Silicon Flatirons
KNOW WHAT'S NEXT.

Transcript

Past as Prologue: Re-Launch of the Encryption Compendium and Discussion

October 7, 2021

Event website: https://siliconflatirons.org/events/past-as-prologue-re-launch-of-the-encryption-compendium-and-discussion/

Contents

Welcome and Introduction; Keynote, Matt Blaze

https://www.youtube.com/watch?v=l1YEpkOXzPs&list=PLTAvIPZGMUXP63tRcI-oBfVijnA2E1w0W&index=1

[00:00:00.45] Amie Stepanovich: Although, you can always reference the event led page for a longer biography on him and all of the speakers that you're going to see here today. Matt is currently the McDevitt Professor of Computer Science and Law at Georgetown University.

[00:00:14.47] His hard work seems to involve from an outside perspective. Matt, correct me if I'm wrong-- getting trolled on Twitter about election security. And basically, talking and educating people about all of the things that he has developed through years and years of research and experimentation deep, deep expertise.

[00:00:36.95] He's also probably one of the key people to thank for the fact that we're not all walking around today with a small thing called a Clipper chip in all of our electronic devices. So thanks for joining us here today, Matt, and welcome to you.

[00:00:52.52] MATT BLAZE: OK, thanks. Thanks very much, Amy, for that very generous introduction and for the invitation to come here. First of all, is my audio coming through OK, if somebody can confirm that on the chat. That would be great. OK, I'm just going to assume that you can hear me. OK, great. All right, so I'm going to talk a little bit about the early history of the crypto wars and talk a little bit about an alternative history to this.

[00:01:30.75] I apologize, I'm going to share some slides for a few minutes. But hopefully, we'll get through that relatively quickly. But I want to focus a little bit on what a perspective that I think has been largely ignored in the current debate. And actually, even in the first debate, which is just how ignorant we are of how technology is likely to go.

[00:02:13.35] And in particular, what I want to look at is the question, what if we had lost Crypto War I? That is what if-- things had gone exactly as the government had intended. And in 1993, the Clipper chip was just quickly embraced by everyone as clearly the obvious Solomon like solution to all of our problems. Where would that put us today?

[00:02:46.72] So the timeline that I'm talking about and the kind of nomenclature that I'm using is that there are either 2 and 1/2 or 3 crypto wars in our history that are of concern to us. The first was Crypto War I, which was concerned with the Clipper chip and more broadly with export controls on cryptography. The second crypto war happened after a period of maybe 10 years of detente in which essentially everyone just forgot about the first crypto war and tried to have all of the same debates again.

[00:03:30.03] And it kind of got nowhere for a while and then somewhere around 2015 or so was replaced by what's probably going to be remembered as Crypto War III. The crypto war to end all crypto wars, which has focused particularly on content scanning on user devices CSAM materials and so on. But I'm not going to talk about either of those last two so much. I want us to remember the great crypto war before we knew that it would be necessary to number them.

[00:04:13.38] So Crypto War I, I think is the period from around 1992 or 1993, depending on when you-- whether you look at the public or the secret world to 2000 when there was a kind of decisive peace treaty signed. So it all started in 1992 or it came to a head in 1992 when AT&T, the company that I worked or although, I work for the part of the company that cost money. This was produced by the part of the company that made money or tried to make money.

[00:04:54.96] They released this telephone device and it was called the TSD3600. And stood four Telephone Security Device model 3600. And that was essentially an encrypting phone that would sit between your handset, which is back-- this is back when phones had separate handsets and the body of your phone. And essentially, it had two buttons. One marked clear and the other was just a red button.

[00:05:40.44] Clear would just let you use your handset in the normal way. If you pushed the red button, what it would do was do some sort of cleverness with the interface. And essentially, set up a modem connection with a pure device on the other end and it would then do a diffi home and key exchange and show the hash of the key on the screen and then do a DES encrypted, Data Encryption Standard encrypted voice conversation over that modem link.

[00:06:29.10] So essentially, it was a way of encrypting your phone calls over an analog connection, which is all anybody really had back in 1992. Now this device was marketed by AT&T in a way that seemed almost designed to make it seem like a ridiculous product. First of all, its list price was $1,400 each. And you needed at least two of them for this to make any sense to own one, and this is 1992 dollars. So this was crazily expensive to start with.

[00:07:10.14] And in fact, I think they sold a couple hundred of them to mostly the paranoid crazies. So but in spite of the fact that this phone was not likely to be successful, at least in this form, it resulted in a complete freakout on the part of the government. Essentially, they worried perhaps with some justification perhaps not that this device would become cheaper and become very popular and would make wiretaps, which looked kind of like this. Wiretaps actually involved tapping a phone mechanically and sending a tap in the wire back to headquarters.

[00:08:06.06] This would essentially make wiretapping obsolete. So it very quickly tried to develop something to either convince AT&T to stop selling these devices or modify them in a way that wouldn't make wiretaps obsolete. And what they came up with was this called the MYK78 chipset. And essentially, MYK78 popularly known as the Clipper chip was designed to be a drop in replacement for a DES hardware encryption chip.

[00:08:54.48] That had kind of similar pin outs and a similar software interface. It used a 64-bit encrypted block in the same way and it had the same idea of initialization vectors and so on and so on. So you could relatively easily take a product that used a DES chip and replace it with one of these Clipper chips without too much difficulty. And it had two important features.

[00:09:26.05] The first important feature is it used a brand new cipher algorithm called Skipjack. And Skipjack was designed by the National Security Agency in secret, and the algorithm itself was secret. But it was kind of advertised as being designed by the same people who designed the encryption used to protect our nation's most important classified secrets. And one way in which it was sort of measurably more secure is unlike the yes, which had a 56-bit key kind of showing its age. Skipjack had an 80-bit key, which was considerably more secure and was designed to be secure well to the foreseeable future and beyond, at least against exhaustive search.

[00:10:17.04] So that was the carrot. The stick was that if you didn't include this, you wouldn't ever be able to export your product. Oh, and it had one other feature that they thought maybe no one would notice, but they didn't try to hide it. And that's that it would also send an encrypted copy of your key as part of the key exchange in a way that the government could decrypt it using essentially keys that were held for each chip in escrow by the government.

[00:10:56.17] This was as it turns out very controversial. And it set off a kind of immediate discussion in the world that wait a minute, do we really want to build wiretap ready telephones? This was very, very controversial. And in fact, the argument was mostly focused around the question, can we trust these people to keep these keys secret and not misuse them and abuse them outside of the legal process?

[00:11:37.85] So this was very, very controversial. And it really was acted as kind of a denial of service attack against the cryptography community because while we should have been designing new cryptography and figuring out how to integrate new cryptography into the emerging standards that would become the foundation for the internet and the web that was just starting to become a thing. We spent all of our time arguing about this instead or big part of our time arguing about this instead. Myself included.

[00:12:18.64] Now, I personally had just finished grad school when this all came out, and just started a job, a kind of dream job at Bell Laboratories, which was a division of AT&T, which had another division that was actually producing the first product that would use the Clipper chip. They essentially recalled the TSD3600 and replaced them with a version that included Clipper.

[00:12:54.82] So I was sort of inadvertently a little bit in the middle of this. I thought, wow, this Clipper chip is a terrible idea, nobody should use it. And I was very public in saying that, and then I found out, oh, actually, the company I work for is the first customer for this thing that I had said was terrible. But fortunately, I worked for Bell Labs, which at the time encouraged people to actually engage with the research community and be honest about their technical opinions, which was actually very refreshing, particularly considering this was basically my first job.

[00:13:34.03] So Clipper used this classified algorithm, and that meant that the cryptography had to be implemented in classified hardware. You could buy these chips, but they had tamper resistant features in them intended to prevent reverse engineering of what the actual cipher algorithm was. So the effect was that you couldn't implement this in software. You had to buy the hardware in order to do any encryption.

[00:14:08.77] And they produced a couple of versions of this. One was the Clipper chip intended for integration into devices like the telephone security device. They also produced something called the Tesora card, which they later had to rename because it turned out there was a trademark on Tesora and so they had to quickly rebrand all of them, which was a PCMCIA card. I'll get to what that was in a second that you could plug into a computer and essentially use as a co-processor to perform your encryption for you.

[00:14:47.14] There was a central key database, and that was maintained by the government. And that's really where most of the focus of the debate around this was. Can we trust the maintainers of this key database to actually secure it? It also turned out to be easily bypassed. So I discovered really in the first day of looking at this. Somehow, the NSA agreed to give me a sample of the PCMCIA card. And they invited me down to NSA and I got to go in and got a little bit of a tour and then they handed me a bag with a PCMCIA card reader and a couple of the Fortezza cards. And they said, feel free to go play with them.

[00:15:36.67] And kind of on the first day, I figured out a way of using it in a way that bypassed the key escrow feature, but still used the good 80-bit cipher. And that kind of helped to derail it, but it really wasn't the problem. It was a very simple technical hack if I hadn't discovered it somebody else absolutely surely would have. But it would also have been relatively easy to fix had this been something that there was any real demand for.

[00:16:17.92] So Clipper had technical weaknesses, but they weren't the real problem. So we finally won the crypto wars in 2020. The Clinton administration finally basically got rid of the stick. And agreed to allow non-escrowed cryptography to be exported and allowed for the market to just introduce unescrow cryptography into standards. And it cost us seven or eight years of arguing about this. But in the end we were finally able to get to work and securing the web and the internet, and all of the things that we're seeing today.

[00:17:14.53] So we finally won. But what I want to look at is the question of what if we hadn't won? What if it had gone a little bit differently? So there were two big risks with Clipper. One was, can we trust the system if it works properly? That is, can we trust that the key escrow database would only be used for the stated purpose of enabling wiretaps with warrants. And that was chiefly a political and policy question. A really difficult political and policy question.

[00:17:55.21] But it didn't really have to do-- you know, it kind of assumed that the technology worked properly. And then there was a second question, which is this whole thing was designed in secret. Can we trust that it will work properly? Can we trust that there isn't some backdoor way of getting access to this key escrow database? Might someone break into it, might there be some weakness in the algorithm that would allow somebody to easily break Clipper encrypted conversations. Or was there some way to bypass the system?

[00:18:33.67] And as a member of the technical community, and I think most of my cryptography peers were really focused on that question. So the two big risks are, what if it works properly, but is misused? And the other is, what if it's got a flaw in it that allows it to be misused by others? But actually, there was a third much worse risk that really we hadn't thought about very much, which is what if Clipper had been a great success?

[00:19:06.49] What if we figured out a way to ensure that the key escrow database would not be misused? I don't know how we would do that. But let's assume somehow we were convinced that the only way you could get access to this would be with a proper warrant. And that we were all happy with that as a proposition. And there hadn't been any technical flaws or anything like that. What if Clipper had just been a big success?

[00:19:37.93] And this became the cryptography standard that we all used as the US government had hoped. And somehow all of the international problems of why should people outside the US use this. What if everybody just decided, yeah, this is the right thing to do. We all trust the US government. And we all trust this database and nothing went wrong. What if it had succeeded? And I would argue, that would have resulted in a far worse outcome for us today than we would have had any of the things we were worried about come to fruition.

[00:20:16.04] So in order to understand why I would say something like this. I want to go back to 1993. In 1993, there were crypto wasn't really one anybody had heard about, but to the extent anybody had heard it, it still meant cryptography. We were discussing crypto policy on a usenet news group, which was like a message board that everybody on the internet had access to called sci.crypt.

[00:20:50.50] And when we wanted to share papers and results and documents and things like that, we did it via something called the FTP protocol. And that was true because at that point the web really did not exist. It had just been sort of proposed a few people had early web browsers, but it wasn't really anything that anyone heard of. Certainly, nobody confused the web with the internet back then because most people hadn't even heard of the web to the extent that it was there.

[00:21:23.55] Mostly the internet meant the compact disks that AOL regularly sent out in the mail to people that you could use to load the AOL software on your Windows 3.1 machine or you could use it as a coaster or have fun microwaving it. So most of the people that were on line were using proprietary services like AOL that they reached via dial up modem.

[00:21:56.58] Fax machines were still incredibly important. And were largely more important than things like email for business to business communication. In fact, there was a third Clipper chip product, although, they never actually brought it to market, which was the encrypted fax machine because I think they understood that you couldn't really be taken seriously as a communication device, unless you supported fax.

[00:22:27.99] The future of telecommunications was ISDN, which allowed for a kind of native 64-bit connection with two channels. So 128 kilobits of incredibly high speed data to your home. And that was really regarded as the future of high speed data. Cell phones existed back then, but they were mostly an expensive luxury and they were incredibly awkward and clunky.

[00:23:01.51] They still mostly had models that were designed to be installed in your car. We still hadn't figured out back then that telephones were associated with people rather than with places. So this idea of communication of wiretapping and what you were securing was really place to place rather than person to person. And this idea of mobile computing wasn't something that anyone other than crazy visionaries really thought about.

[00:23:37.65] No one knew anything about Edward Snowden back in 1993. In particular, the NSA had had a few leaks come out of it, but in every single case, they were spies directly selling secrets to foreign intelligence agencies. This idea that NSA secrets would become publicly leaked was simply not something that was within the realm of anyone's experience, because it had never actually happened before.

[00:24:10.84] And the main cipher that we were using was the data encryption standard, which was about two decades old at that 0.56 bit keys and relatively slow to encrypt in bulk in software. So you could put DES in software, but really it was designed to be implemented in hardware.

[00:24:38.73] So in 1993, what everybody kind of understood intuitively was that cryptography was special. It wasn't widely used. There wasn't really a wide need for it because most communication was over wire lines. Tapping a communications link would involve-- actually getting access to the wires, which was who could do that. And the getting access to stored data on a computer would involve physically burglarizing the computer and stealing the disk, which is possible.

[00:25:22.23] But it's certainly not something you could remotely do over the cloud because the cloud in 1993 was a weather feature. It wasn't a place to store your data. So attacks on communication meant physical wiretapping and attacks against stored data meant for the most part actual physical access. And because almost nothing was connected full time to the internet except for big server machines at companies that were sort of still a little bit on the margins.

[00:26:06.15] You could put a PCMCIA card as the main co-processor interface on your 15 pound laptop. And you had a special briefcase for your laptop because it was so big, heavy, clunky, and fragile. So the world, it definitely predated the cell phone and pocket computing. And more importantly, it predated wireless and this idea that computing would be so heavily integrated into our lives.

[00:26:40.60] So what am I getting to? So the 1990s were a really important time in our history because it was just before everything got so big that you couldn't change it. The basic standards for the internet already existed from the late '70s and 1980s. The 1990s were when most of these standards were being finalized. And in particular, that was when almost all of the cryptography and security standards were being developed from the start. And our assumptions were rapidly changing.

[00:27:21.72] Hardware was becoming much faster, cryptography and software was starting to become a real possibility by 1993, even though historically, it had been something that you really needed hardware for. By 1993, we were starting to see that it was practical to use general purpose computers to do cryptography.

[00:27:44.53] So if Clipper requiring are all of our cryptography to use not only hardware, but particularly expensive hardware based on a classified chip that in 1992, 1993 dollars cost about $25 a pop. So it would add $25 just for the chip itself, not to mention the additional engineering cost of including it. So if you wanted to include encryption and Clipper was what you had, you basically had a choice between not including encryption and including what was guaranteed to be expensive marginal cost encryption.

[00:28:36.27] And that might have seemed like a reasonable thing because historically, we had always used hardware to do encryption around 1993. But by 1994 or 1995, that was pretty plainly ridiculous. We would mostly have to do continue using wireline connections for anything requiring security because our Wi-Fi connections, which mostly didn't exist yet. Our cell phones which only rich and self-important people had wouldn't be able to support encryption.

[00:29:20.64] Our web sessions, which hadn't been invented yet wouldn't have HTTPS or SSL encryption protecting them. And pretty much everything else we used for communication, it would never occur to anybody to integrate encryption as a standard required part of the standard. It's also likely that AT&T would still be in business. AT&T in its form that existed back then would still be in business. And a big part of its business would be selling expensive NSA approved telephones.

[00:30:01.32] So maybe that's a good thing. I'd still be working at Bell Labs had Clipper been successful, and it would still be a great job because this company would have had more money to spend on research because it would just be making money hand over fist selling crazy expensive encryption phones to everyone who needed them. So we are-- let me stop this.

[00:30:29.01] I just want to point out. We are equally ignorant today of what the future in 20 to 30 years will look like, as we were in 1993 about what 2021 would look like. The standards we're developing today just as the standards that we developed in the 1990s are being used in 2021. The standards were developing in the 2020s are going to be with us in the 2050s.

[00:31:14.02] So I want to urge us to be very, very cautious and very humble about our ignorance and what we're imposing on technologies that haven't been invented yet. The current debate is have shifted to scanning of encrypted data before it gets encrypted to see if it has CSAM imagery. That's a currently the hot debate du jour.

[00:31:50.38] So what if that debate gets settled and we invent a standard for doing that today in 2021 based on all of the assumptions about what the world looks like from a technological and social point of view in 2021? Are those decisions and those assumptions still going to be valid in 2051? I suspect, we will regret embedding anything today into those standards going that much farther. So I think I have a few minutes for people to ask questions or make comments or give me a hard time.

[00:32:40.30] Amie Stepanovich: Thanks so much, Matt. I invite those in the room to join me in applause. I think you can hear us.

[00:32:47.32] [APPLAUSE]

[00:32:51.11] So not used to clapping anymore. We've been in virtual rooms for way too long. Silicon flat irons has what we call the [INAUDIBLE] rule, after our founder where you always invite a student to ask the first question. I believe we have Taylor here to ask a first question of [INAUDIBLE] here up, and I'm going to step back to give her the podium.

[00:33:18.78] TAYLOR HARTLEY: Hello. Thank you so much for that. My name is Taylor.

[00:33:21.89] MATT BLAZE: Hi.

[00:33:23.77] TAYLOR HARTLEY: OK, thank you. I'm Taylor Hartley. I am an MBA candidate. I was also a cryptologist for eight years within the Navy. I worked at NSA. I worked at NSA during all the Snowden stuff too, lots of fun. But now, I'm in the commercial sector. And I have noticed that the government is switching to the cloud for data storage, and I just wanted to know if you could maybe give me some pros and cons of what do you think encryption has to move with the cloud? What's that going to look like? Is this going to be better or worse? Just any opinion you have.

[00:34:08.10] MATT BLAZE: Well, so let me make two very kind of obvious observations. The first is that the cloud can't exist without cryptography. If you don't have high confidence in your ability to secure data, putting it on random servers somewhere out there on the internet getting replicated, however, many times. It's simply just not viable. So there are all sorts of economic and reliability benefits to the cloud.

[00:34:41.96] There are also some disadvantages. But people seem to really like the ability to do this in particular outsourcing system administration for servers to people who can do it at scale is economically very sensible for small and medium size entities and even large things like the government. But you simply can't get that benefit if you don't trust that your data is secure.

[00:35:13.46] So unless, we have not trust encryption highly available. But encryption that we really trust-- that we trust just as much as we would if we had complete control over that data locally, we just can't have the cloud. The cloud followed the availability of strong ubiquitously available encryption. The second is I don't think the cloud is such an unconditional benefit as we often think it is.

[00:35:47.96] One of the problems-- then this isn't a security problem, but it's rather a reliability problem is that we have kind of lost in small and medium sized enterprises, the expertise to manage things locally. We're utterly dependent on outsourcing servers and outsourcing big, big parts of our IT. Because that expertise is just not available locally at small scale if the cloud services go down. You probably don't have somebody on staff who can stand up something locally. So it's still not without risks, but those risks aren't so much confidentiality as they are reliability and availability and recovery.

[00:36:46.57] Amie Stepanovich: But seeing anything in the Q&A, I think we have time, though for one more. I'm going to take moderator's privilege here, Matt, because you started with three crypto wars on your side, and then went on to talk about what you called the grand crypto war number one, which we didn't know the number. But you reference Crypto War III as the war to end all crypto wars if you remember back. Do you think that's true or will there be a Crypto War IV as you see [INAUDIBLE]?

[00:37:20.92] MATT BLAZE: I'm trying to be a combination of optimistic and pessimistic here. I'm optimistic because I can't handle a fourth crypto war, just the thought of that is just too horrible to contemplate. I'm hoping that whenever it happens, I'll either be retired or dead.

[00:37:39.43] But also, I think this crypto war has the potential to be incredibly destructive because if anything things are moving more rapidly than they were back during the first crypto war back during the 1990s. We are having an acceleration of the way technology is moving. And anything where we normalize and including standards client side mandates for scanning data is aside from the risk of direct misuse or the risk of technical error.

[00:38:20.53] The risk that that's just going to be incompatible with future innovation is I think one of the hardest to talk about, but it's one of the most serious to worry about because we won't know what we lost. If there's some huge data leak, at least, we find out that there's been a disaster. But had Clipper been successful, we wouldn't have the cloud, we wouldn't have the secure web. Cell phones would have to have this extra chip hardware in them. And we wouldn't know that that wasn't normal.

[00:39:04.10] Amie Stepanovich: So we do have one more minute and there's a question in the chat I've been alerted to from Simon [INAUDIBLE]. Has CALEA achieved-- CALEA is the Communications Assistance for Law Enforcement Act, for those of you who don't know the acronym. Has CALEA achieved in some part with the Clipper chip failed to do?

[00:39:21.39] MATT BLAZE: So CALEA actually happened at about the same time as the Clipper chip. You know, they were roughly simultaneous. And they were concerned with different things. CALEA is much less relevant than it was at the time because at the time CALEA was passed, voice telephony was the way people communicated, and fax machines and so on.

[00:39:48.36] To a large extent, a lot of the communications that were envisioned under CALEA have been supplanted by internet communications that mostly are encrypted today. So I think actually not.

[00:40:09.96] Amie Stepanovich: All right. Well, we are at time. Thank you so much for such a great presentation to open our day. Thanks for joining us and tuning in.

[00:40:16.61] MATT BLAZE: Oh, thanks for having me. Thanks for having me. I'm looking forward to hearing that today.

[00:40:20.48] [APPLAUSE]

Student Presentation on the Encryption Compendium

https://www.youtube.com/watch?v=Y6rvEl1_wLI&list=PLTAvIPZGMUXP63tRcI-oBfVijnA2E1w0W&index=2

[00:00:00.06] Amie Stepanovich: They're in the room a 2L here at the University of Colorado School of Law, Stacy Weber a 3L at the University of Colorado School of Law, and virtually we have Will Shand a PhD student at the University of Virginia. Hi, Will. All right. I well let you all take away. Thank you so much.

[00:00:41.39] STACEY WEBER: Good morning. My name is Stacey Weber. Bryan and I are going to do our best to stay six feet apart up here, we're just delighted to be here today, just want to start with a big thank you to Amy, to Silicon Flatirons center for the opportunity to work this project and to get to share some of our work with you today. So we'll start with some introductions again, I'm Stacey Weber, I'm a 3L here at the law school, I was on the first research team of the encryption compendium in January of 2020. So that initial phase getting up and going getting resources, and contributing to the research portion.

[00:01:25.49] BRYAN HINDIN: Hi, everyone. I'm Bryan Hindin. I'm a 2L here at Colorado Law, I was on the second iteration of the encryption compendium research team, my team focused primarily on taking all of the work that Stacey, and Will did, and getting it into the format you can now see online today.

[00:01:44.04] WILL SHAND: And Hello, everyone. I hope I'm coming through, OK, so I could be there today, but I'm Will Shand, as you mentioned, I'm a PhD student at the University of Virginia. And I was also part of the first team working on the encryption compendium, mostly focused on designing the website, and making it to like, a publicly accessible resource that you can all see today.

[00:02:07.30] BRYAN HINDIN: So you may be asking yourself, what is the encryption compendium? I think the best place to start is with our mission statement a little bit of overview what we did. The encryption compendium at concept is meant to be, your one stop shop central hub for policymakers, legal practitioners, anyone in the general public who's interested in learning about the encryption debate. As Professor Blaze indicated in his fantastic presentation earlier, it's quite a broad subject, a lot of different opinions, and subject matters that really need to be fleshed out in full force. And we wanted to create a one stop reinforcing database for that.

[00:02:48.04] Now, as was also indicated by Professor plays, a lot of debates surrounding encryption have been somewhat cyclical in nature. And there are recurrent themes, and the encryption debate is largely characterized as two competing interests. We have user privacy set against different iterations of the conversation around national security, on one end encryption provides really valuable resources, and importance user privacy, and security on the internet, and the way that we conduct our daily lives. And on the other end, those same protections, at least from the standpoint of national security interests are conceptualized, as an impediment, they impede law enforcement investigations, and in different facets investigations, and the prevention of cyber crime and intelligence gathering.

[00:03:38.70] STACEY WEBER: So in building the compendium we really wanted to be able to counter these various threads, and reflect the conversations that were going on. But also do so in a way that allowed everyone involved to trace the way those ideas have evolved, have resurfaced, have recirculated with each turn of the wheel. And we are hoping that would allow understanding of the conversations to help us better navigate them moving forward. So for example, as we have up here depending on how you might count, we've been through, at least three cycles and sets of terminology around the need for government access, what that should be called, what it should look like. And we wanted to make sure those themes, and those consistencies where reflected in the compendium.

[00:04:25.86] Which really brings us back to the mission that we were working on, and the way it unpacked into three major. So we wanted the encryption compendium to have a comprehensive aspect, we wanted

to capture resources from 1970 to present, not every single thing that's ever been written about encryption in the last 50 years, and drown users in mountains, and amounts of resources. But still quality over quantity, pulling together the major resources, the big conversations, the turning points, the major themes that reflect the breadth of the debate in a usable and accessible way for users.

[00:05:05.56] And that means it also had to reflect all facets of the conversation, if it would be useful to anyone, much less everyone as we're hoping, it needs to be holistic and needed to be balanced, and complete. So we aim to work to give all of the powerful arguments that were contributed from all sides. And then finally, we prioritize tracing the historical development, and the substantive policy positions making sure we had the big pieces. And then layering the themes on, as we've been saying quite a bit to really pull out. Here's what happened at each stage, and here's how it connects, here's how it traces through a larger picture and pattern.

[00:05:48.84] BRYAN HINDIN: There's an overarching long term focus of ours, maybe somewhat optimistically. We're hoping that the collection of all of these resources in one place can at least contribute to ending the stagnation, and cyclical nature of this conversation. With the idea being that if all of our resources are readily available in one place, we can readily identify how these conversations have transpired in the past, and also hopefully prevent repetition of the exact same conversation, as we transition into new phases of the encryption conversation.

[00:06:19.64] WILL SHAND: So the Christian compendium itself is a publicly accessible resource that you can see today, it's available on encryptioncompendium.org, if you're looking for it. And when you visit the site, you'll be initially greeted with our mission statements, and this search bar that you can use are accessing the compendium. We currently have about 200 or so compendium entries currently listed, which can either look up by direct text search on the summaries that Bryan and Stacy have written, which they'll be going over a little bit more later on, or you can look up based on tags on the entries themselves, which include categories, like, specific topics, such as the Clipper chip, or time periods countries, that the compendium entries are based around, and so on, and so forth.

[00:07:16.07] BRYAN HINDIN: We may be asking yourself, what's actually in it? Stacey mentioned one of our overarching goals was to get a variety of resources opinions, but we also wanted to ensure that the substantive pieces, were very in and of themselves. And so that in addition to getting a wide array of opinions, you've got a wide array of type of material that would be valuable in understanding the encryption debate, and bring it to the fullest possible. So the first category of those materials is legislative materials, as by and large, this is where a lot of the substantive progress we would hope takes place. If we're going to reform certain aspects of encryption policy, that's going to take place in the legislative capacity.

[00:07:55.84] And so as an example, within the compendium, we have draft bills, like, the 2016 draft of the compliance with court orders act proposed by Senator Burr, which relates to going dark debate and efforts to force private companies to comply with court orders to essentially provide decrypted material. Similarly, in keeping with our goal of capturing the entirety of the conversation, we wanted to make sure that the substantive conversations were captured and that was largely in the text of hearing materials. So we also have hearing materials from, for example, Senator Chuck Grassley, and the conversations in 2015 surrounding the going dark debate, and exploration of the different policy interests that emerged within that debate, and we wanted to ensure that the compendium had those really valuable resources for you on one spot.

[00:08:44.86] The next category of materials that we have are what we characterize, as reporting and advocacy materials. This means largely journalistic coverage of the encryption debate, as well as opinion pieces from legal practitioners, for example, here we have two, examples of the encryption debate happening in real time. The two political articles that you see on the slide actually interact, and respond

with one another, it's a really great example of a conversation that takes place in the encryption debate happening in real time.

[00:09:14.45] The first is a piece from Cyrus Vance, which really stresses the National security interests related to decrypting smartphones. And it's another iteration of the going dark debate that we have and in contrast to that, we have your response, which stresses the importance of user privacy, and why a conversation surrounding criminal activity on smartphones are misplaced, or weighing privacy interests above concerns, specific concerns, that are stressed in the article itself. And similarly, we also just wanted to make sure that news events were captured. So as you can see, we have pieces that cover large developments within the space of encryption from a non-legislative space.

[00:10:03.94] And finally, I think no database of encryption materials would be complete without the foundational scholarly, and scientific works that form the real substance of these conversations. So for example, we have foundational peach's-- pieces excuse me, such as Whitfield Diffie and Martin Hellman's new directions in cryptography, which provides scientific analysis on the efficacy of early encryption. We also have more exhaustive policy pieces, such as cryptography his role in securing the information society by the National Research Council, which offers really extensive background on cryptography, and its overarching policy applications-- implications.

[00:10:40.80] And finally, we have retrospective pieces that similar to what we're trying to accomplish with the encryption compendium, look backwards, and talk about the drawbacks of repetition in the encryption debate. And why much like, our encryption compendium highlighting the cyclical nature of this debate? Can be valuable? In trying to stem some of the impeded progress that comes from repetition. And what we would characterize, as stagnant conversation.

[00:11:10.94] STACEY WEBER: So given this look at, what the encryption compendium is? What it includes our goals, and our mission? We also wanted to take a little bit of time today to talk about, how we created it? What went into making it? For all those academics out there sharing our methodology, and also the lessons that we learned along the way.

[00:11:32.95] So first step, as students we were new to the subject matter, which meant a lot of the way we organized and began our research how to accommodate the fact, that we were on a huge, and incredible learning curve. So we read a couple of introductory sources just to get our feet on the ground a little bit, and then try to divide and conquer, and cast as wide of a net as we could to pull in a lot of sources, and get the research team up and running. It actually turned out that our research styles were quite varied, and that served our research very well, so we all had a different instinct of how we wanted to become immersed in this topic.

[00:12:12.27] One student said, OK, I'm going to go by topic, I'm in charge of Clipper chip and we said, OK, great, we'll stay out of your way. Someone else looked by time period and what were the developments from the 70s to the 90s that led up to the Clipper chip debate, let's make sure we have all of this. Another student type of source saying, what's the government doing? Let's get all those legislative materials, those hearing testimonies as committee reports that Bryan was telling us about, and make sure we have that action in our database. And then another student took a rabbit hole tree root approach, following the footnotes, starting with a couple of major pieces, and then tracing all the sources that the experts cited to make sure we captured those.

[00:13:01.24] We also tried to automate wherever possible to assist our coordination that as we are getting up to speed substantively, we wanted to reduce the administrative work, and we also needed to stay coordinated and organized as a team. So Zotero was our very good friend, it's a free, and open source software, or Foss group resource, and research management tracker that it has a website, a browser plugin, and a desktop app that you can capture sources. It will pull in all the bibliographic information for you, so we weren't manually entering author names, URLs, dates of publication closely.

[00:13:42.99] And lets us designate a source type to organize the information, stores a snapshot of the source, and even has a tag supporting function. So this was a really helpful way that the research team could coordinate things or stay organized, make sure we weren't repeating each other's work, and then also coordinate with the dev team to say, OK, here's everything we have you go do your design and presentation magic. And that was a really helpful tool Zotero and Google Drive were very good friends in those initial stages.

[00:14:17.43] We also, then moved into trying to build out this as an iterative process. So we did look backs, for example, this chart was one look back, looking at our sources by topic, and making sure we weren't missing anything, our topic spelt out, are we missing one is one a little thin? We also look by time period, is there a gap in time that we need to go back and make sure our research is complete? Making sure do we have all voices on an issue not just what we found first, or not something that personally resonates. And we also have that iterative process, and reflection helped us refine our research process.

[00:14:59.49] So two things that really stuck out were we needed double tabs for timing. So we were tagging the decade that each source was published in. But for sources that looked back or gave a history, for example, there are some great pieces in the 2000s that reflect on the 1990s, they needed to be tagged, as 1990 sources to make sure that we had that reflected that those are helping us understand what was going on in that time period. And finally, we were looking at links, so some of them-- some of the links broke, and the Wayback Machine became our very good friend, which meant we were focusing on making sure our sources were all recovered. But then also we had to find a way to make sure we protected our resources so that someone didn't follow after us, and come across links that had broken after our research.

[00:15:57.49] And finally, we had some lessons learned, some of those problems we saw coming, and solved along the way, and other ones we had to go back and face later. One was I've been told this in class, it's turns out to be true now is better than later to do work. Zotero is a magical source, but it's formatting it's inconsistent. Some titles are pulled in all caps, some are pulled in all lowercase, and that's a nightmare to go back and look at and fix later. Some sources are the metadata isn't complete for the bibliographic information and so going back and doing that cleanup work showed us that we it's a good idea to do it as we go.

[00:16:40.41] That also led us to realize we needed to start and go back and find and store clean PDFs of every resource we encountered, some of the sources were behind paywalls that we could access through our student accounts so that was great for us. But not great for assembling a complete resource that's directly accessible, at least within the center, and then realizing that public accessibility is a distinct mountain that would need to be climbed in the future. We also needed those PDFs then to be clean, and not have advertisements printed over them, so that entire process of making sure our data, and our research was protected ended up having several facets to it.

[00:17:19.96] And finally, Zotero is beautiful aiding function of suggesting tags for us, turned out to be a terrible, terrible idea, we had a granularity problem every resource in the encryption compendium could be tagged encryption, but that's not useful. Similarly, some of the tags were overly granular that they were only indicating one or two sources and that's not helping get a sense of the conversations either. So we ended up going back, and doing a lot of tag refinement to make sure we were properly localizing each conversation how it fit together, but in a way that's again user friendly.

[00:18:03.34] BRYAN HINDIN: So the second research team that worked on the encryption company, was primarily focused with taking all of the fantastic resource, and some of the website filled out. But the first team had done, making sure that the material on the site, was actually as valuable as possible to our users, we didn't want just a collection of resources, we wanted you to be able to find the resource you're looking for, and then have a snapshot into what it actually said. We didn't want you to have to go through the exhaustive process of reading what in some circumstances is a three, 400 page book that may have

been as published as recently as 1970, and trying to draw conclusions from it as to whether or not, it's even a value to you.

[00:18:39.67] So our team at the beginning of our semester identified, what we thought were the five most important things we could provide for every resource in the site. That was the source name meaning, not just the title of the material, but who published it, what group or organization they belong to, and their occupation. In addition, we want to make sure that we captured for you a thesis statement essentially, that boiled down to one to two sentence summary of the overarching argument of the resource itself. Third, we wanted to make sure that any relevant factual background we can provide around the resource was there, so especially in circumstances, like with Bill drafts, you understood the context as to, why it had arisen. And ultimately, that brought us to our fourth point, was any post-publication outcomes that we can provide, was the bill enacted, did it die in Congress, or with scholarly pieces, for example, what impact of anything that we could assess that it have on the conversation.

[00:19:37.48] And then finally, if we could capturing an overall purpose and a setting within the encryption debate. So as we go to the next slide, show you an example of what the site looks like now. Now for every resource that you access on the site, you will see a page that looks, like this that's title, tags like, Stacey mentioned, author, publication, date, and the URL. In addition to the summaries that our team built out. And so here while I won't make you read the site in detail, source is captured Professor Alan Rozenshtein of the University of Minnesota Law School.

[00:20:09.78] We have a purpose statement, there's a warning of the dangers of foregoing end to end encryption, and the anticipated consequences of the powers granted to the attorney general, in the then circulating draft of the EARN IT Act. We have a thesis, which is essentially a summary of the main arguments Professor Rozenshtein makes, and a little bit of factual background in post publication outcome. So we have a little bit of a summary around Senator Lindsay Graham's proposition to the bill, and its status.

[00:20:38.98] WILL SHAND: And finally, the web Valentine also learned its share of lessons throughout designing the compendium, over time we-- and I'm sorry, joined by a friend here on camera who wants to talk about out, as well. [LAUGHS] All right, over time we learned a few different lessons about, what the requirements were for a site like, this and what's we want to make sure we built into the site to guarantee that it would be able to live on after us. So our first major goal with design site, right? Was to work with tools that's we like, that with tools that we were familiar with as developers. But also tools that the researchers themselves for developers were familiar with.

[00:21:27.52] So in Stacey's team's case they decided to choose Zotero, which was great for us because their terror has a nice public API that we were able to access, and use to collect all the entries from Zotero, and publish them on the site. That was a major goal for us, making sure that we could actually work well, with the researchers, and accommodate their research style. Another major goal for us was making the site, as easy to maintain deploy, as possible. So that was a lesson that we had to learn the hard way, we came into the project with a lot of technologies that we're familiar with and that we really, liked, like Django, Docker, Postgres, whatever. And about, like 3/4 of the way through the project we realized, wait, this is way too complicated, this is going to be horrible for anybody who comes after us especially if they're not already familiar with these things, right?

[00:22:19.86] So we decided, hey, let's make-- let's strip this down as much as possible, let's make this the simplest as simple as we possibly can. We managed to convert this incredibly complex technical stack that we developed into a fairly basic-- into a fairly basic website basically, as simple as we were possibly able to make it, while keeping the majority of the functionality. So that we could both make the site again, like, as easy to maintain for future teams that were going to join the encryption compendium in the future, but also make it very easy to host a site in a number of different ways, regardless of what resources were available.

[00:22:58.02] The final goal that we were trying to achieve with the website was just making the compendium, as easy to extend in the future as possible, so I'll be going to that a little bit more. But we have all these cool ideas that we still want to add to the compendium to make it, like, the most useful possible resource for anybody who's going to be doing research off of it. And so we hope that our design that we made would help facilitate that extension of that enhancement in the future.

[00:23:31.14] BRYAN HINDIN: And much, like, Will foreshadowed just as the encryption debate is a living, breathing thing ever evolving, we view the encryption compendium the same way, and we hope that our tenure on the encryption compendium won't be the end of its evolution. And as the debate evolves, and move forward, we hope that the compendium will continue to capture these resources, and capture the debates that it can date is of value as we envisioned it. And to that end and I know it will get touched on a much more detail than I could ever possibly do, later this afternoon, and I know Professor Blaze indicated a little bit as well. There's a new frontier in the encryption debate, not necessarily a new software, but definitely a new conversation, surrounding client side scanning. And it's becoming increasingly important part of the debate, especially with companies like Apple, considering implementation of softwares, like, their CSS synthetic systems, synthetic match system to combat the dissemination of those materials online.

[00:24:24.91] So we've continued even beyond our 10 year a little bit to try and capture those resources, and Will is going to go into significantly more detail about how we hope the community at large, can aid in capturing these resources moving forward. But we recognize that this is going to be a very pertinent part of the encryption debate moving forward. So much in keeping with the way that we've captured resources in the past, we have legal practitioner assessments of the status, and implications of CSS in the present day.

[00:24:52.86] And we also have much deeper analysis of the actual efficacy of these systems, and the implications that they relate to user privacy, and evaluating the merits of the National security and in the system context criminal law enforcement investigation capacities. And we know that finding a balance between the interests of privacy and law enforcement entities as has been the case throughout all iterations of the encryption debate is going to continue to be a key focus of research, and policy discussions in this context. And so we hope moving forward, continuing to catalog this research will only aid, and hopefully prevent cyclical conversations surrounding the new manifestations of the encryption debate.

[00:25:37.85] WILL SHAND: And finally, there's still a lot of development going on the compendium so of course, as I mentioned, the encryption policy, the encryption debate is continually evolving it's changing all the time. So we're hoping to get to the point, where we can start accepting public submissions of new compendium entries, and be able to update the compendium in real time, as these debates are happening. We're also looking to add some more tools to the compendium to help researchers, so for instance nice timeline to show the relative event of relative occurrence of different important events, and encryption policy history. Of course, for instance, the three crypto wars that Professor Blaze mentioned earlier, but also more recent events, and smaller events, like, the recent Apple CSM debacle and so on. So tools, like that, tools adding notes to compendium entries being able to export compendium entries in mass and so on.

[00:26:48.30] And finally, we're also looking to include more resources on encryption policy outside of the US so of course, there are many countries outside the United States, where there are parallel encryption debates going on that are equally important to the ones going on here, where we live. And those also have a massive impacts on people living throughout the world. So we'd like to expand the companions to include more international resources going into the future. So today there are two main ways to help get involved in the encryption companion. First is that we have a public GitHub, so if you or someone enjoys contributing to open source projects, the entire encryption compendium is currently open source. And

we're accepting submissions of pull requests for new code and new features that you'd like, to add to the compendium, but also bug reports and so on. And so we do really appreciate any feedback that people provide through our public.

[00:27:49.39] And finally, of course, Silicon flatirons is the organization that's been sponsoring, and posting encryption compendium. So anything you can do to help support silicon, but also help to support encryption compendium quite a bit as well. So thank you all very much for your time, and Yeah, we'll turn it over to questions, if there are any.

[00:28:17.05] Amie Stepanovich: All the way over here. Thank you, bill. And Brian, and Stacey. If anybody does have questions? Please, put them in the Q&A or in the chat, which I'm trying to monitor simultaneously. So if I'm a little slow I apologize, we do have one in the Q&A now, or somebody says it sounds, like, a great compendium so thank you to Andrew Zak. Are there any areas of editorializing, any places where you contribute your own thoughts or opinions?

[00:28:50.82] STACEY WEBER: I'll go first on the research side you can go some research, that was one of the things that we've really focused on is that, we want this to be neutral on the street policy neutral, politically neutral. And we felt that it takes away from the value, quality, and credibility of the resource to put our own spin on it. So that was actually something that was very actively present in our minds, as researchers going back, making sure we weren't missing any voices in collecting the resources. And then I fought the great battle of the tags, and let the summarizing to Bryan and his team.

[00:29:27.27] BRYAN HINDIN: And I think my answer is very similar. We provided an example of a summary that we prepared, that we tried to make as objective as possible. And I think the potential for editorializing really exists in that thesis section of it. So I personally really emphasized making sure that in any summary I provided, I always use the exact verbiage, I often did direct attributions, pulled exact quotes so that I was not editorializing in any capacity, and I know that my team members who aren't here currently also did the same thing. So I would emphasize that we focused on neutrality and ensuring that the resource was not biased, as much as we possibly could.

[00:30:04.56] STACEY WEBER: Although, I'll say we're still human so if you catch something that's missing, or calls on us, we can fix it because the point of the resources to be.

[00:30:15.86] Amie Stepanovich: From Professor Jim Currie, this might be a question for you Will. Do you worry about hacking, or cyber attacks, or-- and then I have dot, dot, dot, dot of scare ellipses, I would say scare quotes. This is like a scary ellipsis.

[00:30:34.46] WILL SHAND: Well, for security, I worry about them personally, especially with how ominously posed that question. But as for the opinion itself, that isn't a major focus of the compendium at the moment although, it does tangentially cover, a lot of things that we were interested in, there are certainly many things, like, backdoors into encryption mechanisms, right? Which overlap greatly with what you're talking about? So while it's not the primary concern of the compendium is definitely something that we have on our radar, and try to incorporate, wherever possible.

[00:31:16.27] Amie Stepanovich: Any other questions in the room, would be remiss without asking? Let's see if anything else on, what I want to offer a huge round of applause to all through this.

[00:31:29.25] [APPLAUSE]

[00:31:32.97] You really, did a wonderful job and we're deeply grateful for everything that you've put into this. And thank you just from the bottom of my heart. We're going to take a short break now from this presentation--

Panel Discussion

https://www.youtube.com/watch?v=RtFTWcCm3Vw&list=PLTAvIPZGMUXP63tRcI-oBfVijnA2E1w0W&index=3

[00:00:00.42] Amie Stepanovich: So to help navigate those waters, I'm joined by four folks with a variety of backgrounds and experiences. And once again, I'm going to direct you to the event website for their full biographies. But in short, please join me in welcoming Carrie Cordero, who is the Senior Fellow with the Center for New American Security, CNAS, Daniel Kahn Gillmor the Senior Staff Technologist at the American Civil Liberties Union, or ACLU, Bedavyasa Mohanty, Public Policy Manager at WhatsApp, and Riana Pfefferkorn, research scholar at the Stanford Internet Observatory.

[00:00:35.55] Welcome to all four of you. Thank you so much for joining us here. Good to see you all, faces at the back of the screen so if I'm looking kind of weirdly askew it's because you're over here and the cameras over here so apologies in advance if I'm not making eye contact with you because I'm looking at you.

[00:00:55.00] So I want to dive straight into the conversation. Riana, I think I'm going to start with you actually and ask what are, in your mind, the major milestones in this encryption debate that you would point to? I know Matt mentioned some of these earlier, but he talked about three crypto wars and really only dug deeply into one.

[00:01:17.04] RIANA PFEFFERKORN: Yeah, I was happy to hear Matt's keynote because it did a lot of the work for me at least insofar as the '90s are concerned. Arguably, that was kind of crypto war two. We could take this back further to the 1970s when professors at Stanford, which Diffie and Martin Hellman together with several of their grad students, including Ralph Merkle independently developed the concepts underpinning public key cryptography something that had been known to the US government and I think also to the British government since World War II but which was highly classified at the time.

[00:02:02.49] Because the Stanford group came up with the same ideas based entirely on unclassified information, you might think that that would have put them in the clear, but nevertheless, the NSA threatened to stick them in prison if they were to go forward with publishing their papers and presenting their landmark new directions in cryptography paper at a symposium that took place in Cornell in 1977.

[00:02:28.59] Ultimately, freedom of information, and knowledge, and academic freedom carried the day, and I'm informed that the vise admiral and director of the NSA who had threatened Professor Hellman is now friends with him later on, that they were able to get past their differences. But that was sort of the first place where it suddenly became clear to the US government that their secrets were no longer solely theirs, and that the development of commercial computers and commercial computing networks, and the invention of the internet were soon going to necessitate the use of cryptography that was not solely controlled by and developed by the government.

[00:03:12.09] All of this is recounted in a story piece called "Keeping Secrets" written for Stanford Magazine by a then grad student named Henry Corrigan Gibbs who's a cryptographer now, which is included in the encryption compendium, which you can look up there.

[00:03:28.75] After that, we heard the entire saga of the '90s, including both the clipper chip and the relaxation of export controls at the end of the 1990s that previously had classified encryption as a munition like bomb making parts, instead classified it under commerce department rules instead. There are still crypto export controls in place, but it is not merely the sort of situation that we faced in the '90s.

[00:03:51.78] We had sort of a quieter period after that for a while. Every so often, the FBI would float a trial balloon about trying to expand the federal laws on the books to include a mandate to add an

encryption backdoor, a work I'm sure we'll talk about repeatedly during this hour to devices or to communications services, and those didn't go anywhere.

[00:04:14.82] And I would say that this whole debate kind of came roaring back when Apple announced that they were going to roll out iOS eight in the fall of 2014, which removed the ability for Apple to unlock encrypted iPhones so device cryptography for law enforcement, something that they had previously been able and willing to do. And Android soon followed suit.

[00:04:40.17] On the communications encryption side, we saw the rollout of Let's Encrypt, which provides a free service for encrypting web traffic around 2015 to 2016 in stages, and now we are in a place where the majority of web traffic is encrypted, something that was not the case a decade ago. In addition, when WhatsApp rolled out the signal protocol in WhatsApp in April of 2016, that turned on end to end encryption by default for a billion people, something that has now grown to I think two billion people, something that I'm sure Beda can correct me on if that's wrong.

[00:05:17.55] And simultaneously in there you also had the San Bernardino dispute between Apple and the FBI happening in early 2016 again on the device encryption side. Simultaneously, we were seeing some laws start to get passed in other countries, even though the United States never got as far as-- knock wood-- so far gotten as far as passing laws that would regulate encryption and require law enforcement access to it to the same degree that the UK did with the so-called snoopers charter in 2016, in which Australia later did with the Assistance and Access Act in 2018.

[00:05:51.51] So we've seen some more action on the international stage in terms of passing laws, although we did have a couple of laws proposed here in the United States last summer that would have severely restricted the ability to offer what I would call strong encryption, the encryption that has not been intentionally weakened at the behest of any government in 2020 so far. Hopefully we won't see those come back, much less get past.

[00:06:17.74] Professor Blaze mentioned in his keynote that there has been this speed up in things happening in the crypto debates. And I'm glad he said that because when I was thinking through where the history of these debates were, you have the 1940s and World War II and stuff happening that it was classified, and you have the 1970s, and then you have 1990s, and it really felt like there's a lot more going on. I wasn't sure if that was just recency bias or because I have only been studying this area since 2015, or whether it really was that things were just speeding up.

[00:06:47.53] And Professor Blaze gives me some reassurance that it is, in fact, the case that things are just happening much faster now, and with perhaps greater ramifications for a greater number of people worldwide now than they used to back when we were just talking about the 1970s when the military and some banks were using cryptography, and that was the only customers for this technology.

[00:07:14.38] But I've rambled on so I'll pause there, and let's move on.

[00:07:19.88] Amie Stepanovich: Good. Did anybody else want to add any key milestones that you think are important to put on the timeline if we're like mapping out a timeline here? Anything else that we should be pinning on? Daniel, I see you kind of starting to speak.

[00:07:33.57] DANIEL KAHN GILLMOR: Yeah. Thanks for the overview, Riana. It's a great view of it. One thing that I want to just point out is that when we think about a timeline, we're often looking at sort of points, like this event happened here, but many of the points where policy decisions were made or things were changed actually have effects that ripple much, much longer.

[00:07:54.09] And I think Matt did a good job of pointing that out in his description of what would have happened had the clipper chip succeeded, but this is something that we continually see as policy decisions that were made like the export controls regime, which ended more or less in 2000. The stuff

pre-2000 was continuing to have an effect on the security of our communications all the way up through, I mean, 2015 was when the logjam attacks were published, which relied basically on this legacy set of crypto that everybody knew at the time was bad that continued to be present and deployed.

[00:08:33.54] We're just not very good at fixing mistakes that we've made in prompt order. So I think when we're thinking about a timeline, we really should be thinking about these bars of something can still have like an effect many, many years down the line. And I think that's a pattern that I'm going to point out repeatedly over the course of this conversation I think. I just wanted to flag that for folks. When you hear such and such thing happened, think also about what the long term effects are.

[00:09:01.43] Amie Stepanovich: Thank you so much. Maybe I'll turn to Carrie and ask, now that we've kind of laid out several-- I don't want to keep using the word milestone but I can't think of a synonym immediately. Maybe just talk about how with each big event we're seeing an evolution in thinking both on the pro strong encryption side as well as the people who are thinking we are going dark and we need more law enforcement tools available to us.

[00:09:36.79] CARRIE CORDERO: Sure. Thanks, Amy, and thanks for the invitation to join the conversation. It's nice to be with all of you all virtually. So I want to focus most of what I'm about to say on the law enforcement and the national security perspective of these issues.

[00:09:58.82] But first, just in terms of to pick up from Riana's comments in terms of the timeline, I think one additional benchmark that we might want to put in is not so much a technological benchmark, which I think Professor Blaze's remarks were mostly focused on the technology of it, but if we want to look at legal benchmarks, 1994's CALEA, the statute that mandated telecommunications providers at the time to cooperate with law enforcement through a legal framework has been a law that sort of permeates this entire conversation.

[00:10:44.35] Because as the technology has changed and things have moved over to internet service providers and all sorts of other technology platforms, CALEA was never updated in the same way as the technology had moved. And so I think in terms of there having been in 1994 a congressional determination to provide a statutory framework for companies to respond to a lawful request from the lawful demand from the government, in terms of a court approved warrant or other court order, that has been a piece of the conversation that is out there. So I would sort of put that into the timeline too, CALEA.

[00:11:31.32] So to focus for a minute on the law enforcement and national security equities and that part of the conversation, because that's sort of where my background and experience comes from, I went back, and I want to focus kind of on the last 10 years or so. Because I think there has been a shift in law enforcement and national security community and leaders participation in the encryption debate. So if I go back, I'm going to offer three thoughts.

[00:12:05.71] One is, what's changed in the last 10 years? Second is, are there some fissures between the law enforcement and the national security side? And to get to the too long, don't read, I think that there are some fissures there. And then three, where does that leave us in terms of a potential legislative debate?

[00:12:27.06] So first, if we look back 10 years ago or so, at that time, the FBI was primarily concerned about technological changes regarding real time interception. In other words, surveillance of communications that were happening in real time. Over the course of the decade, that conversation has shifted significantly to the FBI'S interest in accessing data that is stored on the bytes. So a shift in the conversation from law enforcement perspective from the ability to intercept real time communications to an equally, if not more significant, interest in being able to access stored devices.

[00:13:08.64] A second sort of look back to about 10 years ago is around that time, 2011, the then FBI general counsel was testifying in front of Congress on this issue of what the FBI has often described as the going dark issue. More recently, they've adopted language that talks about lawful access, and I've noticed a real change in terms of how law enforcement talks about this debate, which is lawful access as opposed to using the going dark framing, which they used for a lot of years.

[00:13:39.34] So about a decade ago, the FBI general counsel said that from the FBI'S perspective, changes to encryption technology were not what the FBI was looking for. I think that too has changed over the course of the decade where in more recent years, more recent including the current and the past FBI director, the last FBI director before Director Wray, they both did talk about the ability to have a technological solution, a technological fix for being able to facilitate companies providing the contents of encrypted materials to law enforcement pursuant to a lawful request.

[00:14:23.28] And then the third thing if we look back a decade ago is at that time, the FBI general counsel again was testifying to Congress that the FBI viewed its legal authorities as sufficient. And in that circumstance, I think that probably is sort of still true from the perspective of I don't see the Justice Department clamoring as a policy matter for new legislative authorities, and there continues to be more of a request for working with the private sector and the technology sector to be able to come up with a technological solution that enables companies to be able to respond to a lawful request from information.

[00:15:10.17] And I'm going to wrap up my-- I'll pause here in a minute so others can jump into the conversation, but I would just say that from a law enforcement perspective, the fundamental premise of all of law enforcement's arguments in the encryption debate rests on the notion that it is a legitimate government and public interest for entities to comply with court orders, that we do have legal frameworks that allow for people to produce information pursuant to a lawful request. And that really undergirds the entire law enforcement perspective on that.

[00:15:52.47] So maybe I'll pause, and then later in the conversation I'll come back to what I see as some differences between the national security community and the law enforcement community.

[00:16:04.86] Amie Stepanovich: Wonderful and I'm going to take a pause myself to say it's never too early to put questions in the Q&A if you're watching virtually, but I'm going to keep going with our conversation and open it up to the rest of you. Do you have anything to add before I go with my questions to what Carrie laid out on kind of evolutions and thinking across the different big events that have happened across the different evolutions of the encryption conversation? And Beda, maybe I'll turn to you

[00:16:40.37] To see if maybe you want to provide some international perspective for how these debates are not only happening here in the US, but elsewhere, and the extent those conversations might be also impacting coming back into what is happening in the US as well as vise versa, how what's happening here might be impacted with what's happening elsewhere. We've already had Riana mention UK and Australia, but I know for a fact those aren't the only two countries where these debates are taking place.

[00:17:10.10] BEDAVYASA MOHANTY: Thanks, Amy. So happy to be here, and thank you for convening this important conversation. Earlier Riana mentioned how it appears like when it comes to encryption policy that just seems like so many things are happening right now. And I do think that the primary reason behind that is because so many people care about these issues. They're affected by these issues today.

[00:17:37.14] Through the global pandemic and lockdown, end to end encryption is what has protected most people's personal conversations when it has been impossible to come together in person. And encryption is now the way that most messages are sent globally. Just to give a sense of things of the scale at WhatsApp, during the past two years, we have seen a huge growth in our usage. We now deliver more

than 100 billion messages and one billion calls every day, all of which are protected by end-to-end encryption.

[00:18:12.59] And behind these numbers, the examples that we see of the use, we see some really sensitive use cases. Doctors, lawyers, mental health counselors, businesses, courts, and government entities all around the world are using WhatsApp more than ever to communicate privately. All of this means that the stakes for encryption have never been higher, and the threats to encryption have never been as widespread or serious as they are now.

[00:18:47.99] And I think the encryption compendium is a super important organic resource that is very useful in informing the debates that will come from here on out. And primarily, because these conversations are no longer localized just to the US or to the five [INAUDIBLE] countries for that matter, some of the strongest challenges that we're seeing to encryption are coming from places like India, and Brazil, and the EU.

[00:19:18.45] And the pressures on encryption are no longer restricted to just demands for backdoors alone. We are continuing to see the more familiar exceptional access proposals. We talked about the UK and Australia, and both of them have laws in the books that give the government the authority to mandate companies to alter their systems to enable access to encrypted content.

[00:19:45.19] Earlier this year, Germany came very close to passing a law that would have imposed an obligation on encryption service providers to assist in the hacking of their users' communication. And right now, Belgium is actively considering a data retention law that would require the operator of encrypted systems to be able to turn off encryption only for certain users.

[00:20:12.58] Now while this is super concerning, equally concerning is the emergence of I think two other types of anti-encryption laws and regulations that we've seen come up around the world. And the first are the kinds that impose a duty of care or a liability on encrypted service providers that practically has the effect of breaking encryption. And this liability often rests on encrypted platforms being able to prevent harm that may occur on their platforms, and we saw this in the US with the discussion around the [INAUDIBLE]

[00:20:54.10] The second category of law is one that we are very concerned with that we spend a lot of our time trying to understand and argue against. Of the laws that don't directly seek to break encryption, but propose a technical solution that has the same effect, and we have seen this happen in India with the introduction of the traceability mandate within the IT rules, which WhatsApp has now challenged before the New Delhi High Court. But we've also seen this in the debate around traceability in the Brazilian Congress over the past year.

[00:21:27.80] And what traceability does is it requires private messaging services like WhatsApp to keep track of who sent what and who shared what for billions of messages every day. That goes against the guarantees of end to end encryption. We have also seen an increasing push for client side scanning to scan the content of people's messages, to detect, block, and report illegal or harmful content like child sexual abuse material. The European Commission's DG HOME, for example is currently drafting child safety legislation that may mandate content scanning even for end to end encrypted services. And the draft UK online safety bill contemplates giving the regulator the power to mandate content scanning.

[00:22:14.66] Now all of these taken together are very concerning developments, and it's important for those of us that care deeply about encryption and the ability of people to communicate privately and securely to be vocal about the problems that these sorts of laws and regulations pose. At WhatsApp, we feel an immense sense of responsibility for the more than two billion users that rely on our service every day to stay in touch with their friends and their loved ones. And we believe we can provide both the

privacy and safety in an encrypted environment. And for that, we will continue to speak out against the laws and regulations that threaten encryption.

[00:22:56.75] I'll pause there, but happy to circle back and talk about any of this later in the conversation.

[00:23:04.00] Amie Stepanovich: Anything to add?

[00:23:05.23] DANIEL KAHN GILLMOR: If I could jump in, I appreciate the framing that you did there, Beda, because I think the question at it's core here, I know this event is about the crypto wars, but the real question that we are all grappling with is a question about communications, about control over security communications, right? And we've seen a number of proposals, some of which you mentioned, a number of others that you didn't mention that they claim to not touch the encryption, but actually subvert the underlying goals.

[00:23:38.14] And speaking as a civil liberties and civil rights advocate, this is one of the main concerns that we have. These tools are in place, and people care about these tools not because they care about the mathematics, although some of us care about the mathematics because they're pretty neat, but they're in place because people care about the ability to communicate privately. They care about the ability to store information privately. In the past, your communications were private by default because you would have a communication with someone in a crowded restaurant that nobody could hear what you were saying or you could have your conversation at home and there would be no speaker listening in.

[00:24:17.86] And that has shifted as more and more of our interhuman communications are mediated by these devices. The devices themselves represent a vulnerability and a chance to leak information. Private communication is really important for the social fabric, for people to be able to develop intimate relationships. And so I think that's really at the core of what these debates are about.

[00:24:41.56] And we say, you know, we've been talking here about encryption. I'll point out that there are other technical mechanisms that are in place that are part of those guarantees, those information security guarantees that people care about, whether they care about them by the name information security guarantee or not. Cryptographic authentication is another critical part of those pieces, and some of the proposals that we've seen weaken authentication steps.

[00:25:03.62] If I'm having an encrypted communication to you, Amy, but I can't tell that it's actually you on the other side, then the fact that the channel is encrypted doesn't actually save me much. I could be talking to someone else. So there's a range of mathematical structures and programmatic techniques that we talk about here, but what's really at the underlying core is this question of, can we actually be private individuals? Can we form private relationships? Can we remember things without having those memories vulnerable to extraction by someone who we may or may not trust?

[00:25:41.22] Amie Stepanovich: Thanks for that. I've appreciated kind of the depth of nuance that you've all brought to this conversation so far because I think oftentimes when we talk about encryption, because it's so deeply technical and because people, especially in broader audiences, don't get into the math necessarily, we use shorthand. And we use shorthand because it's accepted, and most people kind of understand what we're talking about when we use things like backdoors or exceptional access. And those words do mean something, but they can mean a lot of things, and different things in different audiences.

[00:26:23.52] And Carrie, I actually appreciated something that you said earlier, and I'm going to turn to you at this question first I think because you referenced that there might be a divergence between specifically the national security side and maybe the law enforcement side of the communities. And those sides might not always agree, and I think that that oftentimes in the simplified approach, places get grouped together. And even I oversimplified it earlier. It made me uncomfortable when I said it. I said the pro encryption side and the side that might be saying that we are going dark.

[00:27:00.24] And we do. We kind of lump them into two camps, and we say these are the two sides, but can we get a little bit into the nuance about what are the interest groups coming at this debate, what are their interests that are at play, and what is the nuance kind of behind the arguments, and the different sides?

[00:27:22.77] CARRIE CORDERO: Sure. Thanks, Amy. Yeah. So this is an observation that I've had for the last several years at least I think. The last five or six years is what I describe as somewhat of a fissure I think between the national security community's perspective. So if you think about what you might hear from an NSA director or a former NSA, National Security Agency, director versus what you might hear from testimony from an FBI director who wears two hats himself, a national security hat and a law enforcement hat. Or what you might hear from a DA, a district attorney, who's responsible for prosecuting cases.

[00:28:06.17] So here's what I think the difference is as it has evolved over the last maybe five or six years or so. I think the national security community and national security leadership has the more probably nuanced view because they are looking at things significantly from a cybersecurity perspective.

[00:28:32.71] So in other words, from an ability to protect classified information, from an ability to protect the national security information they collect, the tools that they use, all of these things. They have a really deep appreciation for the value that encryption provides as a security feature. So if I put it sort of on the positive side from the national Security community.

[00:29:03.91] So that is why I think we have not seen national security community or intelligence community leaders be on the front, public facing lines of the government's going dark or lawful access conversation. I also think-- this is really just sort of my hypothesis-- that the national security community is also very confident in their own abilities so that if there were a national security need to be able to get information, they're pretty confident in their abilities to be able to do so in a national security matter.

[00:29:47.64] Law enforcement, pure law enforcement on the other hand, is in a different circumstance. Because law enforcement is looking at cases like child exploitation, child pornography cases, which are just absolutely-- there is just a huge amount of that volume of criminal activity that affects American families and families all around the world with vulnerable victims, worst kind of possible crime, and that is an area where law enforcement has a really compelling case to make, and a compelling need for information, including stored communications, to be able to solve cases.

[00:30:37.51] And so that's why I think we've seen the FBI directors in particular across administration. So this is not a partisan thing at all. We've seen consistently FBI directors and FBI general counsels over the last 10 years be the ones out front making this argument for why person went to a court order, search warrant, et cetera. The law enforcement needs to be able to have access to information, and so they have been the ones pushing for some sort of technological solution to be able to have companies be able to provide the communications or the content of information to law enforcement to be able to solve those kinds of crimes.

[00:31:20.86] So I'll pause there, but that's where I see that there is some modest, but a little bit of a divergence between the way that we see the law enforcement community express its views on this issue. Also, at the state and local level, they don't have the resources of a National Security Agency, they don't have the technological capabilities of a National Security Agency, or another element of the intelligence community. And so this becomes more of a really day to day law enforcement challenge.

[00:31:57.94] And just one last point on that, as a practical matter, one of the things that has changed the most in the last five years has been the massive deployment of encryption technology for everyday users. I'm over 10 years out of government, and when I was in government handling surveillance matters for the government, this wasn't an issue. It was an issue that the FBI was working as a policy matter, and there were working groups of people who were working on the going dark issue, but as a practical matter,

everyday people, all of us weren't necessarily using WhatsApp or other encrypted devices to talk with our friends, to talk with our colleagues as a matter of just basic personal cybersecurity hygiene, which we do today.

[00:32:51.82] Amie Stepanovich: I can open that up to the rest of you. Yeah, go ahead, Daniel.

[00:32:55.33] DANIEL KAHN GILLMOR: Yeah. So thanks, Carrie. Those distinctions is really an interesting point, and I think it also ties together with the CALEA point that you made earlier, right? That CALEA was a directive for the assistance of law enforcement. And CALEA actually changed the way our telecommunications infrastructure was implemented because it said telecom providers need to be able to provide lawful access. And so you need to build in lawful access intercept facilities in your telephone switches, right?

[00:33:32.16] And the impact that CALEA had, among other things, was that devices that the telcos bought all had this sort of thing baked in. The government basically said you have to put these features in, and those are sold all over the world, not just within the US.

[00:33:52.29] In 2005, a telephony switch that had these lawful intercept functions in it was actually compromised. We still don't officially know who compromised it in Greece, and actually the phones of at least 100 high level Greek officials, including the prime minister, were tapped. We don't know by who. So there were national security implications in this compromise that had been made for law enforcement. Even outside the context of the US, the fact that CALEA was pushing these products to have these lawful intercept functionalities meant that it could be taken over and used.

[00:34:32.67] That whole affair actually ended in the death apparently by suicide of one of the engineers in Greece, one of the telco engineers in Greece. But I think it's really worth thinking about how a goal that comes from one side, even in this law enforcement versus national security split, might end up having really potentially serious blowback in other sides.

[00:35:00.74] RIANA PFEFFERKORN: I'd also like to maybe add in there that when we talk about-- Amy, I agree with you that when we talk about the government as one unified force that doesn't highlight the divisions and differing interests and equities in national security and law enforcement that Carrie was highlighting. But in addition to that, I would say that there is at least a third portion of government that has interest in equities here, which is the consumer protection portion of government, which is looking to the companies that are getting leaned on in a lot of cases by law enforcement to make their users data more accessible to instead try and protect that.

[00:35:39.36] So companies are being pulled in multiple directions. On the one hand, they're producing consumer off the shelf hardware and software products and services that everybody uses that may need some sort of tweaks or modifications to be used within government or military context, for example. And so maybe on a national security standpoint, it's better if they keep their stuff patched up.

[00:35:59.63] On the other hand, they may have law enforcement saying we need to have some way of expeditiously accessing information without having to go through the third party vendors that have cropped up as a cottage industry, such as Cellebrite and Grayshift, which is now in the hands of thousands of law enforcement agencies.

[00:36:17.27] Amie Stepanovich: Riana, can you say a word about what Cellebrite and Grayshift are?

[00:36:20.03] RIANA PFEFFERKORN: Yeah, sure. So one of the other things I neglected to mention when sort of talking about what has shifted the encryption debate, it's been kind of responsive both to technological developments, to political developments such as the San Bernardino shooting, but those technological developments haven't only been on the defense side. If we view Apple, and Google, and so forth, and WhatsApp as the defenders of protecting information security, it's also been on the

offensive side insofar as Cellebrite, which is an Israeli company, and Grayshift, which is a US based company founded by, I believe, a former Apple engineer, provide devices that are able to do basically digital forensics that exploit flaws that exist.

[00:37:02.96] Inevitably, in any software product there's always going to be bugs that are able to exploit vulnerabilities in order to get access to and extract information from encrypted devices for the use of law enforcement. And so those are sold to law enforcement agencies around the country. We know this because of a report that was put out about a year ago by a group in DC called Upturn that used freedom of information requests and very diligently built up the ability to get back information about the number of police departments around the country that have one of these devices, which is a way of making up for what Carrie mentioned, the differing budgets that state, local, and tribal agencies may have vis-a-vis the government.

[00:37:45.59] The federal government law enforcement agencies also have cooperation agreements with local, state, and tribal governments through various national regional forensics labs that are scattered around the country to provide unlocking capabilities and other technical assistance to the state and locals using sometimes these third party tools, and sometimes the things that the FBI can develop in-house since they have significant in-house capabilities for developing exploit and that will take advantage of the vulnerabilities that occur in these things.

[00:38:19.86] So we see this cat and mouse game where there's the development of technologies to circumvent the technologies that had been put in place to protect information. And one of the problems that has grown up around this sort of cottage industry is that they aren't just selling to us as the good guys, and we can talk about when the good guys aren't so good.

[00:38:39.65] They're also selling to a less rule of law respecting, human rights respecting governments around the world. And so we have this additional issue where we have third party companies that sell, such as the NSO group that sell their wares both to let's assume agencies operating on a good faith basis in the United States but also to repressive governments in places like the United Arab Emirates and Saudi Arabia, which brings a bone saw to meetings.

[00:39:11.87] And so those are some highlights. I think what I'm trying to get at, going back to my statement about consumer protection, which is that there are also agencies within government that are concerned with protecting the data security, and the privacy of users. There is the State Department that is concerned with protecting the human rights and Democratic interests around the world. And those are all working in tension with law enforcement here, law enforcement abroad who may not always have laws that we would consider legitimate under our Democratic regime, and national security and intelligence agencies that spy on each other as kind of an accepted means of doing business.

[00:39:51.05] But that nevertheless means that those agencies have dual offensive and defensive equities that they are trying to bring to bear in an environment where it is now largely the private sector that is developing and commercializing these technologies for everybody to use instead of them being, as mentioned, solely in the hands of government.

[00:40:11.51] BEDAVYASA MOHANTY: Going back for a second to your original point, the question, Amy, about what is the driving force behind some of these laws and regulations. And outside of the national security, and access to information, there is also the safety considerations that have been driving many of these policies. And I think underlying this entire conversation is the fact that end to end encryption is a technical concept that is often used in the policy conversation.

[00:40:44.81] And the way it's used is to position it as something that completely obscures information and content and therefore robs anyone of the ability to address any of the concerns that are raised, be it

concerns like terrorism, child exploitation, and so on. And in this binary, often the nuance that's lost is the fact that despite end to end encryption, there are ways of keeping people safe.

[00:41:17.78] There are ways of addressing many of the concerns that drive these conversations and discussions. And the fact that you could leverage metadata, you could leverage user reports to tackle some of the kind of abuse that's the driving force behind these legislations, that's often lost in the conversation around national security, and the lack of access to information.

[00:41:46.79] Amie Stepanovich: So we talked we talked a little bit about the nuance in government perspectives. In preparing for this, one of the things I did was look back through years of my own engagement on this issue, and things that I have come across. And one thing I came across was this history news items related to Symphony, which was a application used by the banking sector, which is very tightly regulated, where they consented to essentially-- again, I'm going to use very simplified terms here-- have a wire tappable system for communication so that if they needed to be investigated under one of the many banking regulations, that those investigations were able to take place.

[00:42:42.89] And the system was often pointed to as look, it's workable within the sector. Why can't we have this in other sectors? So can any of you speak to-- I think that the same nuance from consumer protection to national security to law enforcement within government, do we see similar breakdowns just within the commercial sector where maybe not all sides necessarily agree on the same thing in that side as well? Stumped you all.

[00:43:19.29] DANIEL KAHN GILLMOR: I mean, I think we do, right? Because of the different private agencies, private groups have different incentives in terms of dealing with other people's data. We live in the cloud era where everyone's information is at some level stewarded by a number of other private organizations. If you have a Gmail account, Google has access to your email. If you are communicating via WhatsApp, Facebook has access to the metadata at least of who you talk to, right?

[00:43:54.45] And different groups have different expectations about what they can get. If they're profit driven, what their bottom line is on the information that they have that they are effectively acting as a steward for. So you can see a different set of equities there. If WhatsApp's goal is to connect people to each other, and their goal is not to say mine the content of their communication, then WhatsApp has rightly the goal of acting as a better steward of the content of people's communication. There's no advantage to them to get information out of the content. Therefore, it's better for their users to give them stronger protections.

[00:44:37.49] And I think we do see some differences there among different private groups because some of them see their advantages as being the more information that they have about their user base the better that is. Those are difficult tradeoffs, but I definitely think you can see a spectrum across the different range of companies that offer information services.

[00:45:05.31] RIANA PFEFFERKORN: I think just going up one level too, there's a difference between Symphony and WhatsApp, and the difference is who the target audience is. You've pointed out, Amy, another equity that can get involved here when we talk about the interest at stake here, which is sunshine and oversight. And there are pretty good reasons for deciding that if you work in a heavily regulated industry such as banking, given the risks of insider trading and, price fixing, and manipulation, and so forth, of course, there are reasons to decide that within that context the public interest favors having greater oversight that includes keeping a log of people's chat messages.

[00:45:45.84] It's amazing how many SEC and FINRA enforcement actions get brought against people who are still doing crimes over those exact same channels. But I think it is a folly and a fallacy to equate that to private communications between private individuals talking privately. It's as though you were to say, well, because we have sunshine laws to require open meetings among government and to have their

notes be FOIA-able, we should do the same for me having dinner with my husband at home. There's simply not the same context.

[00:46:23.79] And it is actually a terrifying proposal to say that everybody's private communications and thoughts need to have the same level of oversight, surveillance, and log ability as those who willingly enter employment in a heavily regulated sector. So I never found the Symphony analogy to be particularly persuasive, and really just the opposite for what it was implying.

[00:46:54.65] Amie Stepanovich: Carrie, did I also see you go off mute? I didn't want to talk over you.

[00:46:58.72] CARRIE CORDERO: No, that's OK.

[00:46:59.52] Amie Stepanovich: [LAUGH] I didn't want to talk over you.

[00:47:02.56] CARRIE CORDERO: That's OK. I was just going to maybe put a little bit of a sharper point on part of what Daniel was describing a minute ago, which is that amongst the technology company landscape in the United States and around the world, companies monetize their users information differently.

[00:47:29.81] And so to say that in super plain language, different companies use our information to make money in different ways. And some companies put a premium on being able to provide services that provide a higher degree of privacy, and others use our information in a much more aggressive way in order for that company to make more money.

[00:47:56.00] So I just wanted to sort of sharpen that a little bit because I think there definitely are differences amongst the companies that operate in this space. Just to shift gears a little bit, I think one of the challenges for law enforcement in this debate has been the persuasiveness of the information that law enforcement has brought to the table.

[00:48:22.52] So when different law enforcement leaders over time have been trying to drive a conversation around why they need not access to Riana's private conversations about dinner, but why they need lawful access to communications between the individuals who were plotting the Jan 6 insurrection has been that-- which director Wray testified about earlier this year-- has been that the FBI in the past has been able to-- or Justice Department has been able to provide sort of individual case examples, but they really haven't had the data-- at least that I've seen as I from time to time participate in these conversations with you, Amy, over the years-- they haven't really brought to the table sort of persuasive, comprehensive data for how big a problem it is.

[00:49:22.57] In fact, about three years ago, The Washington Post had reported that data that the FBI director and Justice Department leaders had been using in all sorts of public statements and speeches regarding the number of phones that they had been provided by law enforcement agencies to try to crack, to use a lay term, that the stats they were using were totally wrong. And it was because of a mistake that was made. It wasn't sort of deliberate malfeasance, but it was a mistake that was made. And so the statistics that they were providing, leaders in the Justice Department were providing routinely in public statements were wrong.

[00:50:03.86] And so this is an observation that I've been making, and writing, and speaking for years on this is that there just has not been persuasive enough data to drive the conversation beyond where it's been. So from a law enforcement perspective, we can say this is a problem for investigators conducting child exploitation cases.

[00:50:32.32] But the talking point almost ends there. I mean, sometimes it can get to the point of and it's been this many phones, but that even doesn't really make the persuasive case. So what I for a long time have wished that we would see from the law enforcement community is better data, more persuasive

data, research based data that really supports the arguments for why this is a major public safety problem.

[00:51:04.50] Amie Stepanovich: So before we turn over to some student questions we have in the room and starting to look at the Q&A, we have a question already, and this is your moment, folks, if you want to add questions into the Q&A. One last thing because we are here to talk in part at least about the encryption compendium, to ask you all as we look at this as a resource, how would you see something like this being useful in your work, useful to other folks, or being useful in the future? What would be a good way, a good direction to take it moving forward for folks who might become the next generation of experts on encryption policy?

[00:51:55.36] DANIEL KAHN GILLMOR: I can say I appreciate the compendium synthesis of legal material with policy documents, with regulatory documents, with academic and cryptographic work. I think it's important to see those all as pieces of a larger, overarching situation. As Matt Blaze pointed out at the beginning, he sort of broke out two initial questions that we were worried about with the clipper chip, which was can we trust the folks who want this access, and will the system even work.

[00:52:30.64] And then he had this third point, which was, if it works, what are the knock on consequences even if it did work. And those all require different types of expertise to really grapple with, and they're all tightly intertwined. You can't answer one question without another if you really want to think about what the effects are going to be on society as a whole.

[00:52:50.66] So I appreciate that the compendium, as it stands, is incorporating works from these different disciplines. I think I would love to see more specific case studies that include a little bit more technical detail, and this may be my bias. As someone who is a technologist and not a lawyer, I really appreciate having the legal and regulatory frameworks in there, but there are really interesting case studies of particular types of technological change that were proposed as a fix or sneakily snuck into the public.

[00:53:23.18] For example, the random number generator debacle where we believe the NSA injected into national standards that weakened cryptography for those people who used it. I think those examples where you see a technical change interacting with a policy change interacting with a policy goal or regulatory frameworks really will help to see the through lines over the decades that we've been having these conversations.

[00:53:53.91] BEDAVYASA MOHANTY: To me, I think the compendium is super useful in its comprehensiveness of just the amount of information it has about the debates as and when they happen. Something that we see in the encryption debates over the years is that every two or three years there is a rediscovery of fire. Everyone feels like they have finally chanced upon the solution, the proposal that will finally be able to give you privacy and be able to access funding and so on.

[00:54:26.01] And like Daniel mentioned in the beginning of this conversation, a lot of these conversations proposals don't go anywhere, don't become codified into law, but still tend to affect the conversations that come subsequently after them. So what I think the compendium could do going forward is clubbing together some of these diverse proposals that have unique names like ghost proposal or something else, but are essentially rehashed and repackaged same ideas that have been debunked, challenged, and litigated for years on end by the civil society community, by the technical community, and so on. So that in every subsequent conversation where these ideas are brought to light, the precedent is well established that yes, it was proposed. Yes, it has been countered. No, it will not be effective.

[00:55:26.93] Amie Stepanovich: We have two student questions. I'm going to invite them up in turn and then depart the podium so they have lots of space to come up and ask. And I believe the first one is Caden Daily, if you want to come up.

[00:55:54.73] CADEN DAILY: Can everybody hear me OK? Awesome. So I've heard quite a few times over this that there has been people alluding to potential reconciliation or anything like that. I'm wondering if the evolution in thinking from the '70s to now or the '90s to now has kind of helped move towards a reconciliation, or kind of like one of you just said, how the conversations don't really go anywhere if the evolution is causing people to kind of dig into their respective positions more so, and not want to compromise.

[00:56:49.06] RIANA PFEFFERKORN: I think it moves. I think the debate moves, but doesn't ever come to an end. And so what the locus is of the discussion may shift. So it may shift from devices to messaging, for example, and it may shift from the law enforcement contending that they have no access and that's the problem to they can't get access quickly enough. If they grind on it, they can eventually unlock phones or they have outside vendors. And so the point there has shifted to well, we want to be able to get it faster. But it doesn't come to an end.

[00:57:25.09] I find that frustrating because in the meantime, the technology keeps progressing and keeps becoming more and more ubiquitous. And it seems like it would be advantageous if we could all just accept that strong encryption and end to end encryption are here to stay and we need to live in that world rather than trying to roll it back. But I think that it will be difficult to find that. Because if this were an easy problem, we would have solved it already at some point in the last 30 years. So I don't necessarily see this ever actually just finally being put to bed.

[00:58:02.14] CADEN DAILY: Thank you very much.

[00:58:05.27] DANIEL KAHN GILLMOR: I mean, Riana, I think I would say in response to that there does seem to be a growing consensus that we can't stop the fact that there can be end to end encryption, right? That this sort of mathematics, there was an attempt decades ago to make it so that the mathematics wouldn't be widely known. Now they are known. And there isn't any rolling that back.

[00:58:28.85] And so in some sense, the debate has shifted to well, how can we cabin this thing that does exist and will exist indefinitely? And so I do think that there's been a bit of a shift in the debate where we are actually starting to have some of the debates about values instead of about capabilities. And I think it's important to recognize that there really are values at stake here. I'd like to think that we are moving in that direction, although I share your feeling that this conversation is like an undead conversation at some level.

[00:59:06.18] Amie Stepanovich: So I'm going to invite Jonathan Stokely up to ask our second question.

[00:59:18.89] JONATHAN STOKELY: Hello, my name is John Stokely. I'm a second year master's in business administration student, and I had a few different questions I'm wanting to ask related to data privacy, try and encrypt it, and then going to the other side of well, think about all this data that is encrypted potentially be used for research purposes.

[00:59:37.08] And then I was more curious, especially that I've been around quantum computing, and are we going to reach a point where encryption is even feasible if we have computers able to break it? So what are your thoughts on the latter. In terms of encryption, are we going to get to a point of sophistication where it doesn't matter, and no matter what data or how we try to encrypt it, somebody's always going to be able to unlock it?

[01:00:07.64] DANIEL KAHN GILLMOR: I can take a stab at answering that. I am not a formal theoretical cryptographer, but I've been following the quantum discussions. Quantum crypto will break many of the cryptosystems that we know about today, but let me just remind you, without quantum crypto, we can break many of the cryptosystems that were in use 30 years ago already. So there are new cryptosystems that are being put into place that appear to be resistant to quantum crypto, and that means that things

that use those new cryptosystems, if the theory is correct, will be protected when quantum cryptanalysis comes along.

[01:00:43.94] And this is not a new situation. We've seen this situation before. It does mean that old data that was stored and encrypted with systems that newer cryptanalysis can break will no longer be protected, but in many cases, information needs protection for confidentiality for a limited time frame. Nobody really cares what the secret business dealings were going on between two different banks 30 years ago right now. And 30 years from now, the stuff that's protected with info that will be breakable should quantum computers really come on the scene may have a similar lack of interest.

[01:01:22.13] So this is an ongoing technical work. Those of you who are there who are studying, I hope some of you will be looking into it and transitioning from one cryptographic regime to a new one, improving the strength as we go. We don't know how to do that. I work on internet standards and data storage standards, and it's very easy to see how some of those systems simply-- we don't know how to deprecate old, bad tools. But the technological changes work in both directions, both the cryptanalysis and the cryptography are continuing to level up.

[01:01:56.62] JONATHAN STOKELY: Thank you. Appreciate that.

[01:02:09.37] Amie Stepanovich: Trying to mouse over from one device to another device, and you can't cross devices like that. We have four questions in the Q&A, and I'm going to start with [INAUDIBLE], who's one of our students here at the University of Colorado, and ask, is there an intention to build regulation about the metadata that's collected by private companies and make it available to government agencies. The emphasis only on getting data content might be underplaying the extent of information that can be extracted from the metadata alone. So are we over relying on content? Metadata has so much to it. Beda, I see you're off mute.

[01:02:56.25] BEDAVYASA MOHANTY: Sure. I can start this up. I don't think there are efforts right now to directly start sharing the metadata that companies collect to governments, and I hope there isn't. That being said, I do think that metadata is significantly useful for preventing the kinds of abuse that is often of interest for law enforcement, and detecting and dealing with abuse.

[01:03:23.91] So I agree with the sentiment that there is an overreliance of content in these regulations, in these anti-encryption codes because there is so much that we can already do with metadata to prevent abuse, to tackle abuse [INAUDIBLE] on our systems. WhatsApp bans around 300,000 accounts each month for suspected sharing of child sexual abuse material. We made 400,000 reports to NEC/MEC about individuals that we suspect share child sexual abuse material.

[01:04:01.07] And all of this information, all of this dealing with abuse happens on the basis of information that's shared to us by users like user reports or from metadata like profile pictures, group profile pictures, group information, and so on. So there is a significant role that metadata has to play in dealing with abuse. So it is true that there is an overreliance on content in anti-encryption laws and regulations, but at the same time, I don't think there should be any requirement or cause for the direct sharing of metadata from the companies to the governments. I think that would be setting us back quite a bit.

[01:04:49.80] Amie Stepanovich: Another one we have, in the debate, we often hear these companies scan communications for malware anyway. What's the difference? Is there a technical difference between general monitoring of communications content for systems reasons versus monitoring content for illegal content, or is the difference between the acceptance of why?

[01:05:17.50] RIANA PFEFFERKORN: I think I can let others speak to whether there is a technical difference. I think certainly in terms of purpose there is a stark difference between monitoring somebody who's doing a virus scan or a malware scan for reasons that are intended to protect the user versus turning that system against the user to try and look for illegal content or simply disfavored content,

whether or not it is illegal. And I think that gets to some of the crux of a lot of the discussions around client side scanning and around scanning in the cloud for reason a versus for reason b.

[01:05:53.33] And so I think you'll have an easier time selling to people having a system that is solely trying to keep them from having their data security and privacy compromised as opposed to having their free expression and other privacy interests affected by the same system turned to a different purpose.

[01:06:19.22] DANIEL KAHN GILLMOR: I think Riana is really on point there, that the purpose is-- I mean, there are minor technical differences or maybe big technical differences, but really the purpose is the question. And I think another way of looking at that is to say, does your telecommunications equipment work for you or does it work for someone else?

[01:06:42.86] The devices that most people today carry around with them are very intimate devices. These are devices that know not only your location, and your interests, and your hobbies, and your relationships, they know just a tremendous amount about what you do. You offload your thoughts into them many times. And if that device, which is effectively being used as one of your main ways of interacting with the world, is not working for you, there's a real significant problem there. It means that people are sort of having parts of themselves co-opted to work against themselves.

[01:07:25.83] Amie Stepanovich: Beda, I saw you go off mute also. Do you want to add?

[01:07:28.92] BEDAVYASA MOHANTY: Sure. I think there's these two questions contained in this one, which is why the answer is yes and no. I think when it comes to monitoring for malware or the systems wide problems for scams, spam, and so on, I think there is a technical difference between what the company is observed. There the focus is on behavioral patterns that can help identify some kinds of abuse, and those are content independent. So I think there is a technical difference between that and the scanning of content.

[01:08:02.97] And the problem comes when we start talking about the scanning of content, and there Daniel was exactly right, there values come into play. What is it that you're scanning for? And what is that information that you provide to this company that you somewhat trust? Who is that company then working for? Are they doing it only to protect you, or are they doing it to potentially notify you to law enforcement and so on?

[01:08:34.87] And I think there the question, there I don't think there is a technical difference between scanning from one kind of content versus another kind of content, which is why these proposals are problematic because they might say that this is restricted to [? CSAM, ?] but there might not be any way of ensuring that the scanning is only meant for one kind of content and not any other kind of content that is decided by the company or the government.

[01:09:06.46] Amie Stepanovich: So John Callas asks, I'm curious about some of the debate about lawful access, and is there anything that a person can keep secret? Are there any limits on what a warrant can require to be produced? I've heard law enforcement people say there is not as a warrant is a requirement for them and they'll be punished by judges if they can't find things. Carrie, I think this goes to something you said earlier, if you want to start.

[01:09:30.53] CARRIE CORDERO: Sure. So warrants are issued by a judge based on facts that government investigators provide of evidence of criminal conduct. So if I keep it in the law enforcement side, set aside national security for a minute, just in the law enforcement conduct, if an investigator, a federal investigator, is going to a judge with a search warrant, they have to have facts that establish probable cause that a crime is being or is about to be committed.

[01:10:02.92] And then we get into the details of which crime is potentially being committed, and what the facts of the investigation have, but that is a fundamental premise of what law enforcement is trying to

communicate in this debate, which is that they are not interested in everyday people's communications or trying to get access to those communications. What they want to be able to do is solve crimes, disrupt criminal behavior, and bring individuals who are committing crimes to justice. And that is a fundamental premise of our civil society.

[01:10:40.21] So I'll pause there. I hope that answers the question in terms of yes, they're not interested in getting information about every individual person. What law enforcement is trying to do is focus their activities as it pertains to their mandate to solve crimes, to help victims, and prevent future activities.

[01:11:04.33] Then we can get into sort of the domestic terrorism and terrorism side of things, which on domestic terrorism, expands the law enforcement and national security side, and then there's international terrorism activities as well where, in addition to solving crimes and disrupting them, where the mandate for law enforcement agencies and national security agencies is to try to prevent the actual act of terrorism, whether it's domestic terrorism or international terrorism.

[01:11:33.07] But all of those, if the investigator is presenting evidence to a judge to get legal authority under a statutory framework that has been approved by Congress, is in the construct of a lawful demand for information that's premised on facts.

[01:11:55.76] DANIEL KAHN GILLMOR: So I feel like John's question might be more about what sort of limits would law enforcement be willing to accept on a scheme that would allow them to bypass some of the information security features that encrypt communications offer. And this does come up in past conversations that I've had where people are gaming out different technical proposals to provide encrypted communications that maybe provide some lawful access as well.

[01:12:27.83] Often the technical designers say, well, would you be willing to accept a situation that would only let you unlock 100 devices in the course of the year, or, as Riana mentioned earlier, would you be willing to accept it costing you four days to unlock a device instead of it being an instantaneous unlock? Or would you be willing to submit to a certain type of oversight regime, which requires that you list all of the devices that you've unlocked, maybe with some limited time delay.

[01:12:58.76] And I think this question about what limits would law enforcement be willing to accept in exchange for giving some ground on the cryptosystems, whether that's possible or not, is a really interesting one. Because my experience has been that every proposed limit, whether that's-- maybe the people on this call would disagree, but I'd like to think that we could all agree that a warrant for someone's thoughts would be considered out of bounds. That's a piece of content that I'd like to think we could all agree as a society are out of bounds for police access, regardless of whether there's a warrant or not.

[01:13:36.50] And maybe there are techniques that are out of bounds, right? We wouldn't say you can get a warrant to melt through the structural members of someone's house in order to find out whether they have marijuana inside. There are things that should be limits. And if we're talking about how can we deal with a cryptosystem in the context of law enforcement, there is an open question-- this goes back to the values point that we were talking about before-- of what limits would law enforcement be willing to accept in terms of things that they can access.

[01:14:12.62] In the past, they have not been able to access things. And I don't believe I've ever heard of any story of a law enforcement being punished by a judge because they were unable to reconstruct someone's conversation in a pub. Back before there were microphones in everyone's pocket in a pub, they simply got a warrant to go and ask people if they knew anything, and when people didn't know anything, that was it. It's not a failure to be unable to produce information from a warrant. So I think the idea that people have been punished is also an interesting question. I don't know what those punishments are.

[01:14:49.46] Amie Stepanovich: We could probably go on for another hour, but we are at time. Thank you all so much. I wish I could get more of your thoughts, but I appreciate you joining us. We're going to go into our last keynote. Thank you for your time. Thank you for your thoughts, and for taking time to share those thoughts with those of us in the room, those of us are joining virtually. I hope you'll tune in for the last keynote, and I look forward to continuing this conversation either online or in any other format. We shall continue discussing with everybody. Join me clapping in the room. We can still clap.

[01:15:27.59] [APPLAUSE]

[01:15:31.81] And we'll transition over.

Keynote, Erik Neuenschwander; Closing Remarks

https://www.youtube.com/watch?v=GEdqf7Iuyeo&list=PLTAvIPZGMUXP63tRcI-oBfVijnA2E1w0W&index=4

[00:00:00.90] Amie Stepanovich: As our last keynote, Erik Neuenschwander, who I'm welcoming to our virtual stage. He is the director of user privacy at a very small company you've probably never heard of called Apple. There, he's in charge of the privacy engineering efforts across Apple's products and services. Clearly, I have never used an Apple product in my life as you can tell from the podium up here. Welcome, Erik. Thank you for joining us. The mic and the literal stage are yours.

[00:00:30.24] Erik Neuenschwander: All right. Great. Well, thank you, Amie. And that was a great panel discussion. I want to say overall, good afternoon, and thank you to silicon flat irons for giving me the opportunity to speak to you today. I've had the opportunity to work at Apple-- this small company-- over the last 14 memorable years. And as the director of user privacy, I lead privacy engineering efforts across Apple's products and services.

[00:00:51.10] I was lucky enough to work on a number of firsts, including the first iPhone. But I'm equally proud of having founded Apple's privacy engineering team in 2011 to focus on the privacy by design approach that's been the North Star of Apple products and services, and in which encryption has played a huge role. I'm excited to be here for the relaunch of the encryption compendium. And I want to congratulate everyone involved for all of the hard work that went into developing an essential resource that will only become more valuable moving forward in the discussions.

[00:01:20.45] As we've heard today, the compendium extends back decades, beginning with the encryption policy debates of the mid '70s. 1976 was the year that advances in cryptography by Stanford researchers would feel Diffie and Martin Hellman first enabled encrypted communications to be explored by non-government users. It was also the year of Apple's founding in the Los Altos, California home belonging to Steve Job's parents. Apple's proudly played a major role in the encryption debate since its inception, steadfastly defending privacy and security.

[00:01:51.35] Encryption helps people have trust in the products that they use. It provides critical properties to support that trust, including confidentiality of communication, authentication of the parties involved in the communication, and integrity of the content. Defending encryption is synonymous with defending our ability to freely and fully express ourselves in our digital lives. It's always been clear that our digital lives are worth protecting. And it's a need that's only gained greater urgency in the pandemic.

[00:02:18.80] Encryption has been instrumental in the growth of online communication, financial transactions, health data, other pieces of modern life, including storing our digital lives on mobile devices like laptops and smartphones. Apple's commitment to encryption has withstood not only the test of time, but also forceful external pressure notably publicly from the US government.

[00:02:38.96] I hardly need to remind this audience that in 2016, we opposed a government order to develop new software that would have created a backdoor into iPhone. It was phrased in terms of one of the attackers in the San Bernardino terrorist attack. But we would have. We contended weakened security for everyone. Though we've done everything in our power to assist the FBI in its investigation up to that point, being asked to build software that would have the potential to unlock any iPhone was unacceptable.

[00:03:06.84] This wasn't a debate about our technical ability to write this code, but a question of our willingness to do so in light of the risks it would create for all of our users. While good intention, the request failed to recognize that no one can break encryption just for the good guys. The bad guys are always there looking to access people's personal, sensitive, financial, and medical data, creating a

method for anyone to ransack our most personal devices and all of the sensitive data stored within them would have opened Pandora's box.

[00:03:36.23] The very same day we received the order, Tim Cook published a letter to our customers explaining Apple's decision not to set a dangerous precedent by circumventing the security features we worked so hard to build. What Tim wrote half a decade ago still holds true today. He wrote, we can find no precedent for an American company being forced to expose its customers to a greater risk of attack. For years, cryptology and national security experts have been Warning against weakening encryption. Doing so would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple to protect their data.

[00:04:11.65] Our decision not to build a backdoor was not one we took lightly. But we made the difficult choice to say no and instead chose to protect the personal data of more than 1 billion active Apple users around the world, and we continue to do so every day. Encryption and privacy are core values shared not only by all levels of the company, but also by our customers. That's why we build them into products from the outset with both privacy lawyers and privacy engineers partnered with development team is working on every single Apple device and service.

[00:04:43.86] That's why we've become known not only for supporting strong passcodes and end-to-end encrypted messaging, but also on device intelligence, leaving users data under their control, for minimizing the data that we as Apple collect, for being transparent about the data we do collect, and giving users choice. For example, Apple doesn't have access to the biometric data like your thumbprint or facial scan that you might use as a biometric credential to easily access your phone. That data is set up by you and stored on your device because we believe that your data, like your device, should be personal to you, under your control.

[00:05:22.24] Just this year, we enabled App Tracking Transparency to give users a new choice. App Tracking Transparency or ATT prompts users, asking your permission before any app tracks your activity across other companies apps and websites. This puts you in control of your own information and your own online experience. Together with privacy nutrition labels, which clearly explain how an app uses your data rather than in confusing legalese. These tools give you both the understanding and the choice to control how your information is used.

[00:05:54.18] This is a key part of the online freedom I mentioned earlier, and it really shows how important individual awareness and understanding is to privacy. Technology can only be one part of the solution. As a technology company, we know that we share much of that responsibility. And we believe that privacy and technology must evolve in tandem. With that in mind, we unveiled additional privacy features at our worldwide developers conference earlier this year.

[00:06:20.65] Catching up on emails is stressful enough without your activity being tracked, so we introduced something called Mail Privacy Protection, which closes off your inbox to spy pixels that track your email activity. This prevents senders from learning creepy information like your location and if and when you open a message. Similarly, new privacy features in the Safari browser hide your IP address from trackers, removing a commonly used method that's used to silently link your activity across different sites.

[00:06:49.78] If you spend time online, you've probably noticed the one product you absentmindedly clicked on haunts you for weeks on end across sites and even across devices. This is thanks to an entire industry of data brokers and ad tech firms that feed off tracking you without your knowledge. And this is exactly why we created these tools.

[00:07:11.14] In keeping with our commitment to transparency for our users, we also introduced the app privacy report, which details just how often each app has used the access permissions you previously

granted to things like phones, camera, and contacts. We unveiled an iCloud tool called Private Relay that encrypts all your website traffic so that not even Apple or your network provider can read it.

[00:07:34.03] We also introduced on-device speech recognition, which allows audio data collected by our voice assistant Siri to be processed right on your device. This way, your voice stays with you. You don't have to worry about unwanted audio recording. This directly addresses the most common concern consumers have expressed about voice assistants.

[00:07:54.21] It's a common misconception that machine learning and artificial intelligence require a treasure trove of data just to work well. And every day, our progress proves that on-device machine learning, like that which is used by Siri delivers great features with great privacy. More recently, we've applied this privacy-first approach to another area, using technology to better protect children from abuse.

[00:08:20.26] In early August, we announced expanded child safety protections consisting of three separate tools to be released at a later date-- Communication Safety and Messages, expanded guidance in Siri and Search, and Child Sexual Abuse Material Detection in iCloud photos. These tools were designed to better protect children from sexual exploitation and grooming online.

[00:08:42.15] While we announced these three features together, they're distinctly different and worth exploring separately. Communication Safety and Messages is a feature parents or guardians can set up for child accounts that are part of family sharing. It warns children when they might be sending or receiving nude photos in the Messages app. In either case, the photo's blurred and a warning message appears along with additional resources to help them understand and safely navigate the situation.

[00:09:10.32] On-device machine learning analyzes the images. Apple never views them. The tool can also be used to notify parents of children under the age of 13 when their young children receive or send sexually explicit photos, showing parents a separate set of resources designed to foster the kind of healthy discussion that's so important to have in a world that only continues to go more digital.

[00:09:34.14] Siri and Search will also be equipped with resources to help in this effort. For example, by showing or telling users how they can report incidents of child exploitation. That update will also allow them to intervene when users knowingly seek out harmful and illegal material in this area. And the third tool is called Child sexual Abuse Material Detection in iCloud photos, which applies only to images that are uploaded to the iCloud photos service and uses a hybrid client and server approach to together identify iCloud photos accounts containing a collection of known Child Sexual Abuse Material or CSAM.

[00:10:12.12] The CSAM uses hashes or digital fingerprints of known CSAM collected and verified by the National Center for Missing and Exploited Children called NCMEC for short and generates something that we call Cryptographic Safety Vouchers for each image comparison back to that set. Unlike other technologies that scan every image, our CSAM detection system was designed to mathematically enforce that Apple's human reviewers only have access to information about matched images once the collection of images crosses the threshold for that account.

[00:10:46.06] Ultimately, this enables us to identify and alert authorities of accounts with collections of known CSAM. Now, with all that's going on in the world today, you might ask why these features? And why now?

[00:10:59.54] The spread of material reflecting the abuse of children online is a worsening problem, infiltrating all corners of the internet. Criminals are using technology to remotely groom children and to share illegal content that goes undetected and then goes viral, worsening the impact of the abuse every time it's shared. This is clearly an urgent need to make progress in this space.

[00:11:22.70] We knew that developing a technology that can identify collections of known CSAM while respecting user privacy, essentially protecting children while protecting privacy would be exceptionally challenging. We also knew that we found alternatives. The alternatives of doing nothing or decrypting every single photo that our users store in iCloud. It would be unacceptable. And we knew that they would be unacceptable to our customers.

[00:11:47.38] We believe that we've developed a solution that allows us to stay true to our privacy values and use technology for good. We don't have to choose between privacy or protection. We can accomplish both. With system detection in iCloud photos, Apple does not learn anything about the data stored on a user's device. As an image is being uploaded to iCloud, it will have this new safety voucher, but nothing could be learned from that voucher unless it's from an illegal image, is identified by NCMEC, and a second recognized child safety organization.

[00:12:18.44] In one of the many checks and balances built into the system from the start, both of these child safety organizations databases must list the photo is illegal. We also designed a threshold into the system to make it extremely accurate with an expected false positive rate of one in one trillion account per year. Finally, any account that's flagged goes to manual human review before any action is taken.

[00:12:44.17] So our system therefore is designed with both device side and server side components to ensure that nothing can be learned about the contents of the device. The device remains encrypted. We still don't hold the key. Still, I think the gut reaction of many-- no doubt including some listening today-- was hey, get out of my phone. That response is understandable, but I'd ask you to consider the alternatives. One alternative is to do nothing.

[00:13:10.83] Some have suggested that we simply should not attempt to build a feature that could detect collections of no CSAM stored in our service or a feature that could help protect children from grooming behavior. Others have suggested we adopt the practices that are common at other companies. Just scan all the files stored in our systems in an attempt to detect and report CSAM.

[00:13:31.65] Compared to the feature we described, the risks to that approach are greater. There's less transparency about what's being detected, less transparency about how it might be targeted to specific accounts. So such a system appears to us more vulnerable to external pressure. We are not naive to the threats we face-- those who would like to exploit this technology and its capabilities.

[00:13:54.49] After the San Bernardino attack, when the FBI requested that we develop software to break our own encryption, we never said we couldn't build that operating system. We said that we wouldn't because it would have impacted every single user's iPhone in a way that was unacceptable. Tim said it best in his remarks during a press conference around that time. He said, we have a responsibility to protect your data and your privacy. We will not shrink from this responsibility.

[00:14:22.15] So we proposed those features to balance the utility of protecting children while preserving privacy. We heard the concerns that our CSAM scanning could be hijacked to search devices for something else entirely. And we're aware that this demand will come. And our response couldn't be clearer.

[00:14:38.60] We will not build an operating system that would negatively impact the users who rely on their devices and on us. We will not adapt this feature for a purpose other than detecting collections of known CSAM. We don't believe that this feature erodes encryption, and we remain as committed to privacy and encryption as ever. But while we believe we built robust protections into the features design and the other child safety features, we know that others may have ideas on how to strengthen these even further to protect children. We want to listen to that feedback.

[00:15:10.36] If you have substantive suggestions on how to build stronger child safety features, we want to hear them. At the end of the day, Apple builds consumer products, and consumers face threats.

Ransomware attacks on governments, corporations, and individuals are in the headlines every day. The threats we all face have never been so severe. And we're constantly looking to stay a step ahead so our users don't have to.

[00:15:34.66] Here's what we're up against-- attackers generally consider three things-- the number of devices, the number of opportunities, and the value of access they might get. As of this past January, there are more than 1 billion iPhone users worldwide. And because smartphones can do so much, they represent several vectors for attack. You could be delivered malicious software by visiting a website, downloading a file, or otherwise attacked.

[00:16:00.26] And for attackers, a connected device like iPhone is absolutely worth their while. For the wealth, personal, medical, and financial information they contain, including credit card details, contact information, photos and locations of our loved ones, and more. Threats that have been present since the day we launched the App Store, we continually take into account.

[00:16:21.50] Last year alone, during a pandemic that drove work, school, and play inside and onto our devices, our app review process, which relies on human reviewers, as well as technology prevented more than $1.5 billion in fraudulent transactions. We also stopped nearly 1 million apps from making their way onto the Store and into the hands of users. I want to clarify that not all of these applications were rejected for being malicious or otherwise misleading.

[00:16:48.05] Our strict guidelines on privacy, security, and spam overall make app store the safest place to find secure, high-quality apps. Other apps might be rejected for a range of reasons. Last year we rejected more than 48,000 apps for containing hidden or undocumented features. We rejected more than 150,000 apps for being spam, copycats, or misleading to users. And we rejected more than 215,000 apps for privacy violations.

[00:17:16.21] A strict app-review process isn't the only factor that sets us apart. We also require that users download apps directly from the App Store rather than sideloading them from an internet browser or an unauthorized third-party app store. This prevents our users from being exposed to unvetted apps from questionable sources. This one move has done wonders to protect our users and build trust in the app ecosystem not only among consumers, but also among developers.

[00:17:45.41] With more than 1 billion iPhone users and nearly 2 million apps available in the App Store, it's inevitable that problems still surface. And successful attacks do occasionally occur. That being said, we're confident-- and security experts agree-- that Apple is more secure than our competitors.

[00:18:03.48] Coupled with the security and privacy protections that are built into our devices, the App Store presents users with a key line of defense. A 2020 report on malware attacks in mobile and fixed networks around the world found that the pandemic fueled a massive surge in attacks on mobile devices, and yet less than 2% of infections were attributed to iPhones. In comparison, Android devices represented nearly 27% of infections. Over 10 times more.

[00:18:31.30] It's worth noting here that Android's operating system allows for sideloading. Users can download apps from just about anywhere. And the amount of malware on their devices reflects that. Our integrated system presents a different choice, and one we believe has strong benefits to developers and users. It creates the security and the seamless user experience that we're known for.

[00:18:53.23] It's why consumers love our products. It's why they trust their devices to store their most sensitive personal information. That's why they download new apps from the App Store every day and then use and complete transactions in those apps, inspiring developers around the world to keep on dreaming and keep on creating.

[00:19:11.24] There is no absolute security nor absolute privacy. But working toward this goal is always worth the effort. The second we stop moving forward as an industry, we fall behind. I can only speak on behalf of one company, but I'm confident that we have the talent and the tenacity to make a difference for Apple users around the world.

[00:19:31.04] Much of our work is relying on yours in this community. And I'm here today to recognize that important partnership and assure you of three things-- our commitment to encryption is steadfast. Our commitment to privacy and security is steadfast. And most importantly, our commitment to consumers is steadfast. Again, thank you very much.

[00:19:53.70] [APPLAUSE]

[00:20:01.00] Amie Stepanovich: Thanks so much, Erik. We have three student questions for you. The first one comes from Richards, so I'm going to invite him to the stage. And like before, I'm going to disappear to give him lots of space to ask his question.

[00:20:18.45] Richard Koch: You want me to sit?

[00:20:20.17] Amie Stepanovich: Whatever you want to do.

[00:20:24.28] Richard Koch: Hi, Erik. Thank you thank you so much for speaking with us today. You said in your speech that the CSAM detection technology was developed as a response to a worsening problem you characterized as an urgent need. And you also said that the system will not be expanded to cover other types of content. How can you give an assurance that there won't be another urgent need in the future?

[00:21:09.26] Erik Neuenschwander: So I think that the material that we're talking about is so far over the course of history. It's been unique in that it is widely recognized by countries around the world. There's a clear definition of the illegality and the harm to harm to kids. There are plenty of regions that find other things to be specifically bad for their region or given their history, but this one is effectively universal around the planet.

[00:21:37.69] So I would tend not to speak in terms of full absolutes. There might be in the future possibly some other urgent need, but the properties of our system would say even if there was a similar consensus around something else, that the actual implementation would change in a way that is noticeable to people. And so I think that there isn't anything that meets this same level. That's why we were motivated to approach this one singular issue with a whole suite of new technology. And I think it has been a growing problem that we as a tech provider should be devoting resources to addressing and mitigating.

[00:22:18.42] Richard Koch: But other types of content may be addressed in the future. Is that correct?

[00:22:23.40] Erik Neuenschwander: I mean, I'm speaking, you're saying over-- what I took your question to be is over the arc of human history sort of thing. This is a system that's designed for CSAM and has a number of protections to make it be exactly that. We're not going to design this system to do more. If there were something else that was an equal challenge, I think we would rise to meet that challenge as well. I don't know at all that it would be that system. It's this system. It's really a hypothetical, right?

[00:22:46.70] Richard Koch: True. Thank you.

[00:22:48.29] Erik Neuenschwander: Sure.

[00:22:52.93] Amie Stepanovich: All right. Our next student is Megan Cook. You want to come up?

[00:23:13.25] Megan Cook: [INAUDIBLE] right in the back. Thanks, Erik, so much for sharing all that information today. The one thing that I really took away from this is how many different challenges,

privacy, and opportunities from all different constituents. And as a result, you all have to walk a really fine line between privacy and protection.

[00:23:39.68] Can you walk us through some of the specific criteria you use to make those types of decisions? I imagine that you all have to have a pretty strong sense of what that line is in order to rule things out like the child protection services.

[00:23:54.47] Erik Neuenschwander: Mm hmm. Yeah. We overall use-- at the highest level, we have four pillars or principles that we use to organize our thinking when we're looking at some new features, some new service that Apple might introduce. And in my mind at least, they're ordered.

[00:24:12.74] And so first and foremost in that list is data minimization. We really seek to have the system process the minimum amount of data, or at least to expose Apple to the minimum amount of data to deliver great functionality. That's where you heard me talk about on-device intelligence as part of the talk.

[00:24:30.65] And on-device intelligence is something left under the user's control on their device. It isn't data that gets exposed to Apple. It's a great technique for achieving data minimization. Other things like degrading the quality of data or limiting retention or other ways to minimize data.

[00:24:47.42] Second is restricting the use of that data. So ensuring that it's only used for the intended purposes. And that has sometimes a policy component. Things like access control lists or whatever have a role to play limiting who can get data-- who can see data once it's been collected. But there are also technical means that we can take to degrade that data away from other uses.

[00:25:08.66] So things like Local Differential Privacy is a technology we've used. And this in short randomizes the data on the device before it ever comes up for analysis. And that means that it only works to analyze that data in aggregate from a number of different submissions.

[00:25:25.34] When you get an individual piece of data, you can't conclude anything from it. When you get a large collection of data, you can learn trends from that. And that's a much more powerful way than simply collecting individual items and then saying, oh, we'll only look at the aggregates. We're actually imposing a technical control so that the data is only useful once aggregated. It's only informative once aggregated. So that would be a way of looking at use limitation.

[00:25:48.92] Transparency and control is the third pillar. And these are very important. It's important to be transparent to users and to have them be able to have control over data collection. But you'll note it comes after the other two. It's only after first asking the question of is this data necessary at all? And how can we restrict that use down to the minimum to provide the great functionality? Yes, you should have transparency. You should have control.

[00:26:10.97] And then last but not least, not really fourth in the list is security. Security has two different aspects to it-- security underpins all the three things I already talked about. If a user is supposed to have control over something and there's a way for an attacker to evade that control, that's a breach of security, and it undermines the notion that you've given control over access to say that sensor or that data.

[00:26:33.53] But security also has the role to play in encryption, what we're talking about today. And that's encryption both of data at rest and data in motion. Encryption provides the capability to help assure things like the confidentiality of users data. And so when we think about things like our imessage communication service, end-to-end encrypted between the sending and receiving devices so that even though those messages transit Apple's servers, even though if you're on an airplane, like, maybe people will get back to doing, and the message can't be delivered, and so it's going to be held by the server, it's held encrypted with keys that Apple never possesses.

[00:27:07.88] And that means that we're able to provide privacy assurances around that service built directly on top of the encryption primitives and the design of that algorithm. So those are the four things that we reliably look at as lenses to apply to each problem. And then for any given more specific project that we're talking about, we start looking at individual threats or risks and the assurances around privacy that we want to be able to provide users for the specific thing we're designing.

[00:27:37.14] Megan Cook: OK, Thanks.

[00:27:38.54] Erik Neuenschwander: Thank you.

[00:27:45.19] Amie Stepanovich: Our last student questioner is going to be Dave.

[00:27:59.46] Gabe Rudin: Hello. Thank you for your time today. I really appreciate it. And it's a pleasure to meet you virtually.

[00:28:05.65] Erik Neuenschwander: Thanks you too.

[00:28:07.35] Gabe Rudin: So I have a question for you-- or two rather-- and there on the subjects that you've been talking about today. And the first is that the CSAM detection material in general has-- as you've said, it's a lot more secure because of on-device scanning that you've done in the way that you've implemented it as opposed to other players in the industry that may have on-server scanning in a way that you've said is less transparent or it enables greater access to clients data.

[00:28:40.85] But what would you say to people who are skeptical of this approach only in that it may have broached a new territory where client side scanning is now just the beginning of something else? Where it may not be a threat in the way that you've ruled it out or with the scope that you've said it is, but it becomes an area that's now more familiar to consumers and that hurts civil liberties in general going forward.

[00:29:10.85] Erik Neuenschwander: Yeah there's a couple of different directions to unpack that. I guess first I would say, you mentioned in the way that you've implemented it. I think that that can lead to a misconception that this is something that we're rolling out now and it's something that we brought out and described and proposed. We'd done enough work to feel confident that it was something that could be implemented, but the phase that we're in, for people that have those concerns is one of discussion listening and dialogue.

[00:29:36.35] And so this isn't something that we're fixed on in terms of the approach. What we're fixed on is that it is something that we think we need to do across child safety to do more to disrupt grooming, to do more to disrupt this kind of hoarding and exchange of material. Specifically for why we think it has that greater protection and how people interpret it, I'm not quite sure that we've all agreed on the words.

[00:30:02.54] I wouldn't call it client side scanning because client side scanning would seem to imply that there's a result known based on data on the device. And that's not possible. Under this system, it requires the server side processing and the server side storage of the data and the result of the first half of the private sector interception protocol.

[00:30:22.79] The part that I think people would call the matching or the scanning. The way it's designed, the result isn't knowable until a threshold of material has been accumulated within an account. These are properties of the math of the system. And that's very different from what I think people would intuitively understand client side scanning to mean. Maybe that means we need different words. Maybe it just means we need to be more precise.

[00:30:46.43] And so then to your third point, I think it's important to have these norms and properties in a system that we've designed a number of different checks into the protocol, into the approach so that we feel that this is a system that would actually work very solidly to not be able to be expanded beyond the

scope that we've discussed without the properties-- without that being transparent and required to be transparent at a technical level. I think those are key properties in the system that we proposed. And a system that we rolled out would need to-- in my opinion-- at least have those implemented in some way, shape, or form. And the current state of the art that we saw or we were able to conceive of for a scanning based on server-held data on servers didn't have those properties.

[00:31:34.41] Gabe Rudin: OK, thank you. I appreciate that. And underlining everything that you've just described there, there seems to be, as you were saying a commitment to strong normative values. And I was wondering-- and you know you protect US citizens very strongly in that regard. And I was wondering if in your opinion, Apple has that same level of commitment to citizens of other countries and other locations.

[00:31:57.85] Erik Neuenschwander: OK. I want to answer that generally and then make sure-- because I feel like you're asking in the context of the proposed features. I'll come back that too. First, we've said-- I didn't work it in today, but privacy is a fundamental human right. That's a belief of the company. And if you think something is a fundamental human right, that means you apply it universally, and you don't consider it to be one thing for a US person and another thing for another person.

[00:32:19.45] So absolutely, that's our approach to privacy. That's underpinned by the fact that we have are one global operating system that we ship features in the same way. For the system detection in iCloud photos feature specifically, it's something that in our proposal, we had only completed our analysis to even contemplate launching in the US. And it would be additional analysis about the risks to users of our products before we expand it beyond the US. We're most familiar with US law, US policy, and the US organizations that support child safety. And that's still going to be our focus as we look at what kind of features we want to ship.

[00:32:58.32] Gabe Rudin: OK, I appreciate it. Thank you for your time, sir.

[00:33:00.84] Erik Neuenschwander: Thank you.

[00:33:09.80] Amie Stepanovich: I'm going to start turning to the questions that we have that came in over zoom. Give me a second to get to-- I keep trying to push my mouse from over here to over here, forgetting that they're not connected to one another.

[00:33:26.03] Erik Neuenschwander: Not yet. That's a feature in Mac OS monterray and iOS 15.

[00:33:30.68] [LAUGHTER]

[00:33:31.58] Amie Stepanovich: Thank you. Keep working on that. So Andrew Zach asks, can Apple claim that imessage with communication safety turned on is still end-to-end encrypted if it detects explicit images? It may not be definitionally client side scanning, which you just spoke to, but is it still true end-to-end encryption?

[00:33:56.99] Erik Neuenschwander: OK. So what I just spoke to, I want to really draw a clear line first. And first I'll say, the clear line I have to draw now is Apple's fault. We introduced three things all at once. So I have to talk about all three things now because it's what we talked about and it's too confusing. And so right now, what we just did, I'm drawing the clear line for everybody as we move from the prior question, which was about our iCloud photos feature, and now we're talking about the communication safety messages feature, which is totally fair.

[00:34:25.98] But everything that I was talking about in terms of the design of the scanning applies to that feature. And I have talked about this other feature differently. That said, it's still obviously a valid question. So can Apple still contend that imessage is end-to-end encrypted? There's obviously very active debate on this. My personal view is that end-to-end encryption protects communications from unwanted

or unintended disclosure to someone who's not party to the communication. That's what I think as technologists the assurance that we can provide people.

[00:35:00.74] It doesn't say that if you message me right now that everybody in this conference won't see it, because I could hold my phone up to the screen and then everybody would see the message. And we don't have a technical way to prevent that, right? So that's why I think that it makes sense when we're talking about end-to-end encryption to look at the unwanted unintended disclosure. And the feature that we propose leaves any notification to the parent under the control of the child who is a party to the communication.

[00:35:32.45] That doesn't mean that the analysis is done. That doesn't mean that oh, well, since no keys were harmed in the making of the feature it's obviously a good feature. It's still quite right to ask questions about the use, abuse, misuse of this feature. And that's part of what we're discussing with a number of experts.

[00:35:48.47] But I as a person who considers himself a staunch defender of encryption and works at a company, who's very keen on encryption, I'm very worried about trying to make broader claims and what the technology can support when we want to signal to anyone who would undermine end-to-end encryption where those lines should be.

[00:36:15.80] Amie Stepanovich: I have a question from Matt Blaze-- I like the idea of our first keynote speaker asking questions of our second keynote speaker-- asking what detecting terrorist training materials have been considered an equally urgent need immediately post 9/11?

[00:36:34.20] Erik Neuenschwander: So was that a statement or a question? I guess would we have considered it?

[00:36:38.76] Amie Stepanovich: [INAUDIBLE] detecting terrorists. So you're talking about CSAM as an urgent need. Would terrorist training materials have at the time immediately post 9/11 have been considered an equally urgent need?

[00:36:51.47] Erik Neuenschwander: Right. And it's tough to retrospectively talk about that hypothetical. If I give just my gloss of what I think the properties were at that time, it wasn't that there was a globally-- two things-- that one, there wasn't a globally identified definition of exactly what material like that would be. And two, there wasn't a global norm that said that the mere possession of that material was itself illegal.

[00:37:23.25] I'm on the engineering side, not a lawyer. So I don't want to make too many assertions about what's illegal or illegal, but through our work on this feature, it's just not acceptable. It's not acceptable under the law to hold the material when we're talking about CSAM or C-A-S-M. There's been no such push in the US and therefore no such push at a wide range and globally across many countries to make that same definition around a set of defined material.

[00:37:51.39] So I don't see them as being the same. I think implicitly in that question is wouldn't that there have been a lot of pressure to go use this nifty tool to go look for terrorist material? And again, it's hypothetical, but sure, that seems plausible to me. I think that for cloud services that process material in cloud services, that pressure is technically greater because the ease with which a search can be particularized and the ease with which an algorithm can be modified are lower than in a system where you have a hybrid approach that involves the device and the server. The device attesting to some aspect of the algorithm as we roll out our operating systems give some additional properties that I think help provide disincentives or raise the cost of scope creep.

[00:38:44.60] Amie Stepanovich: So you've talked a little bit in response to a couple of questions about the fact that this isn't something that's actively being implemented right now. One of the questions talks

about how you have started a process of collecting input. And they ask, is there a structured plan for ensuring transparency in that process that Apple plans to follow? And will that plan include-- if the plan exists, I'm assuming-- the creation of documents to codify your findings, such as through a human rights impact assessment?

[00:39:18.16] Erik Neuenschwander: So we've been very-- we think the transparency around what we're proposing is critical to improving trust. Part of why I think there's been able to be so much engagement on our proposal is the bunch of material-- wealth of material that we published as part of the initial announcement. We're going to continue to be transparent about the choices and trade offs as we move forward with the features.

[00:39:44.15] Amie Stepanovich: I'm going to ask-- there's two questions I kind of want to ask together if possible. To start you there have been-- I think the first question refers to a few different systems. For example, it says researchers have identified flaws in some of the privacy tech that Apple has pushed in the past and references privacy loss parameters, differential privacy, and the neural hash collisions.

[00:40:12.34] And then talks about-- gets to a question of how should consumers approach having confidence in Apple's privacy efforts given-- I think what they're identifying as a discrepancy between the math and the talking points. And then the second question relates to this in a way to that question of trust-- of given that you're scanning children's incoming communications, is there any special consideration that children should have about the fact that their communications are now being scanned coming through the iPhone? That may be what happens on the iPhone isn't staying on the iPhone. Kind of referencing that public communications piece as well.

[00:41:07.91] Erik Neuenschwander: OK, you put them together, I see the questions a little bit separate, but let me hit them both. Starting maybe with the second one is a little bit simpler. So a child will know that the communications coming in through the Messages app are being scanned. So first of all, what happens on the device in that context is just on the device. The notification piece is separately under the child's control.

[00:41:34.49] And again, going back to the technical definition of end-to-end encryption, I find this to be again, somewhat just challenging to draw a line technically because let's say I send you a message in the messages application-- over imessage-- that message is decrypted and processed just to be rendered onto the screen. To be displayed so that you can read it. It's a photo or if it's a text, your device is processing those bits.

[00:42:00.59] Under our communication safety feature, it additionally processes the bits using a classifier to decide if an image that came in is maybe a nude image. And then it further renders those bits a little bit differently. It doesn't just show you the image. It shows you a blurred-out version of the image. And all of this is to service you. A nude image came in, you maybe didn't want to see it, it's processing to blur it out or it would process it to show it to you. And this is just local processing. We can call it client side scanning, but it is already being processed by your device just to provide the functionality to you, which is what safety's there for.

[00:42:39.74] Separately, on top of that, there's an additional step that if you confirm the parent could have set up a notification-- and there's been a lot of conversation about the utility of those notifications and how a child will really interact with them, especially across a range of years. And we continue to be interested in experts opinions and research studies on the notification piece. But that's separate I think from the blurring. And the blurring is a feature which is only occurring on the device. So I see those as pretty different.

[00:43:10.79] Broader with-- so I'm going back to our launch of local differential privacy and such. I think you said that there's a discrepancy maybe between the math and the words or the description. I don't

think there's a discrepancy. But what we saw in the local differential privacy example is a great example. Is that there are limits to what math can assert or assure. When you deploy and embed a system that runs on devices and uses the internet, there are a bunch of things involved which math has nothing to say about.

[00:43:40.83] And so one of the critiques of local of our differential privacy was well-- I'm going to try not to make this be like too often the weeds technical, but there's this idea of epsilon, which relates to the amount of randomization or the amount of privacy risk of the submission. And there's an additional concept called the privacy budget, which basically says, don't take too much data or you'll end up with an epsilon that goes to infinity.

[00:44:07.40] And so people said, well, this device keeps submitting data, and so Apple shipped an infinite epsilon, and that's really bad for privacy. Well, within the math, there isn't a way to answer that question. But within the system, the packets that are collected from users devices don't have any identifying characteristics retained. A real technical person would say, but it has the IP address.

[00:44:28.85] My response is yes, the IP address is dropped at the network boundary and not held by the system that processes the data. So there's no IP address that's left with the packets of data that get processed to do the analysis. And so the basic assertion of well, if a device keeps sending information, then you have a perfect idea of Erik over time, it presumes that the system can actually go find two pieces of information and relate them together, let alone assigning them back to Erik.

[00:44:53.45] And we designed different protections into the system to prevent that. Everything I just said has nothing to do with differential privacy though. It's about packets on the internet, and storage and databases, and a bunch of things that fall outside of what differential privacy has anything to say about.

[00:45:09.92] That was a challenge and that continues to be a challenge with features we roll out, where we have a level of protection, which is technical based on math, based on crypto or based on whatever and what that system could possibly say about a system-- I'm sorry. What that mathematics could possibly say about a system deployed in the real world. This is a communication challenge.

[00:45:30.92] And to try to get to the last part I think of that question, so then how to assure trust in these systems which have technical complexity? I think it comes down to both the transparency that we provide in terms of our descriptions of the assurances and of the implementation. And wherever possible, where we can put that implementation or that code into the hands of people through the operating system image so that if we have it wrong, somebody will call that out.

[00:46:01.61] And this isn't to presume, or to say, or to claim that out of our billion users, very many of them have the technical wherewithal or the time or the resources to do that. But it doesn't take all of them. In a world of Twitter, it takes one to find it, to tweet it out, and then if we were trying to pull a fast one-- if anybody who tries to pull a fast one, the jig is up at that point. And so really, I think that the transparency in terms of our descriptions and the transparency where we can in terms of the code give a lot of avenues for people to increase their assurance around the claims that we make.

[00:46:41.00] Amie Stepanovich: Thank you so much. You've stayed with us a little bit over time. I appreciate that. Thanks for giving so much of your time for talking through what you're doing and where you might go next. So Thanks for sharing some time with us.

[00:46:53.76] Erik Neuenschwander: I appreciate it. Thank you especially to the students for the great questions, but for all the questions and engagement. Thank you.

[00:46:58.76] [APPLAUSE]

[00:47:06.92] Amie Stepanovich: So that conc--