Alex Cooke 00:00
Hello and welcome back to ACT's Global Tech Swamp podcast! I'm your host, Alex, happy to be back at the mic. It's been a busy few months since you last heard from us so let me share a few updates.

First, we've launched a brand-new website at actonline.org so be sure to go check it out and let us know what you think.

We've also returned to our roots as the Association for Competitive Technology, fondly known as ACT.

And we've been traveling to as many tech hubs across the globe as we can spending the summer months touring the EU and UK, September in Brazil learning, and in November, we will be back in Europe for Portugal Tech Week, Web Summit, an event at Station F in Paris, and in Helsinki for Slush. Plus, with the U.S. midterm elections just around the corner, there is no slowing down as we prepare for 2027.

But 2027 is still a few months away, so let's talk about what happened in October! October 21st was Global Encryption Day, and we marked the occasion with a panel featuring James O'Sullivan of ACT member company Nuke From Orbit, Dr. Joseph Lorenzo Hall of the Internet Society, and Josh Tabish of Chamber of Progress, moderated by ACT' Policy Associate and all things privacy expert Morgan Stevens.

Encryption is a critical tool developers and companies of all sizes use to protect their users' most sensitive data, but proposals that call for mandated back doors to encryption threaten those protections. For more from our panelists and the conversation, I'll turn things over to Morgan!

_____

Morgan Stevens 00:12
Good morning, and happy Global Encryption Day. My name is Morgan Stevens, and I'm a policy associate here at the Association for Competitive Technology. Thank you very much for joining today's webinar: Encryption Policy and Law, Navigating Governmental Pressures and Tech Industry Responses. Encryption plays an essential role in protecting consumer privacy, securing sensitive data, and keeping the digital tools and platforms we use every single day safe. But despite its importance, we're seeing a growing push from governments to weaken encryption in the name of lawful access. In the United Kingdom, the government has reportedly sought to require Apple to provide access to encrypted

Transcribed by https://otter.ai

backups. Meanwhile, in Canada, Bill C 22 proposes new lawful access requirements that raise important questions about the security of encrypted systems, while these debates are often framed as battles between government and big tech, the consequences extend far beyond the largest companies. Weaking encryption puts consumer privacy at risk, undermines cybersecurity more broadly, and threatens to secure tools that small businesses rely on every day to protect their operations and their customers. To help us unpack these developments and what they mean for the future of encryption, I am joined today by a wonderful group of panelists: James Osilvin, CEO and founder of Nuke from Orbit; Dr. Joseph Lorenzo Hall, distinguished technologist at the Internet Society; and Josh Tabish, senior director for Canada at the Chamber of Progress. As we get started, just a quick housekeeping note that your questions and comments are most welcome. If you have a question, please leave it in the Q and A box at the bottom of the screen, and we'll get to it during the Q and A session towards the end. For now, to get started, I'd like to turn it over to the panelists, starting with Josh.

Speaker 1 01:58
Hi everyone, thanks so much for having me here today. Thanks to the organizers for inviting us all to be here. As Morgan mentioned, my name is Josh Tavish. I'm the senior director for Canada at Chamber of Progress. For those of you who don't know, Chamber of Progress is a tech industry trade association that advocates for responsible innovation. You know, governments are definitely putting pressure on tech companies to weaken encryption, create new access mechanisms, to create new backdoors, and this is certainly the case in Canada. You know, from my view, in Ottawa, we see a concerted effort with the Carney government to ensure that companies that handle sensitive personal information are subject to new surveillance techniques that are subject to new orders that can come down from the minister in Bill C 22, the government's lawful access legislation. You know, in in response to this effort, nearly two dozen technology companies spoke out as recently as September in an open letter. These are small companies. You know, we're talking like 10 employees to like a couple, like 100 employees, raising concerns about the bill and what it means for Canadian competitiveness, for the security of their systems, and for the security of end users. And so, Chamber of Progress was happy to add its name to the letter and has been part of a has been heavily engaged in the legislative process since the bill was first introduced last spring. And I'd be happy to tell you more about Bill C 22 and what it means for tech companies as we go along.

Morgan Stevens 03:45
Thanks, Josh, and over to Joseph.

Transcribed by https://otter.ai

Speaker 2 03:50
Thanks, Morgan, and thanks to ACT for hosting this on Global Encryption Day, which is, I admit, my favorite holiday. One of my favorites. My wife would probably kill me. She loves Halloween. I'm Dr. Joseph Lorenzo Hall. I'm a distinguished technologist at the Internet Society, where I lead our security portfolio. And for the app makers and small technology companies and access community, this issue isn't abstract. Many of you know that government decisions about encryption show up in your products. They show up in your customers' trust. They show up in compliance costs. Right, we've seen that this year with Canada's Bill C 22 signal said it would rather leave Canada than break its promises to its users. DuckDuckGo said it would pull its VPN service. Proton, I think, yet vowed to fight the bill in any means available to them. In addition to very big showings by many, many other companies showing what this means to them, and years ago, when an Internet Society staffer suggested that a global encryption coalition ought to have a Global Encryption Day, I don't think any of us expected the coalition to. Be more than 500 members in more than 100 countries, or that would be marking our sixth Global Encryption Day, but never has it been a stranger time, as you can see with things like Canada's Bill C 22, and that's just one example around the world. Right, we've never had to work so hard for confidentiality and integrity that encryption provides for the younger folks out there. Crypto meant cryptography long before it meant cryptocurrency, some of us in the more silver-haired category have spent decades fighting something we call the crypto wars. And what do I mean by that? What I mean by that is ever so often governments discover or rediscover the idea that a key to everyone's digital live locks might help law enforcement, and then we have to explain why designing systemic insecurity into technology makes everyone less safe. Some of us thought those crypto wars, so to speak, were over. They're not, and we got a stark reminder this week of just how fragile this can be private keys associated with eight Emudra intermediate certificates were found to be compromised. To give you some idea, those keys could allow someone to impersonate websites and read or alter the traffic on those websites. And I'm sorry to say, one of those private keys was the number four. Yeah, not a long, securely generated random number useful for encryption, just for the number four. Mozilla, which operates one of the major browser root programs, moved the block those certificates and what they chained up to within about three hours, which is very very helpful. But you will see today there are a number of fallout problems related to that, related to a very serious vulnerability and something called PHP that are making it a pretty challenging global encryption day for those of us who actually run things. But but anyway, I'll end with that's the lesson here that public key infrastructure, the stuff we use to keep people safe online-it's one of the most mature security systems we know how to build,

Transcribed by https://otter.ai

and still serious failures happen. We have to know how to deal with those failures and recover from them. But to end, we should be deeply skeptical when someone proposes creating another privileged capability and promises that only the right people, only the good guys, will use it. Thanks.

Morgan Stevens 20:26
Thanks, Joseph, and over to James.

Speaker 3 20:29
Hi, everyone. Thanks for for having me, Morgan, and for for act for organizing this. I'm James O'Sullivan. I'm the founder and CEO of Newt from Orbit. We are a company that helps with the the maintenance of user privacy in the event of device theft, and I've been involved in technology and mainly security for a number of decades now, based out of the UK. Recently, have had a number of conversations with government and policymakers regarding various TCNs in the UK. The most famous example, more recently, is Apple's refusal to back down and compromise the security of backups to give UK law enforcement access to those in certain circumstances. Yeah. Okay.

Morgan Stevens 21:21
Thank you, and thanks to all for joining us today. So to kick us off, Joseph, I'm wondering if I could start with you. Where does encryption show up in everyday life, and why does it matter? What do consumers stand to lose if it's undermined?

Speaker 2 21:37
Yeah, I love that question. Encryption is literally working behind the scenes in almost everything you do online, logging into accounts, making payments, getting software updates, as I was talking about, messaging your family. If encryption is weakened, it's not just your privacy at risk. You may find yourself unable to log into things. Your payments could be intercepted or even misdirected or changed, and then private conversations you have with loved ones, which you have to admit some of the most sensitive and most intimate conversations we have are with our loved ones. Those start to become vulnerable, and so the trust that you're really talking to who you think you are and that your data hasn't been altered, disappears, and that's not just a concern for tech experts or activists. After the Salt Typhoon incident, even U.S. Department of Homeland Security CISA recommended everyone use end-to-end encrypted apps like Signal and do one quick little thought experiment with me: If we were to completely outlaw privacy entirely, say there were no more secrets allowed, no more secrets. First,

Transcribed by https://otter.ai

that's not a world I would want to live in. But second, even in that world with no more privacy and no more secrets, we would still want to know that this software update really came from that vendor, or that your e-prescription health records haven't been altered. That the text from someone you love is what they actually sent, and so integrity and authenticity are two other really important parts. While we tend to think of encryption as being about hiding stuff, about confidentiality, about privacy, there's these other pieces that even if we outlaw the confidentiality, we would still depend on to run everything that we do constantly. And maybe you you're watching this and you don't live in the city or you don't do digital things, but many of us have a mesh of sort of encrypted services that that mediate our daily lives, including the Zoom webinar right now. Thanks.

Morgan Stevens 23:45
That's an excellent point, Josh. I wonder if there's anything you'd like to add to that.

Speaker 1 23:49
Yeah, I think you know. I think I would just add a couple things. For countries outside the U.S. there's a lot of discussion right now about so-called digital sovereignty-that is, making sure that countries have the ability to regulate digital services and that they have the ability to control their data and that it stays safe and secure. Now, for technologists, digital sovereignty can be a pretty fraught subject and probably a pretty frustrating subject because you know there are ways in which the internet is inherently global and inherently decentralized, and there's ways and there's many reasons we'd want to keep it that way. But it is understandable that governments want to keep their data safe. It is understandable that governments want to make sure that foreign countries or bad actors aren't spying on their sensitive information with respect to health information or security or you know national defense. And one of the things that I find confusing is that at the same time the government of Canada is saying digital sovereignty is a priority, and that we need to make sure our data stays safe from again poor and bad actors and governments. They're also introducing this bill, Bill C 22, which could undermine and weaken encryption, and insert surveillance access points into large connected networks, whether that's for cloud service providers or telcos or or whoever. And so there's this kind of like why I find this confusing is the government is saying that digital sovereignty is a priority, but they're also implementing you know they're on their way to passing this legislation that could make our networks less secure, that could create backdoors that the good guys and the bad guys could access, and this could ultimately undermine their goals of keeping Canadians' data safe. And so, you know, I would just I just wanted to layer that kind of sovereignty perspective into this. You know, any

Transcribed by https://otter.ai

government that says that they take sovereignty seriously has to take encryption and security seriously, and we see these two things in tension around the world.

Morgan Stevens 26:09
It does seem like quite the contradiction. And James, over to you. You know, as a small business owner, where does encryption show up in everyday life, and why does it matter?

Speaker 3 26:20
Yeah, I think encryption doesn't show up in any overt place, and that's part of the reason why it doesn't get the the press and the the front of mind experience from people, because you won't necessarily understand unless you're in technology when your communications are encrypted, because all you'll see is the end result of the the conduit of that data from source to destination, and it's that bit in the middle that you don't see where it takes place. Now that can be anything from messaging. It can be in this this meeting now. It can be in my banking. It can be when I'm going to a website. It can be the payment for for services on there. There's really a huge array of things, as as Joseph said. If I'm taking a download of an update to software an hour ago, I had to do an update to to PHP after a critical vulnerability, and and thumbs up there. And it's good that I can I can check that it has come from the authorized source. We've seen numerous attacks on the supply chain in various bits of software, where signatures of that software has been vital to us in the tech community, knowing that the updates that we're getting are the ones that were intended, and that there have been no malicious interventions in in the middle of that. So yeah, you don't often see it, but if you if you were to look behind what you were doing, you'd find that there's very few bits of day to day business life that don't involve or should involve encryption of some description.

Morgan Stevens 28:07
Thank you. Yeah, I just checked our Zoom webinar today. Enhanced encryption is on, so we're protected today. Josh, getting back to you about C 22, can you give us a quick overview of the bill? What would it do, and where does it stand now?

Speaker 1 28:23
Sure. So there are really two parts of the bill for folks who are new to it. It's Bill C 22 is also called the Lawful Access Act, and it's the government's attempt to modernize digital investigative tools for law enforcement and intelligence agencies. So as I mentioned, there's two parts to the bill. The first we're

Transcribed by https://otter.ai

just going to kind of skip over. It's really focused on new powers for law enforcement to obtain subscriber information from telcos and platforms, but it's actually like reasonably privacy protective and fairly uncontroversial. The second part of the bill, however, is much more controversial and has attracted a lot of scrutiny from civil liberties groups, legal experts, technologists, the tech industry itself, because it mandates new surveillance architectures that will threaten the privacy and security of all Canadians. So this part of the bill establishes the lawful access framework. You know the the kind of key like headline level provisions are the government can issue secret ministerial orders telling any company to do anything in their network at any time for any reason. The second is it there's a provision of the bill that can force a certain class of core providers, and here we can imagine like cloud service providers being a core group of core providers or social media companies being a group of core providers. It can force them to retain metadata for up to six months. This was initially 12 months, up to 12 months, but it was amended as the bill moved its way through the House, which I'll touch on in a sec. But here, of course, you know the the obvious problem is that metadata, though does not contain the contents of your conversations, can be incredibly revealing about who you talk to, when, for how long, where you are, what your relationships are like. You know, metadata was the stuff that we all freaked out about when we found out when Edward Snowden told us that the NSA was surveilling all of us. So if you freaked out during that period, you should freak out again in Canada. And then you know the the the kind of so yeah so that's the metadata. Oh, the third part, obviously, because we're here to talk about encryption, is the bill can also undermine encryption. There are some exceptions to this, which I can talk to you about in a minute. But right now, the bill gives the government and intelligence agencies considerable power to mess with encryption in ways that could weaken it for end users, so in terms of process, the House, sorry, the bill passed the House of Commons. That's our our first chamber, and it's now awaiting study in the Senate. We're hearing that it should be referred to committee later this week, so the Senate will have an opportunity to study the bill. That's going to be really important because the study in the House was pretty superficial. It was bogged down in a lot of partisan politics. There really was no opportunity to substantively engage in amendments to the bill. You know, if I had to pick three issues that everyone agreed needed fixing, it was the metadata requirements, the encryption provisions and the lack of oversight for the secret ministerial orders, and so the Senate I think has a really golden opportunity here to help facilitate a substantive discussion of the bill and help fix it before it goes any further.

Morgan Stevens 31:59

Transcribed by https://otter.ai

Thank you. That's a really comprehensive explanation. Appreciate it. To drill down a bit further, so I know the bill includes language intended to prevent systemic vulnerabilities. Can you explain that? How well would it do that in practice if enacted?

Speaker 1 32:14
So yeah, there's there's a few things I draw folks' attention to here. The first is the bill says the government can't force a company or network operator to install any kind of measure that would create a systemic vulnerability, and here this is really defined as like a risk that an unauthorized person could get access to data as a result of this measure, right? So the the situation they're trying to anticipate is, you know, backdoors. Unfortunately, the exception doesn't work super well, or I don't expect it to work super well. There's a few problems. First, it focuses on electronic services. The language is there can't be systemic vulnerabilities in electronic services, but it doesn't talk about hardware. It doesn't that that obviously doesn't include things like devices and operating systems necessarily. So that's one problem. I think the second is the bill doesn't have an explicit statutory ban against mandating backdoors or product redesigns that circumvent end-to-end encryption, and so what we mean here is, you know, the government still has the power to say to issue a secret order to a company that says, "Hey, you're not allowed to use end-to-end encryption in that service, or you're not allowed to use end-to-end encryption in that service for those people, and so that's something we're still concerned about. And then the third is, and this is a little in the weeds, so bear with me. But the systemic vulnerability exception basically says, as long as unauthorized parties can't access the data, the measure the government is putting in place is fine, but this only this doesn't apply to people who are under investigation. So if the government has a warrant to go after somebody, and they and they feel assured that there's no reasonable expectation that the circumvention can be accessed by an unauthorized party, then it's all good, and we just know, you know, the my my my colleagues on the panel here will know that that's just really not technically feasible. So yeah, and then the final thing I'd say is they at the last minute they added this other exception that says that was borrowed from Kalea in the U.S. that says the government can't force companies to decrypt information where they don't have the keys available. So that is gives you partial protection for end-to-end encryption, which is a step in the right direction. But it doesn't. But the problem with this is that by copy-pasting that language out of Calea, Calea didn't anticipate things like cloud service providers who are managing keys for their customers, and so those folks who sold their services as being privacy protective, as the you know the company that their their clients that they're working with, their data will be protected with encryption. All of a sudden, it could now be exposed to these secret ministerial orders, because

Transcribed by https://otter.ai

Kalea has like a much narrower scope. But anyway, that's that's the exception. So I mean, they made some amendments. They they they addressed the right things. They just didn't go far enough in fixing the the bill to help protect the security of the networks.

Morgan Stevens 35:37
Thank you. And moving across the Atlantic. So, James, for those who haven't followed the UK TCN situation super closely, how would you explain what's at issue and why it drew so much attention?

Speaker 3 35:51
Well, I'd question what people were doing if they weren't closely following the UK's TCN situation. But in the eventuality that they do have some sort of life outside of technology. the the The very high level view is that in late 24, April 2025, the government asked Apple to give them a backdoor into iCloud backups, specifically regarding the advanced data protection services that Apple was rolling out, there are obviously a number of issues here. Many of them similar to which Josh has just articulated. That when you have a backdoor, it is a bad thing in general, in principle, and it's often difficult to make it constrained to just the good guys, the the second point about about this is that the the TCN or the technical capability notices in the UK are secret by default, so the provider wouldn't need to advise their user that they were subject to one, which means there's a loss of independent and public oversight as to what companies are doing with your data. That obviously, the the lack of transparency therefore in that process means it's very hard for the public to gain gain trust or certainty about how their data is being used, and that that impacts their decision of making an informed decision of which services they'll use for for what type of of operation.

Morgan Stevens 37:33
Thanks, and I know you talked about this a bit earlier, but just to really kind of drill down, how do you and other small business owners depend on encrypted tools day to day, and what would it mean if those protections were weakened?

Speaker 3 37:47
So there's different different levels of encryption that you need for different things. So at a very basic level, it might just be how the passwords that you're using to log into to websites into my social media. It's it's a thing that I don't want someone else to get access to, but it's-it's not going to kill me if if if someone does manage to break that encryption. Then it scales all the way up through a number of

Transcribed by https://otter.ai

different levels to things to do with with with money, with medical records, with digital verifications of my identity, that kind of stuff. So, if I'm going to try and pay online using a card or open banking payment, if that communication is not end-to-end encrypted, then I can't know that the money is going to the right place for the right amount. There's basically nothing is certain about that packet of communication. When you think about that in terms of communication in general, when I'm using email with PGP or or WhatsApp or any other end-to-end encrypted messaging platform, the certainty of knowing that the person at the other end is who I meant to send this to, and indeed they are. They are the person sending me data. That is that is just vital. Otherwise, you get yourself into the the the spider web of things that can happen just just expands out from that point, and and you very quickly get yourself in in an extremely difficult situation when you can't can't be certain of the destination or the origination of communications.

Morgan Stevens 39:31
Absolutely, and James. Also, maybe we could start with you on this next question and move to Josh, Josh and Joe. But this debate has often been framed as government versus big tech, what do you think that framing misses?

Speaker 3 39:47
It's been framed like that because largely that is what it is. You you have government on one side and you have big tech who control the data, so you will always have those two opposing parties. The problem that I think this debate has is that both sides have very good arguments for why they are correct. So, from our side, from a security and privacy a data perspective, it seemed very obvious that you can't have backdoors; you must have encryption from a security, a national security from a law and order perspective, not being able to gain access to to criminal data does hamper investigation and makes it harder to do things that the public would would want. It then hinges a lot on the lack of knowledge of the public, because if you ask a man in the street or or a woman in the street what they thought about these things, like should the police have the ability to read your messages or read criminals' messages, the default answer is going to be yes, because who wouldn't want that? What that misses is to enable that kind of access. the The blast radius of that permission is so much wider, and that's why I think governments are the world over are treading a very difficult line. Certainly, with Bill C 22, I'm I haven't followed it as closely as I probably should have, but the and the the details about the holding of metadata on the messages, I think that is probably going to be the place where we'll find compromise because without having the data of the message, you still retain a reasonable amount of

Transcribed by https://otter.ai

your security by being able to associate locations and people together. You allow law enforcement to build a picture of people that they want to without being able to get that direct data. I think this is a an incredibly difficult job for policymakers to do because of that dichotomy of of people that say on the one hand we want to protect citizens on the other hand we need to preserve privacy so I I don't envy them in in this in this endeavor.

Morgan Stevens 42:18
Josh, is there anything you'd like to add to that?

Speaker 1 42:21
Yeah, I mean, I would I would jump in and say you know you know James is a good point. Big tech is definitely part of the discussion, and they have access to a lot of folks' data, and so they have a lot of exposure in these debates. But what I think the big tech versus government framing misses is that there are a lot of other people who are concerned about this. You know, I'll speak to the Canadian case. There are a number of Canadian innovators who are concerned about what Bill C 22 means for their business, what it signals to their investors, what it means to customers who are considering considering choosing Canadian tech solutions to keep their data safe. You know, as I mentioned back in September, we published this letter from nearly two dozen tech firms demanding changes. These were Canadian companies, and these were also European companies. You know, one of the goals of the Kearney government is to create new trade and economic opportunities with Europe and with Asia to diversify our reliance away from the United States. Well, Bill C 22 complicates that that objective. You know, it makes it it will make it harder for Canadian tech companies to attract investment. It will make it. It will undermine trust in Canadian tech. It could create trade barriers between Canada and the EU. You know, this is something that folks are talking about increasingly. Like, how will C 22 complicate deeper trade relationship and future trade deals? So I think it misses that there's a lot of homegrown concern about this bill, and you know it. You know for the small business community too, and we can talk about this more later. But like small businesses are in scope of this bill. It's not just big tech companies. The scope of Bill C 22 is wide open, and so you know, a boutique small, rather a small business running a boutique security service could suddenly find themselves subject to secret ministerial orders. And, you know, my parents were small business owners; they didn't have the security lawyers on staff. I mean, like you know, they're just trying to get stuff done. So anyway, so I think it. I think it's convenient, especially you know in the Canadian context. There's a lot of anti-American sentiment right now. We're in a trade war with the United States. The Canadian government

Transcribed by https://otter.ai

is, and you know, relationships between Canada and the U.S. are probably the worst they've ever been. And so it's easy to say, oh well, this is just a concern cooked up by big tech, but it's not. It's a concern that's shared across the ecosystem for small companies in Canada and abroad. One

Speaker 3 45:08
point that I think Dr. makes very well there is about how these policies will impact international trade, because any time that you have a difference in regulation from zone to zone, you're going to enforce different requirements on companies. So, therefore, a company that is in the US, in Canada, in the EU, or the UK, or even or even Asia, etc. they are going to need to adhere to different legislation and different protocols in each area that they operate, in some cases that is just going to be impossible. So where one where one jurisdiction says privacy must be maintained, and another says privacy must be backdoorable, no communication between those two zones can exist because, by nature of doing that, you would, you would be breaching one one side of that agreement. So, I think while governments are legislating on this individually, I think there needs to be a high degree of correlation between between requirements to enable a global framework that is achievable for all companies of all sizes, rather than just being something that the big companies can can maybe get around to doing.

Morgan Stevens 46:30
Joe, anything to to add there?

Speaker 2 46:33
Yeah, I'll be quick. I got a lot to agree with with what both Josh and James said. I do think big tech versus government that framing in many ways misses almost everyone with a real stake in the outcome. What I mean by that is, big platforms have lawyers, engineers, they have leverage to fight back, or in some cases even build a separate product for one market, or decide to pull out of the market, which is hard for many providers to do. Small developers, nonprofits, clinics, journalists, and the nonprofit cybersecurity organizations that we work with at the Internet Society that protect critical infrastructure around the world-they don't have those kinds of things. They inherit the security model that comes out of the fights that they're deeply in on the front lines, whether or not they've ever had a seat for any of this stuff. That framing also treats governments as like a big monolithic thing, and government is not in the United States. We have our cybersecurity and information security agencies, CISA, telling people to use Signal, and then and other internet encryption services. While governments elsewhere are working exactly to make that Signal style encryption, so to speak, harder to offer. That's

Transcribed by https://otter.ai

not government versus big tech. It's a much bigger argument about whose security actually matters, and who bears the risk once a decision has been made to compromise that security?

Morgan Stevens 48:08
Thank you, and to stick with you for a bit. So, from a technical standpoint, is it possible to build a backdoor into an encrypted system without weakening security for everyone else? What are the kind of technical considerations that policymakers might be missing.

Speaker 2 48:23
I love this question. No, it's not possible to build a backdoor without weakened security for everyone else. If we could do things like that, we could hire law enforcement personnel that wouldn't commit crimes. I'm not saying all of them do. I'm just saying that that does happen in the line of duty. Or intelligence officers that wouldn't go rogue, you'd be able to really say this is a bona fide good guy. Good guys don't stay good guys. You know things change, but that's just it. It's not really a technical problem here. This is a problem we can't really solve with technical means. No one has shown that they could make a bad guy-proof backdoor, so to speak, or maybe an access mechanism that would only allow the good guys through, so to speak. We had a problem here in the United States with something called the Salt Typhoon Incident, and that was the real stark, real-world test of exactly what you're talking about, Morgan. Chinese state hackers got into hundreds of U.S. telecom carriers through not like exotic or daring attacks or like espionage, but through boring stuff like unpatched gear and stolen passwords. By the way, you should patch stuff this week. It's a big patch week. Update all your software, folks. But once inside, these Chinese state hackers went exactly after what Jonathan was talking about. Kalia, the law enforcement wiretap system, they used these run-of-the-mill things, and then they went right for the east of the castle, right for the prides. And why did they go for the wiretapping system? Because that's the one thing that has clear text access to everything that people are doing, even internally, even you know deputies you may have working with you that are part of law enforcement. All that stuff is in the clear once you have compromised these these systems. So the whole point now for many attackers is to go after those wiretapping systems, those exceptional access systems. I don't like saying the word lawful access because the lawful presumes a whole bunch of stuff that doesn't exist in many cases here, and and we've been warned about this way back with something called the Athens affair in 2005, which is really dating myself here, where very similar flaws in telecom equipment, where they had the U.S. wiretapping systems in that equipment that they sold to Greece, some attacker just turned them on. Basically, fooled the thing to say they had a license for this

Transcribed by https://otter.ai

wiretapping stuff, and they tapped the Greek government in high society for 10 years. Right, so we know that these things happen. That people then people take advantage of these backdoors meant for good guys. Thanks.

Morgan Stevens 51:06
Thank you. And you've got open history, but but just to kind of expand on that, how would you describe the current U.S. approach to encryption, and how do you think it's evolved over time?

Speaker 2 51:18
Oh man, there are books. There needs to be another book lately that goes over recent stuff. Honestly, it's pretty conflicted. We sort of won the export control in the '90s, so we could ship open source code that actually did this encryption math and share it with the rest of the world and protect people in other and family and other countries. In my case, as I mentioned today, we have agencies like CISA recommending end-to-end encryption. They're saying don't use your phone as a phone. Don't use the cellular telephone on your phone because Chinese folks have access to all that. You should use VoIP. You should use telephone over signal apps because they are or WhatsApp things that are better encrypted. When it comes to the legislative front, Morgan here we have things like the Stop CSAM Act, which surprisingly would do nothing to stop CSAM, but would significantly mess with encryption. That's writing in the Senate's defense bill package called the NDAA, which scares me. Under that bill, if passed, encryption can't be the sole basis for liability for something that happens. But evidence that you use encryption, encryption would be admissible against you, which is pretty dumb, as dumb as all hell. Because we use encryption constantly, all the time and everything we do digitally, so it's pretty dumb. But to be clear, that one's not a backdoor mandate. It just makes strong encryption legally risky to offer. And so I think the the in one concrete piece of evolution, we've gone from you need to build in backdoors. And in one case, it was hilarious, right? Around the time of Edward Snowden, the FBI had this idea that your fines would would double every day if you couldn't produce a backdoor. Well, I don't know if they did math, but if you do that, very quickly get to the like entire like cash flow of the United States within about two weeks. And so there have been some pretty brain dead proposals in the past, but now it's not things like that. It's much more liability arrangements and and other kinds of duty of care and things that are much more complicated and harder to to argue technically that you shouldn't do these things. And we get into much more policy and law arguments about liability.

Morgan Stevens 53:40

Transcribed by https://otter.ai

Thank you. So I have a couple more questions for our panelists, but I just want to remind everyone that we will be doing a Q and A session towards the end. So feel free to drop any questions that you may have in the Q and A box at the bottom of the screen. So for all the panelists and Josh, maybe we could start with you. If one country succeeds in requiring a company to change how its products are secured, what happens to users and businesses elsewhere? Could companies then face you know conflicting legal obligations in different jurisdictions?

Speaker 1 54:11
Yeah, I I'll share a couple of thoughts on this. I mean, you know, the first and most obvious thing is if there are laws in another country that compromise the security of users or services in that country, and you are in a different country talking with people in that country. Obviously, you will be exposed by by extension, right? You know, thinking about the the Canadian context here, Bill C 22. It's a little hard to predict exactly how this is going to play out because the scope of Bill C 22 is so broad. It applies to any electronic service provider, which is basically anybody that generates digital information about someone and is connected to the internet. And so the scope is wide open from from the things you'd expect like cloud service providers and messaging services, but all the way down to like doctors' offices and smart device manufacturers, right? It's the full spectrum, and so I would say, like it's a little hard to make concrete predictions, but it's not that hard to imagine situations where Canada has compromised the government of Canada, rather, or law enforcement have compromised networks, and foreign users are exposed to bad actors as a result. I'd also just add quickly, you know, because of the kind of small business focus of our conversation so far, this could really hurt the adoption of Canadian technology solutions. If privacy-conscious consumers or businesses out there are looking for someone to help keep their data safe, they may be worried that Canadian tech is compromised because the orders are secret. There's no way for a consumer to know if a company has been forced to install a backdoor. That is all confidential. And so, what I worry about is that there will be a cloud of suspicion around Canadian tech after this bill is passed, and that could put our startups and small businesses at a competitive disadvantage. But I'll throw it to my colleagues to see what they want to add to the discussion.

Morgan Stevens 56:29
James, anything you want to add there?

Speaker 3 56:32

Transcribed by https://otter.ai

Yeah, I think it's it's it's very interesting when you look at at the software that people are using, and then the requirements for for encryption and for that to be preserved, because the you have to take a few a few steps along the journey here. So let's let's assume we're in a world now where WhatsApp has been subject to some some order that requires it to backdoor its its encryption. So that is a that's a thing that's happened in the world today. There there exists people with the ability to reverse engineer software. So recently, there was a GitHub account that released a very good reverse engineering. I think I think it was called Harness to allow you to do weeks of reverse engineering in a few minutes. That is going to give many more people access to something close to the underlying code of that software, meaning that it will be easier to to deduce that there are these backdoors in them and develop exploits to use them. So we're going to see an explosion there. I think we've done very well to not mention AI for the first 45 minutes here, but I think we have to have to stop the fuck on that now because you have to think right. Well, we're now in a world where we know that WhatsApp is compromised and can be reverse engineered by people. So, what do people that are trying to hide stuff do? Well, they're going to stop using WhatsApp and they're going to move to Signal. So then they get the backdoor into Signal, etc. But the end result of this is that they stop using services that are centrally owned by big tech or small tech, and they're going to use their own AI and public tools to build their own networks that are not commercial that may exist in a in a decentralized manner, and they're not going to be places where any encryption busting is going to be listened to or enacted, that all means that the entire goal of these backdoors, which is to get data in places where it's needed for good reason, fails because the people who would be giving up that data aren't going to be using the services where they know these backdoors are, so I think that that is probably the strongest argument from a rebuttal perspective as to why you wouldn't want to have backdoors because backdoors don't give you access to the data; it just pushes the data to places where you have even less oversight, even less knowledge of of what's being said.

Morgan Stevens 59:15
Thank you, and Joseph, I don't know if you also have a big dad.

Speaker 2 59:19
Sure, real quick. I love, I love this conversation. I love Global Encryption Day. Power just doesn't care about borders, as my colleagues have said. For many reasons, most companies just won't maintain a weaker version, or even a second version of a product for one market, and they may not be able to decide if they can leave. So they either ship these weaknesses everywhere, or they end up leaving the

Transcribed by https://otter.ai

market that is putting the pressure on them. Like as we had said, Signal said it would leave Canada oversea 2020, which I think that means it's ostensibly can no longer offer services to Canadians because I think the way C 22 works is that it operates on where the users are, not where the company is, and so you have to find a way to actually do your best to figure out if people are Canadian. Which I hope doesn't mean that if I'm not Canadian, I go to Canada, signal stops working, but we don't know yet, right? And the conflicts here are really real, as Josh mentioned. Proton's point here was that complying with Canadian order without going through Swiss legal process where they're located could itself break Swiss law, which is that conflicts of laws doctrine, and one glance at all the Commonwealth countries is all you need to know to know that precedent travels too. We have TCNs in Australia, technical capability notices. We have them in the UK. We may get them in Canada. Who knows? But once one democracy does one of these things, others will cite it in authoritarian regimes, where you know there are people in authoritarian regimes who need the internet, who need knowledge too, and they'll be emboldened to repress their people even more and do even more heavy-handed tactics on the digital plane, so to speak.

Morgan Stevens 1:01:08
Thank you. So we have a few audience questions. To start, are small businesses that are not specifically in security business affected by backdoor access mandates? And not all of them make end-to-end communications or storage services, but are they affected nonetheless by requirements for the devices they run on or the messaging services they use have built-in vulnerabilities? James, I don't know if you want to take a stab at that one first.

Speaker 3 1:01:35
the The short answer is probably yes, because these companies will be using a third party to do something on behalf of their client or their customer, in the same way that yesterday Google's power decided to take a break in London, and that affected many many digital services. Google weren't on the hook for that to the end customers, so I, as a Revolut user, couldn't use my account very much yesterday. I don't go to Google; I go to Revolut for any restitution. So, yes, I think the answer is if I, as a company, have chosen a provider and that provider ends up having issues, I am on the hook for the choices that I have or haven't made with that provider. So, so the answer is probably yes.

Speaker 2 1:02:32

Transcribed by https://otter.ai

I'm happy to jump in quickly. I think I agree. Backdoor mandates don't affect only the companies that are building the encrypted services, and all of us use those products and services. And so, ordinary small, ordinary. As if there's an ordinary small business, ordinary. I'll just say it. All small businesses depend on those services for payments, and it's a payroll customer data cloud source. It's a best practice to use software as a service because why would you maintain something that you don't have the core competency to to maintain? You you would hire that out, right? These small guys, I'm speaking as one of them, don't control the designs. We often get sort of slapped around by design from where it comes up higher, but they end up inheriting everything from above. So if if it gets weaker security gets built in, you end up inheriting that. If if there are more things that they have to do that raise costs, you end up inheriting the higher costs. You end up inheriting inheriting this sort of ambiguity of customer trust, where they don't know if you have a backdoor or not. So, in some cases, you would rather be able to tell your customers. Use it under your own risk, but I can't tell you what's inside this thing. So, in that in that case, today, as I said earlier, many of us are bearing risks without having a seat at the table.

Morgan Stevens 1:03:57
Thank you. So, for a second question, how much signal message encryption are better protected from hand than hats P?

Speaker 2 1:04:07
What was that?

Morgan Stevens 1:04:08
How much signal message encryption are better protected from hand than hats P? There might be a typo in there, so I guess.

Speaker 2 1:04:19
Yeah, I don't know what that means. You either are talking about part of the signal encryption protocol, the double ratchet, that I don't understand. But if you want to try again, feel free to write a different question. And

Morgan Stevens 1:04:36

Transcribed by https://otter.ai

then also, what role, if any, is there for government in mandating encryption? So doing the reverse. Josh, can I start with you on that one?

Speaker 1 1:04:47
Well, I mean, they could start by not trying to weaken it, but that would be a great initial step, and you know I think I think they're you know I understand I say that a bit facetiously I think you know government's in a tough spot right they're trying to balance competing interests I think what they need to recognize is that at the end of the day you know the math just doesn't math for backdoors that only let the good guys in, and and and you know the math just doesn't math to weaken encryption in a way that only authorized personnel can have access to the messages they're looking for. You know, in in Canada, Bill C 22 is a real opportunity to give law enforcement a number of tools. You know, as I mentioned earlier, part one of the bill is generally viewed as pretty uncontroversial. Like no one's really fighting about it. They made some amendments to it to make sure that people can get that law enforcement can get subscriber information with good process and oversight in a you know privacy respecting way. I think that there are still unresolved issues though in part two of the bill around how encryption will be protected in this country. You know, as I mentioned earlier, the Carney government has said that a big focus is to protect Canada's networks from foreign interference, to protect our data from foreign snooping, to decrease our reliance on the U.S. and a strong pro-encryption mandate. I think is going to be essential to achieving those objectives, and so I actually think there's an opportunity for government here to be a booster of encryption, a booster of privacy-protecting technologies, in an era where we're all concerned about our privacy. Yeah, that's what I'd say.

Speaker 3 1:06:47
Yeah, I think I think definitely governments have have a role to play here, and there are fairly recent examples of them doing this very well. So, certainly in the EU, in 2018 or 19, they they enforced PSD two for as a payment standard that required strong consumer authentication, and that has that that has had great effects in in removing certain types of financial fraud, then the other role that you so that's a time where they've done it well. However, the problem is that the wheels of government do turn turn slowly, and they look at a narrower sort of subset of the things that could and should be encrypted. You've only got to look at Google's enforcement of all websites being over HTTPS to achieve a higher ranking. That that change alone has made the internet a a more secure place, and that happened much quicker than than a government could do so. So oftentimes industry will move itself faster. Government can certainly help it in the right direction and mandate for the most important

Transcribed by https://otter.ai

things. But I think often often business is better placed to either differentiate itself by having a secure encrypted service or by saying we're going to push you in the right place with a with a punishment if you if you don't do the right thing.

Speaker 2 1:08:17
Quickly, as an American, I really owe this is personal, not my organization. Although I'm sure many of us would agree, I want to. We owe our Canadian friends an apology for the 51st state nonsense and threatening a close ally's sovereignty is like no way to bring in a serious conversation about anything, let alone security. So I just want to personally apologize. Government does have a role, I think. I think it's to strengthen security and not mandate weaknesses. Right, in the U.S. government sense, and a few others, they're already requiring federal agencies to migrate to post-quantum cryptography because today's encryption is not going to withstand tomorrow's threats. They're requiring a very nerdy thing called RPKI, which secures the actual internet routes that we use to communicate on. Ron Wyden, of all people, the senator in the U.S. has a couple of really interesting bills. One's called the Secure Data Act. It would prevent federal mandates to build backdoors or other vulnerabilities into software. And man, I would love to see an affirmative law that said, "Hey, let's just not let's agree not to do this ever again. And then I could spend my time doing other things, and we can all you know fight about different stuff. Wyden also has a recent, I think, global trust in American online services. I gotta read my notes. Yeah, global trust in American online services act or proposal. I don't know if it's introduced. I think it may be. Must be if I'm talking about it. Again, talking about things that aren't introduced. But that would prevent foreign governments from using cloud act agreements to force U.S. providers to reduce product security, and so I think that's the right direction. Mandate stronger security where appropriate, not just because it feels good, but when we need to actually have rules in place and then protect providers from those demands that might introduce insecurity.

Morgan Stevens 1:10:17
Thank you. So going back to our earlier question, how is Signal encryption how Signal encryption stronger than WhatsApp? Is I think the

Speaker 2 1:10:28
happy to get us started. So both WhatsApp and Signal use strong end-to-end encryption based on what's called the Signal protocol, which is a whole lot of fun, and I could bore you to death about this thing called the double ratchet. WhatsApp means its own implementation and famously uses a bunch

Transcribed by https://otter.ai

more metadata about you to do certain things. It has a whole set of like agentic offerings that can, in businesses and stuff that can do things for you in the middle of an encrypted conversation. I guess what I would say is Signal, not in the encryption side, but in terms of privacy and what they do with your data. Signal's privacy advantage is a lot less about the differences in encryption and more about collecting and retaining less information about the messages. If you go to Signal's website, you can actually see law enforcement requests. They publish all of them and they show you the response. And the only thing they have about you is your phone number, your account name, and the last time you use a service-that's all they keep, right? That's all they need to keep. Anyway, pontificate. Thank

Speaker 3 1:11:42
you. Yeah, there were some more options on that. So, so I totally agree with what Joseph said. The the service that I think offers the best in terms of communication security, is is simple X because it uses a rotating identifier for each of its users, which means that if there is metadata being stored, it's much harder to piece together who someone is over time. So it's a it's a very minor technical tweak, but it does add an extra layer of security.

Morgan Stevens 1:12:13
Thank you. So, just to wrap us up real quick to all our panelists today, you know, moving forward, what's the most important thing policymakers should keep in mind about encryption? And Josh, yeah,

Speaker 1 1:12:27
yeah, sure. I'll jump in and just say I think that policymakers need to know that small businesses and startups care about this, especially in Canada. So, if you're out there and you're listening to this or watching this, and you're concerned about what Bill C22 means for the security of Canada's networks and our digital infrastructure, or your own exposure as a business, please write a letter to your senator. The bill is about to be studied by the Senate. There's a real opportunity here to improve the bill. They need to know that this isn't just a government versus big tech issue. That this is an issue that concerns the startup economy and the competitiveness of of Canada more broadly. And there is a chance still to change this. So please look up your senator, or look up look up senators who are going to be studying the bill. Look up a senator assigned to your area. Their email addresses are all public, and and get in there.

Speaker 2 1:13:27

Transcribed by https://otter.ai

Let James have the last word. I think the most important thing for policymakers to internalize is that encryption just doesn't know who the good guys are. Doesn't know, doesn't care. It's math. It's all numbers. Good and bad are things that humans need to care about and have created. Salt Typhoon I mentioned really fascinating case. I wrote a wrote about a search for Joseph Lorenzo Hall typhoon, but that case showed us what happens when we build a special door and promise that only authorized people are going to use it. Someone else finds that door and walks through it. So I guess my my advice to policymakers without increasing my lobbying hours, here is to start with what you're actually trying to accomplish. You know, whether it's catching criminals, is it protecting children, and ask: Is the thing that I'm writing here going to actually need the medal, or is this to get me out of a political box, or to you know whatever? But making everyone less secure is not going to be the answer. You have a whole mountain of problems that you never expected by thinking that that's the answer. We have a lot better tools than breaking the security that all of us depend on, and we need to start building those tools. Thank you.

Speaker 3 1:14:49
Yeah, I 100% in agreement with with Joseph there and Joseph's thing. I think the the government need to look at or listen to the experts who are saying you can't do this because you technically cannot do this in a way that is good, and they need to move beyond the easy point scoring of we want to do this for X or Y good reason, and move into a place of saying right. Well, let's look at how we can achieve the same goals, but with solutions that are implementable and don't have enormous amounts of collateral damage. And and yeah, and look at look at those policies. That's that's it for me.

Morgan Stevens 1:15:34
Well, thank you all to our wonderful panelists for an excellent conversation today, and thank you for everyone tuning in. I hope this was an insightful conversation, and I hope you all have a great day.

Speaker 2 1:15:46
Thank you, Morgan. Thank you, Act.

Speaker 1 1:15:48
Thank you so much.

Alex Cooke: 1:04:33

Transcribed by https://otter.ai

And that's all for this month's Global Tech Swamp podcast! Thank you, Morgan and thanks to James, Dr. Hall, and Josh for their incredible insights.

If you heard anything on here that piqued your interest, head to our show notes on our newly designed TechSwamp page on the actonline.org website! And of course, we have transcripts available! You can find them on podscribe.com – just search for TechSwamp!

And of course, if you liked what you heard, please don't forget to subscribe wherever you listen to podcasts.

And that is all for today folks. Thanks for listening and we'll be back next month!

Transcribed by https://otter.ai