter what it is that you put on your phone, we're going to talk about the caveats. But you're still going to do it anyways. I do it, too. It's OK. Let's talk about the caveats. This is what end to end encryption looks like. This is an example of an end to end encrypted chat that was entirely taking place over Google Hangouts when they used to let us do this. This is using a protocol that's called Off the Record or OTR. And why that's important for you to look at is because a lot of people think that end to end encryption is magic, and it absolutely, absolutely is not magic. So if Google were ever to be served with a subpoena for the conversation that my friend Rose and I had a couple of years ago, this is literally all that Google would be able to hand over. If they like, of course, didn't fight the subpoena and they found out that they had to, this is all that they would have to give people. That's great because actually it only means that my device or Rose's device would have the keys on them, the physical cryptographic keys on them, in order to take this gibberish and turn it into like actual content of our conversation. But if you recall, when we were talking about the vocabulary, there's content and there's metadata. And so if we're going to point out what's the who of it, obviously we have people's names here clearly visible. And that's just a fact of the Internet, how it works. We could have even had avatars should we had put them on, but we didn't. All of the stanzas, we like to call them, start with question mark OTR:, and then a whole bunch of gibberish. And that question mark OTR: that actually refers to the protocol, the off the record protocol that we were using to communicate. So once again, we have the how of this conversation. We also have things like time stamps and subject lines and like a variety of other things that in the event of a subpoena can still be handed over. And now that end to end encryption with all of these apps that we use are what we like to call facts on the ground, that means that, like in the event of retaliation over investigations, then that just becomes like the gristle for the mill of any particular prosecution.

So some of you might have seen this if you have been in trainings with me before. And I'm not going to go over it because at this point I've done it so much, and I wanted to talk about something wildly different with you today. But this is what we like to call the Matrix, which is a visualization tool that we like people to think of when they're choosing which type of communication platform on mobile they're going to go with regarding what we have on our horizontal y axis, what actually works, meaning it's ticking off all of those boxes in the vocab that we went over before, like end to end, right? Yes. Like perfect forward secrecy. Awesome. Like how does it handle metadata? Like, how does it preserve your content? Were there servers? Like all of these questions, versus how accessible it's going to be to anybody that you want to have a conversation with. And so in my experience, everyone's matrix is going to look different. But in my experience, this is kind of what mine looks like, where we have Signal being like my favorite thing in the world to communicate with, because of it's minimal use of metadata, the fact that it has end to end encryption,

perfect forward secrecy, doesn't have plausible deniability, but that's another problem. That's OK. But like a respectable transit at rest, encryption at rest, encryption in transit, etc.. But I also know that Signal is not as popular of a tool as something like WhatsApp, which we see on the other end of our spectrum, where that is on upwards of maybe like 1.5 billion phones on the planet in every single continent on earth. Your mileage may vary. Sometimes during times of political unrest, people might try to prevent access to WhatsApp's servers, so it becomes unusable or unreliable. Please do ask your questions in the chat about that. But it still has parity of features in that it has end to end encryption. It now has enabled a perfect forward secrecy in terms of like its disappearing messages. But it does have a slightly problematic relationship with Facebook in terms of the metadata that they aggressively seek because they're trying to monetize this product that they had invested so much money in acquiring. And also it's Facebook, and you know how Facebook works. This is not our first rodeo. It's been years since we've been talking about Facebook. But that said, it's less problematic if you are talking to, let's say, like sources in international situations where they are in political climates where if someone is stopped at a border and they are compelled to open up their phone to a border guard and the guard sees that they have Signal on their phone, that could have like perhaps more implications for that particular source. So then you can justify taking that particular conversation to WhatsApp just for them to preserve their operational security. Because you as the person who's a little bit more knowledgeable about these things, you have like the duty of care to make those appropriate decisions. Same thing with Facebook Messenger. It's Facebook. Also like the secret chats, and this is very similar to the Telegram discussion, the secret chats are only in a certain mode in Facebook. You actually do have to like explicitly enable end to end encryption in your Facebook chats. And that doesn't work on desktop, for instance. So if you're talking to somebody who's like only on desktop, and this does happen sometimes during like a manufactured politically-motivated Internet shut downs where people's mobile data will automatically stop working, then they all jump to desktop, and then you lose the capability to have end to end encrypted chats over Facebook Messenger. And in which case you got to take it back to WhatsApp, because at least that is end to end encrypted across the board. As long as you're not using SMS messages, they are so surveilled, they'll never be encrypted ever. And the least safe of any, any messaging platform to use.

OK, so everybody's on their phone, but when we reel it back to talking about journalists themselves. What about our privacy? And so sorry, like I always do this, and if either of them reach out to me and say, "please stop picking on me," I promise I'll change my slides in the slide deck. But I'm going to talk about Lorenzo and Joseph from Motherboard, who are amazing, and they're brilliant people. But they are always available with their Signal phone numbers, like pretty much the same phone numbers that they speak to their mothers on. But meanwhile, a lot of women in this field, people of color, like non-binary folk like that actually puts them at way more risk than like the dudes at Motherboard. It's just a fact. And so if you are going to be like using your presence as a tip line, think about doing the following: Getting an auxillary number, linking it up to perhaps Signal desktop or where available, like whichever platform. WhatsApp actually kind of stopped doing this because they worry about fraud, and it's Facebook, and they're corporate or whatever. But you can still do this on Signal. Recommend Twilio, just link it up to your own phone number in order to bootstrap yourself onto Signal. But just understand that, as I said, like, your mileage may vary, especially with tools like WhatsApp. Also be aware of like Signal desktop stuff. I'll have you look at these slides. But in the meanwhile, here is just like the best take aways. Full-disk encryption, encryption at rest on your desktop because if your laptop is ever seized, you don't want people to have access to that. And also know that the notifications, the Growl notifications, pop ups, et cetera, that can often mimic the data

that's coming in via end to end encrypted line, and so you want to prevent your computer from duplicating any of that data that you might receive.

There's a lot of nerd stuff in the slide, but actually like talking about how people have remixed Signal because it's an open source project, meaning it's code based and is available to anybody who's interested. And so in doing so, there's been a couple of really, really awesome projects that remix like the Signal protocol for tip line purposes. So I'd like to shout out Signalboost, signalboost.info. This is a remix of Signal, where you can use their server if you wanted to, but you can also host your own server, which is preferred, where you can use this as a tip line where you and an unlimited number of fellow investigators can work together, receiving tips on your phone via Signal. So someone can publish a phone number, and it's a virtual phone number. So it's not your own phone number at all, but you publish a phone number. People, the public at large, can Signal you like tips or attachments, whatever you want to do. And you and your investigative team can respond directly to those people via your phone on Signal. And you can also have like a private channel for administrators, and there's a middle tier for people on, let's say, your investigative team in order to gossip about whatever is coming in. So we haven't completed it yet, but we've kick the tires on it. And we're really excited that in coming months, we will actually have, hopefully, unless you steal my idea and get it first, we'll have the world's first investigative unit Signalboost based tip line. So, let us know if you need any direction on that or if you want to bounce off ideas.

Finally, and I know I only have about three minutes before we open it up to Q&A, but I want to talk about just some of the caveats overall, no matter if you're using a Signal tip line, if you're talking to people on WhatsApp, or if you're using OnionShare, if you're using SecureDrop. If someone has your stuff, it is game over because there is what's called the analog hole, meaning that ultimately, when I was showing you what end to end encryption looks like, which is incredibly important, but ultimately, if you are subject to a legal request, and you have to comply, and whatever general counsel you're working with cannot save you in that regard, no matter what, you're going to have to comply. And that could either mean confiscation of devices, where they will take forensic images of it and use whatever tools they have available in order to find whatever forensic artifacts reside on that device. Or you can enter into e-discovery where you just have to hand over the phone in general, and tell them what the passcode is, and then your lawyers have to do keyword searches in your entire Signal history for certain things. Or they could just literally take your phone, put it down on a copy machine and then wait for the bubble notifications to come in that say, like your WhatsApp messages, like the entire content of your end to end encrypted WhatsApp messages because you have the bubbles turned on on your notifications. So this has happened before in a variety of ways. And it behooves all of us when we're thinking about our digital security to think about like the auxillary choices that we have to make in order to make sure that these things stay safe.

In interest of time, yeah, a shout out to iMessage. iMessages are end to end encrypted. They're great. However, iMessages can wind up in your iCloud, and your iCloud can be subpoenaed. So, like, sucks, you know. We're never going to win. It's always a game of cat and mouse. So in conclusion, I'd like to present a philosophy that I really, really like, which is the asymmetry of preparedness. We talked about like those particular caveats. But ultimately, your source is not ever going to be as lawyered up, or probably not, as lawyered up as you are. And so in addition to having that duty of care to up their skills and keeping good communication with other people at your organization to help you go through any of these conundrums that you might face, just know that there are organizations out there, Freedom of the Press Foundation, Reporter's Committee for the

Free Press, also whistleblower networks like WIN, and the Signals Network, not to be confused with Signal, it's totally different, that are there if you need help afterwards. They're not going to have as much endpoint security as you do. So yeah, you can be on WhatsApp, but if your phone is like a $50 Huawei that you got second hand, trust me, your end point game is not strong, and you can't control that. And also we talked about the finer points of all of these tools, and it's important for you to know that there's always going to be caveats.

Last thing, let's talk about tip lines. So you might have noticed, shout out to ProPublica, they use the commons of the Internet, where that's your organization's website, Twitter, Facebook pages, wherever, that is safe for people to find all of these resources. ProPublica has an excellent page. Also, CNN has a really excellent page that also gives people a little bit of pro tips on how to use it. But when you're having these discussions, think about how to maintain secure first contact. So your contact page, should you have posted one on your own site, https it's got to be encrypted, so people don't know that they're going to like CNN.com/tips. They only know that they're on CNN. And that's innocuous in the case of an audit of any kind. Nix the ads and the tracking, and I know sometimes you have to talk to the people who manage to CMS and see if you can make an exception for these specialized tip pages. Also continue to mirror that stuff on the commons of the Internet, so Twitter, Facebook, GitHub, et cetera. I'm rushing because I know we have Q&A coming up. Also, plan for success as well as failure. So like if your tip line is going to go down, if like SecureDrop is not working out for us, we're not really into it. Or like we lost this Signal phone number, or X, Y, Z. Be sure you have a shutdown plan and communicate that to people. Also, avoid the bus factor, and make it less independent on any particular person in your team to keep things running smoothly. And this is especially important in the COVID era because it's like, OK, so who's checking the SecureDrop? Like, who has the gear to check the SecureDrop? And that's actually serendipitously one of the reasons why our SecureDrop workstation pilot was so impactful is because we could just give people a bunch of laptops, and you all can check the SecureDrop, rather than relying on a single point of failure.

OK. Yeah, finally, be available everywhere. So I'm available everywhere. However you want to have this conversation or to continue this conversation. Thank you so much, ISOJ, for having me once again. And yeah, that's the state of confidential tip lines and source communications. Hit me up if you want. We have a whole bunch of guides about deeper digs into using these tools at our training site. So freedom.press/training. I can be reached at Harlo@Freedom.Press, or you can find me on Twitter @harlo. And that's my story, and I'm sticking to it.

OK, now I'm going to head to the Docs. All right, so for the last five minutes, I believe, there's a Q&A, and these are a lot of really, really excellent questions. OK, so I'll start from the bottom and work all the way up top. Does OnionShare have a cost? No, it is entirely free, entirely open source. And it's just up to you to figure out where you're going to put it. You can actually use it on your own computer, which you know is OK. However, if you're receiving files from random people on the Internet, I really, really, really would advise against that. However, using the share files function is great. Using the chat function is really, really awesome. And also, as I mentioned, we have that really excellent blog post by Micah Lee about how to spin it up on a very cheap Raspberry Pi. OK, I'm going to pick at random. To run SecureDrop, we have to use Tor, or can we also run it in Chrome? SecureDrop absolutely has to be done in in the Tor browser. Chrome does not allow you to look at any onion links, only the Tor browser allows you to. OK, here's another question. Are there tools to move safely and protect sources that are based on the block chain? This

is a really cool question. So short answer is no, because the block chain is a public ledger, meaning that everything is entirely auditable and should live in perpetuity. But that said, there is a really cool thing called Keybase, which is actually kind of block chain adjacent that does provide that end to end encryption, that perfect forward secrecy. And if you set it up correctly, you have to be a little bit stealthy in how you do it, but if you do set it up correctly, you definitely can maintain anonymity. OK, I'm going to skip around at random. Signal is very well protected when using a phone, but why is it so easily accessed when using on a laptop? And so it's not like more or less easily accessed when using a laptop than it is on a phone. I just think that normal users are a little bit more savvy about how to navigate the file systems in order to find those files where Signal has left it. If you are worried about that, just so you know, like let's say if you're on a Mac or something, I don't know actually where it is on Windows off the top of my head, but if you're on a Mac, if you go to library, applications, Signal, desktop, then like within that folder, there's all of your files, and that's exactly where it lives. And so if somebody did seize your laptop, that's where they would go, and they'd be able to look at your Signal desktop stuff. It's still end to end encrypted. But it just means that your computer is the place where it's being decrypted, and that's where they stored that data so you can read it. On phones, for us, regular people, were not usually like hunting around in our phone's file system in order to find where those files are, but they're pretty much there in the exact same way. So, yeah, it is what it is. And just a reminder, that's why you have full disk encryption, hopefully, on all of your machines, phones, computers, laptops, et cetera, because when you power them down, no one will still be able to access those files. OK. Let's see. Freelancers do need more support as they're not connected to a media outlet. And so what security congestions would you give them? So there are a couple of really excellent organizations that put on trainings similar to these for freelancers. There's two things. One is that like keep in touch with this particular community in order to get access to press umbrella organizations when you need help. Some of them even have resources like emergency funding in the case that your device gets smashed at a protest that you're covering or something like that. And I think that between training, consistent training and regular training, and support for actually having good hardware, those are two places that I can say that freelancers need the most support. Just keep in touch. I know that there were so many questions, and I think I have two minutes left. OK, let's see. Is Signal the best? Yes, Signal is the best. I mean, nothing is the best, but the point is that we try. And that's the state of it today. All right. So I'm out of time. Thank you so much. It was really awesome to talk to you today. Thanks for listening to me, and continue to reach out. Enjoy the rest of ISOJ.

Mallary Tenore Thank you so much, Harlo. That was wonderful, and a super helpful workshop. I love that you really delve deep into SecureDrop, but also offered up a slew of other tools that journalists can access to secure their communications, which is increasingly important in this day and age. So thank you again.

To everyone in the audience, I hope that you enjoyed this workshop and that you'll stay with us for the rest of today's programing. We have two other panels coming up today at 1:00 p.m. Central and at 4:00 p.m. Central Standard Time. Now, normally, if ISOJ were in person, you would leave the session and you would start chatting with all the other ISOJ'ers. And we can't quite replicate that in-person communication, but we are using a virtual platform called Wonder, which you can use to have a private or group conversations with other ISOJ'ers and speakers. So we'll be dropping a link to the Wonder room in the chat throughout the day, so you can access it as many times as you would like throughout the sessions and in between them. And I also want to mention that we have a pick and post page on our website, ISOJ.org, and we'll link specifically to that page in the chat. But there you can find these really fun graphics that say, "I love ISOJ." You can basically use

those, download them directly from the site and post them on social media to let everybody know that you're here and having fun and attending. And you can use the hashtag #ISOJ2021. So we will be back here in about a half hour for a panel titled COVID-19. It's all about sort of fighting misinformation during the pandemic, and we've got a great lineup of speakers for that. So I hope you will join us back here at 1:00 p.m. Central Standard Time, and we'll see you soon. Thanks so much.