
# Global Encryption Day – October 21 2024 - Encrypt Today to Safeguard Tomorrow: The Encryption Summit

## Encryption, Arrested: The Arrest of Telegram's Pavel Durov

**Greg Nojeim - CDT:** Hi, everyone. My name is Greg Nojeim. I'm with the Center for Democracy and Technology. Welcome to this part of Global Encryption Day the panel on Encryption Arrested the Implications of the Arrest of Telegram's Pavel Durov on Encryption Related Charges. As I said, I'm Greg Nojeim. I'm with the Center for Democracy and Technology.

I direct our Security and Surveillance Project. I also sit on the steering committee of the Global Encryption Coalition, which is sponsoring this event and Global Encryption Day every day each year. I'm sorry, on October 21 each year, the Global Encryption Coalition consists of 434 members, located in over 105 countries.

The steering committee of the Global Encryption Coalition is Center for Democracy and Technology, my organization, Global Partners Digital, the Internet Freedom Foundation, Mozilla Corporation, and Internet Society, which has graciously provided the logistics for Global Encryption Day.

The background on this case is that in August of this year, French police arrested the Telegram CEO Paval Durov at the Charles de Gaulle Airport in France. He was arrested by French police. He is a citizen of France.

He was charged with failing to abide by takedown and disclosure demands made by the government of France, and also with failure to register an encrypted service and

register the export of encryption. It's important to keep in mind as we discuss this case that the encryption related charges with respect to Telegram are a little bit out of place in the sense that most of the communications on Telegram are not encrypted.

Only one to one communications are encrypted, only when one of the parties enables encryption, and only when both of the parties are online at the same time. A lot of communications on Telegram are on channels, they are broadcast to a large group, or they involve large group chats. Neither of those types of communications are encrypted.

So Telegram is more social network than private messaging app. Nonetheless, Durov was arrested on charges that include failure to register an encrypted service. And I have to say, it was of a lot of concern to folks who are involved in the encryption advocacy, including our organization. In fact, I can say with confidence that the arrest of Mr. Durov was the most talked about development in all of 2024 on the Global Encryption Coalition participants list.

So let's turn to our panelists now to, shed some light on this case. First Noémie Levine. is the policy advisor for La Quadrature du Net, a French organization fighting for digital rights, a leading French organization fighting for digital rights. She's been working for several years with them now, especially on surveillance topics, such as limiting intelligence services hours and the documentation of police practices, such as the use of algorithmic biometric based CCTV, and on encryption as well.

We'll start with Noémie. Noémie, could you please tell us what laws in France Mr. Durov is accused of violating, and why was he arrested, and guess so publicly, in a sense, right at the airport in Paris.

**Noémie Levain - la Quadrature du Net:** Hi, hello everyone and thank you for the invitation and to talk about this important important subject. The, as you described it well the case is quite singular and complicated and it doesn't look like so as a French organization, we were the first in the first row to see that.

And we could, and as you mentioned, there is two kind of levels in this case. There is a legal one and a political one. On the legal aspects. It's quite difficult to know exactly what's going on because the only information we got is information given by the public prosecutor. They don't have an obligation to say what is going on, but they decided to do it.

And this is how the legal and the political aspect joins, meaning that if Durev was arrested such in a spectacular way and with the public prosecutor. Wanting to disclose information about the case. It means that they want to make it political and they want it to make it as a warning, we think, or as a big I mean as a important event and a warning maybe to other encryption or Internet services.

Once I say that, so what do we know right now? We know that Pavel Durovoi has arrested for several things. The main one is not encryption, is more about content moderation because Telegram is well known for not moderating content. enough the content shared not in the encrypted private messages, but on the public list.

So what we understand from the public prosecutor information is more than that. It's this, that is Approach to Pavel Durov, meaning that he's prosecuted for being for complicity of several several offenses, such as pedopornography, child pornography, and saying that As a given mean of sharing information, Pavel Durov is criminally responsible as the CEO of Telegram.

But once we say that, when we dig a bit further on the information we have we see that it may not only be about content moderation, but also about encryption and more general about being a technical intermediary. We think that because in the several grounds and that legal basis that was that was communicated, we see some some things about, as you mentioned registration or declaration of being an encryption services, which is actually an old law coming back from the early 2000s that is not really known for being enforced or oftenly enforced.

But when you see that the judge, the prosecutor, uses this legal basis, is that there is something to see about around the private messages being encrypted. And the other thing we have in mind is that they say that Telegram didn't comply to the obligation to disclose information to the police to do some legal interceptions.

And usually this grounds is more for Wiretapping or classic phone. And so we're like, okay, so if Telegram has to disclose information for interception, maybe it's encryption keys. We don't know. Still, this is only from the public prosecutor press release. And it's, we, and it's really hard to know what will happen, but we see it's pretty complex and behind the content moderation, we can believe that it might be also an open door to then ask questions about how the service works and maybe ask for information about encryption.

**Greg Nojeim - CDT:** So how does, where is the case in the legal proceedings right now? Is he going to go to court very soon or is this us where we are in the proceedings.

**Noémie Levain - la Quadrature du Net:** So it's only the beginning of the investigation. He was arrested only to be asked some questions. We will further know if the public prosecutor will keep all the legal grounds he communicated with, or if maybe he will say, okay, we only sue.

Pavel only for three of them, and we drop all the rest. We don't know that, and it's still the beginning so it can last for years. And also, as I mentioned earlier, There is no obligation to disclose information about the case, so we are a kind of dependent linked to whatever the public prosecutor will say or, as it happens a lot in France, if there are some leaks to the press.

So now it's just investigation to see if Telegram has a part to play, had a part played more in all the all the offenses and and the legal grounds he was accused of, such as complicity of several crimes or not be declared some encryption tools or not disclosing information for interceptions.

**Greg Nojeim - CDT:** So what is the political context for encryption in France? Is the government friendly to encryption?

**Noémie Levain - la Quadrature du Net:** So if we come back in the nineties, it's important to know that France was one of the last countries to drop encryption when it was, it used to be some state private competence.

So it only liberalized it and made it free at the, so yeah, the late 90s. And we've been worried the past years because we saw some attempt on encryption and private private communication at several aspects, political and also in judicial case. For example last year there was this big trial against activists.

There was a lot of stuff that were in this case, they were sued for planning an attack that they didn't do, but Among all the elements they were it was said that they were using encryption tools such as Signal or Tour, or VPN, and the judge said that they, it showed that they want to live in clanestivity and that they want to hide something.

So we were like. 30 years back in the old approach of encryption saying it was some criminal tool. So this was really precedent. We were really worrying about that a judge could think that using signal could make you make as a clue. In, among other things, that it can make someone a criminal.

In other stuff, we see a more general political context, where the French government always say that some social networks, or some Some communication are part of some crime. Let me explain myself. For example, last year, there were some riots in the country after a policeman killed a young boy.

And the government asked the social media to remove some content and said that the social media were part of a response had a part of responsibility. Same thing happened this year in New Caledonia. Which is a French department where there were some riots and the government blocked TikTok in the entire island.

So we see a new age of the government targeting social media, targeting Targeting communication means saying they are complicit. You could see the clue of complicity over the crime. And just to finish, we see also a lot of cases where the police, French police, helped. Undermining encryption, such as AnchorChat, or SkyECC, or more recently, the Ghost Messaging app, where the police took a big part in undermining, in finding a way to to circumvent encryption.

So you can see that right now it's a big thing in France, and actually some Institutions say that today encryption is an obstacle for them, and they are trying to find ways to circumvent it in criminal cases.

**Greg Nojeim - CDT:** Let me stay with you for a little bit longer. It really startled me that a person could be arrested for not registering an encryption service, especially when most of the communication on the service aren't even encrypted.

It really was a shock. And I think it sends a message to other CEOs of large companies that they have to worry about about being arrested when they travel.

Do you have any, again, it came out of the blue, have you ever heard of somebody being arrested for failure to register an encrypted service? Have you ever heard of another country requiring such registration?

**Noémie Levain - la Quadrature du Net:** No, actually it's the first time and this is why at the beginning I was saying there is both linked legal and political aspects because we think that they use this old law.

So this this obligation to register came at the early 2000s with the liberalization of encryption. They said, Okay, encryption is free, but there are a few obligations to keep a bit of control of it. But we never paid attention to it because we never heard some stories. So when you see that some judges, some prosecutors, are taking back this from the bottom of the laws, that everybody forget about it.

You're like, okay, maybe they want to try whatever they want, whatever they can to get to Paval Durov, including encryption messages. Or maybe they dunno what they do, or maybe they actually really know what they do and they really want to get to the encryption part, or they want to get to Telegram in general, because Telegram is shown as the enemy, I don't know if it's the right word, but this is why we think it's very political to make it public, to arrest him like this, to arrest him on very weird and surprising legal grounds, is to show a signal, to show a warning to other services that would not comply with legal obligation of content moderation.

That's what we think. But it's still disproportionate. It's normal that you were surprised, and it's normal that you are worried, and we are worried too.

**Greg Nojeim - CDT:** Yeah, I have to say it was a shock. Our other speaker Daniel Kahn Gilmore is having trouble logging in, so we may have to proceed with the event, just you and me, Noémie.

Let's continue the conversation. So what I wanted to talk to Dan about was the fact that encrypted services are not all WhatsApp. They're not all huge. In fact you could have an encrypted conversation in a game. And there are people who are developing all kinds of

means to communicate. that include encryption but that aren't really large services. They're just something that somebody created for to have the ability to communicate with their friends and with their like minded folks.

Talk to us a little bit, Noémie , about how surprising it might be for a person who's developing an encrypted messaging service to all of a sudden face a requirement that they couldn't know about to register their service with a government.

**Noémie Levain - la Quadrature du Net:** Yes, of course, I am sure a lot of people just discovered this this obligation. And again, I think here, the specificity of it is, again, to link it with the political aspect. I'm not a magician, I don't know everything, but I don't think the government would do that with a small one, not yet, it's not the first enemy yet but still, enemy. For example, I discovered that France was the only country to have this kind of obligation. We knew it was an old law, but when I saw you being shocked, and I saw a lot of people in the world being shocked with this obligation, we realized how bad France was with this.

And also, we know that Telegram has a lot of issues with a lot of countries. And when you see that France is the one who decided to shoot first, and not caring that much about encryption rights and privacy rights, you could have, you can feel that democracy right now in France is not, it's not at the best stage as as it was.

But of course, for small providers, it's not a good sign at all for what, what can come in the next years, if the law change or if some judges decide to enforce this law that everybody forgot about.

**Greg Nojeim - CDT:** Thanks, Noémie . Let's turn to Daniel Kahn Gillmor , who has joined our discussion.

Hi, Daniel. Why don't you take a minute and introduce yourself and tell us about the significance of this case to technologists and to other people working with encryption.

**Daniel Kahn Gillmor - ACLU:** Sure. Thanks. And again, apologies for the delay. I'm Daniel Kahn Gillmor .

I'm a technologist for the American Civil Liberties Union. It's a US NGO that focuses on civil rights and civil liberties and I work within the speech privacy technology project there because our infrastructure has an impact on the sorts of rights, whether that's privacy or censorship concerns I'm also a free software developer, and I contribute to the Debian project, which is a foundational Linux free software distribution.

It's an operating system. It's what I'm calling you from. And I tend to only run free software, which explains the challenges that I had connecting here, because Zoom kept wanting to route me through their proprietary software, which I would rather not use.

That said I'm also active within the IETF. I see some folks in the chat already who are also active within the IETF.

The IETF is the Internet Engineering Task Force. And I'm concerned about how we make sure that we have functional infrastructure to have secure communications and to have censorship resistant communications. One of my big concerns, so France is not the only nation to have laws that regulate import or export of cryptography.

And I've only managed to hear parts of the session due to some of the connection challenges that I was having. So I hope this wasn't, I'm not repeating too much ground here, but the U. S. is a classic example. The U. S. had laws on export of cryptography in the 1990s, and those export laws constrained what cryptographic technology the U. S. companies could export. And that itself had issues for people around the world because if they were receiving tech from a U. S. company, they would only receive the weaker versions of the encryption technology.

We no longer require those same controls from the U. S., but we actually still see decades after those regulations were rolled back, we still see these legacy weakened crypto systems just deployed around the globe. So there are some concerns about making regulations that limit import and export of cryptography because even when we realize that they're not useful, that they cause harm to folks who want to communicate securely, which is everyone.

Even when we fix those problems, and we say, let's take those regulations back, sometimes old software is still out there. And worse yet, because some of the old software is still out there, other people might say we're going to make our tools interoperate with the weaker systems because we want to talk to everybody. And the result is, you end up with systems that are able to be downgraded or weakened to the legacy mistakes we've made in the past.

So I wanted to flag that as one of the concerns for cryptographic regulation is that the more hurdles you put, it's challenging to make a functioning cryptographic system. And the more hurdles we put on making one that actually works, the more risk we have of getting it wrong, not just now, but into the future.

We should be removing the hurdles to be able to have secure communications, if we believe that it's worthwhile, that people be able to talk to each other across the globe.

**Greg Nojeim - CDT:** Dan. Great. How many encrypted services are out there? Are we talking hundreds, thousands? Is there a way to count?

**Daniel Kahn Gillmor - ACLU:** Let me push back a little bit on the frame of encrypted services, actually, Greg.

So when we talk about encrypted platforms today, we think about the Internet in terms of platforms, right? There's platforms that are operated by Meta, there's Telegram, there's you know, Signal, and we think about them as these services that run. But the cryptography, if it's strong cryptography, happens on your machine.

It happens on your device, whether it's an iPhone, or a computer running Debian, or a Windows machine, or whatever. The cryptography, the end-to-end cryptography happens on the endpoint that the user controls. And it is possible to overlay strong cryptographic protections, it's challenging, over a communication system that doesn't have them in the first place.

The service doesn't have to be the thing that's encrypted, it could be just the software. That's doing the encryption. So when we say how many services are there we could count the web services, the services that are on the network and see just how many of those there are. And we could probably come up with a number in terms of, widely used ones in the dozens.

But if we talk about what pieces are there out there that provide cryptographic mechanisms those are fundamental building blocks to how we use the Internet today, right? A piece of software that provides the ability to use TLS. Which everyone is using today to talk to this session, right? This Zoom session is covered with, everyone who connects to it uses transport layer security.

That's an encryption mechanism to connect to Zoom servers, to get the audio feed to hear what I'm saying right now, and to see all of our faces in the video stream. The people who build TLS toolkits are widespread. Now, there's not more than a dozen functioning, widely used TLS toolkits, but TLS isn't the only thing that does encryption.

There's encrypted email mechanisms. There's encrypted messenger apps, right? Again, I don't consider Telegram to be a fully encrypted messenger app. It's only partly encrypted. There's a little bit that you can turn on encryption. It's not actually What I would want. It's not best of breed for encryption, but in terms of distributing tools that provide encryption mechanisms There's lots of those out there and they're not because those tools are also redistributable.

There's not one distributor, right? So the Debian operating system collects a bunch of software packages. Some of those do cryptography and those come from different places Who is responsible for the import or transfer of these cryptographic systems? Is it the French Debian contributor? I'm not French, but there are French Debian contributors who takes a piece of cryptographic software from someone in, say, Sweden and puts it into the Debian Archive, which is distributed on mirrors that are all around the globe, and then it suddenly gets re downloaded into France?

Where does that happen? And is it, who's responsible, who's going to get stopped the next time that they change planes in Charles de Gaulle because they operate a Debian

mirror? Because they uploaded something to Adebian Archive while they were in France, what if they weren't French? There's a whole bunch of questions that this law poses for people who want to distribute the building blocks of effective infrastructure.

That Durov's arrest on those two charges in particular raises big, warning flags. Should I be worried as a Debian developer? I work on cryptographic software, and I help contribute and package that for Debian. I'm not responsible for all of that software. I'm in the middle between the folks who are working on it, full time, it's their focus on that particular software, and the folks who use it, which is many more people.

But should I be concerned next time I travel through France that I've actually helped to distribute free software into France that happens to have cryptographic capabilities that are not limited to authentication? And and I don't know, it raises these questions that that are pretty worrisome if we want a functioning, widespread, auditable ecosystem of cryptographic communications.

**Greg Nojeim - CDT:** We don't have the French prosecutors on the call but it sounds like you have some concern and Noémie, should people be concerned? People in Dan's position, should they actually be concerned? Has the prosecutor sent any signals not about Signal, about what their intent is with this law, or this suite of laws?

**Noémie Levain - la Quadrature du Net:** Again, about the cases that were just described, I think it's not yet. The one that the prosecutor will look for, but still as it's legally possible, you may not know, but as I was saying before you got here, Daniel, that the law, this law of registering the one that was used against Pavel Durov, it's an old law that nobody actually cared about because it wasn't reinforced, and also because it doesn't fit how actually encryption works in the world as it's a freely used, distributed and developed, but we see it can be used as a like legal weapon against some, someone that is that is designed as an enemy of the state. And here it was Telegram and Pavel Dubrov.

So even it was firstly for content moderation, we see that this old law can be used as another option. So I would say that still, you have to consider this law in the political context of Telegram. Maybe the charges on this ground will be dropped, maybe not, and if not, I think this is the thing. If the charges are not dropped on this, we will need to be very careful on how the judge will appreciate it because I think it will be one of the first time.

So it can be a legal precedent and then help us consider if someone is in danger when they come to France in Charles de Gaulle. But again we need to be I would be more worried about the general context in France about encryption and about criminalizing everyone, everyone that is using an encryption tool, whereas as being worried of people being developing them.

Right now the attention is more when we see a lot of criminal cases, they are fetching for people using it. And also being worrying about, I talked about it very briefly, but there's a cases of what happened with KICC, with AnchorChat, and what is the French police technical means right now, it's very difficult to know, but it seems that they are quite strong and that will be my point of attention.

**Daniel Kahn Gillmor - ACLU:** Yeah I agree with you, Noémie, that there's a strong concern about what the technical capacities to break cryptographic communication is for law enforcement agencies and not just for the French. As an American, I'm concerned about the American capabilities as well as, capabilities of American adversaries or American allies.

And the other strange thing is that for a nation, for nations that adhere to at least the that claim to want to encourage people to freely communicate and to have free association, these are ideals that are enshrined in the American Constitution, to be, for the government to hoard the ability to break people's communication.

If the communications tools are working well, even the vendors of the communications tools should not be able to reveal the contents of the communication. And to the extent that the nation states are discovering vulnerabilities, failures in those tools, or in the tools that surround them, to be able to break into that communication that puts the government at direct odds with the needs of the citizenry and the people who depend on that infrastructure, right?

It's if you were to know, oh there's a brick that if I pull out, I can knock down this bridge. But let's not fix the bridge, let's leave the brick there so that when we want to, we can pull the brick out and have the bridge collapse. But people need to use the bridge, and the government should be in the business of making sure that the infrastructure of society is functional.

for the goals that we want. So I agree with you that we have a, it's a very strong concern about what the technical capabilities are. I wanted to address your point though about whether, the fact that this law has been very minimally enforced previously. That kind of selective prosecution happens in the States as well.

And it troubles me to see if you if it's used as a weapon against the enemies, imagine the charges against Durov around the content moderation charges. Imagine those don't pan out for whatever reason. They could still continue to prosecute him in the same way that in the US, we went after Al Capone for tax evasion when what we were trying to go after him for were charges around being a mobster and getting people killed.

I don't object to going after people for tax evasion. We should go after people for tax evasion generally. But if you have a law that effectively criminalizes what's otherwise reasonable conduct, Then prosecutors can, and prosecutors can use it at their whim if everyone is being criminalized or if a class of people are being criminalized just for the

sake of, trying to help the global infrastructure function but we're just going to use it to pick off specific people.

That seems like a problem to me. That's not a situation that I would want us to be in generally.

**Greg Nojeim - CDT:** I'm going to turn now to some of the questions that are showing up in the chat and in the Q&A. We can't get to all of them, but let me just start. Joe Hall from ISOC asks, It seems like export/import control is really a relic of the past for cryptography?

Is there a legitimate modern rationale for controlling encryption or other types of privacy enhancing technology like differential privacy? It's not controlled, but if there's encryption in your solution, Like secure multi-party computation, etc. Then you have to send a note to France and a copy of your source code if they ask for it.

That's what the law says, that they can ask for the source code too. Is it a relic or is there a legitimate modern rationale for controlling encryption?

**Daniel Kahn Gillmor - ACLU:** I'm not sure whether relic is the term that I use, but I would say it sounds singularly unfeasible to ask for export controls. The source code is a relatively small amount of data. I'm not as concerned about the idea of requesting the source code. I tend to prefer that the source code for my communication systems be completely open and visible and modifiable for that matter.

That's the sort of the essence of the free software promise is that the users are in control. But the idea that you would effectively prevent its transfer, these are a small number of bytes. It's a very small amount of data that provides this capability. And to think that you can actually keep it from leaking across borders at this point seems implausible to me.

It's saying, we're fine with you doing math, but if your math involves, long division is out of bounds. We don't want you to talk about how to do long division yet. Without letting us know that you're doing it. And, that's just not plausible.

Long division falls out from other pieces of mathematics that you're going to do, just like cryptography. Now, I give the French decree of 2007 some credit for carving out cryptographic services that do only authentication and verification. from services that do encryption. At least they didn't try to block us from verifying software updates without first checking in with the authorities.

Right? That's good. They at least saw that you couldn't do that. But once you have the tools to do cryptographic authentication and verification, which, by the way, are

necessary to do strong cryptography, you need to know who you're talking to. It's just not a big stretch to go from there to adding an encrypted layer to it.

These mechanisms are useful in, in, in all of these forms. So the, I just, I don't see the export control being something feasible to to operate. In particular, if the goal is keeping strong encryption out of the bad guy's hands, that's just not going to happen, right? Once you let the cryptography mechanisms in general, even setting, encryption part aside, once the cryptography mechanisms in general are widespread, you're not going to prevent the worst of the worst from using the encryption mechanisms.

So all you're going to do is prevent everyone else from using the encryption mechanisms. And as a result, who will have the weakest communications basis? It will be the general public. That seems counterproductive to me.

**Greg Nojeim - CDT:** So there was a question in the chat that I want to highlight for, I'm sorry, in the Q& A that I want to highlight.

I'm not sure if anyone has the answer, but the question is there a punch list of bad encryption laws globally? I. e. Let's get this French law changed. But what's next on the list that needs to be changed? It's, I haven't seen that. Is there such a list?

**Noémie Levain - la Quadrature du Net:** I don't know, I don't know if you mean globally or in France, but globally, I don't know. Me in France, I also follow what's going on at the European Union level. I also know that there are some attempt in the European institution to undermine encryption that that is coming.

But right now if there is a list of existing law to punch, I actually don't know if there are some other targets to spot and to make better. Maybe Daniel, some or...

**Daniel Kahn Gillmor - ACLU:** I was hoping to defer to you since you have the legal expertise, Noémie .

**Greg Nojeim - CDT:** This actually sounds like something that we ought to put together at the Global Encryption Coalition, if we can.

**Daniel Kahn Gillmor - ACLU:** I agree.

The challenge is that no one... I don't have legal expertise within the US legal system as a technologist, that's not the expertise that I have. And the folks who do have legal expertise in one legal system probably don't in the other 180 legal systems that are out there.

So it's, it would need to be a collaborative effort and of course, there will be some nation states that we simply won't be able to budge. But, identifying some of the

common patterns, identifying the similarities would certainly be useful. And as Noémie mentioned, there are multiple pending attempts, this has been going on ever since the crypto wars of the 1990s, to add these laws, right?

So we should not only be, we should not only have the punch list Bad laws, but bad proposed laws, because those need ongoing swatting back. Within the U. S., the language that comes from law enforcement is this sort of going dark debate, and it gets tiring. We've had this debate for a long time.

It doesn't seem to change all that much. And, the ultimate, the underlying trade offs are whether we want to have a society where people can communicate without worrying about interference from a third party. Whether that third party is law enforcement or criminal adversaries or industrial espionage or chilted lovers or whatever.

**Greg Nojeim - CDT:** It strikes me that it would be really hard to put together this list because there's the laws that explicitly control encryption that they say you can't export it or they say you must register. But then there's also the laws that make it so that offering an encrypted service becomes risky.

Because you can't moderate the content as well when you can't see it and a lot of governments are talking about imposing duties of care on the platforms that are difficult to shoulder. when you can't actually read the content. One question asked in the Q& A was, to what extent is encrypted messaging a canary in the coal mine?

Kind of an early warning sign for other security technologies like TLS. That is the Durov case, it's a dispute between the state and a software provider because of what people are sharing on the platform. I think that's probably right. At what point does this kind of pressure? push down from the application layer to coerce content, to coerce other actions.

**Daniel Kahn Gillmor - ACLU:** I can speak to that from the cryptographic protocols perspective. So we have definitely seen attempts to get the lower level cryptographic protocols to provide additional features for the purposes of wiretapping. And in the U. S. we have the CALEA legislation. The CALEA is Communications Assistance for Law Enforcement Act,

and it basically mandates that you have backdoors in telephony mechanisms. Which does not include TLS, fortunately. But those mandated backdoors have been forced into telecommunications equipment by the U. S., and those telecommunications equipment backdoors have themselves been the sites of numerous compromises, including, you can go back to the Athens affair in 2005, where parties other than the law enforcement agencies that are asking for these features have gotten in and compromised people's communications.

The wiggle room that you're talking about, identifying bad laws, Greg, is tricky. I've only read a translation into English of the French decree in this case, so I don't know how accurate it is, maybe, knowing that you can speak to that, but it seemed to have some carve outs about the declaration being marked as acceptable or unacceptable by ANSI, on the basis of whether it put at risk national interests or national security interests or something like that.

And that's a big... when I hear the words national security, I worry because those are used as a stalking horse for whatever agenda people are pushing. So Noémie, I don't know if you can speak to those those carve outs there.

**Noémie Levain - la Quadrature du Net:** I don't have all the decree in mind, but it's true that as you, you have the right on the spot, every time there is national security exemption or objective, it is a way to, to enforce some very intrusive measures, but In France, it's very, I don't know what will happen next, because you see a lot of political intention to attempt to encryption, asking for backdoors, but also the ANSI, so it's like The cyber security agency there is tension between government and ANSI because ANSI will keep on saying if you undermine encryption for criminal procedures, you undermine encryption for everyone and for a lot of other technical layers, et cetera.

So the tension, as you said, has been going on for years and decades but we see, right now, more efforts. And the thing is with in a messaging encrypted app is that they have this image in the media political world of being some bad guy tools. So this is why they go to their first. To this kind of tools first every time you read an article about, I don't know, some gangs, they say that they were using encrypted apps, even if has, if it has nothing to do with the thing.

So you can see that it got worse in the, in the, narrative is the imagination and this is why we are worried because if the narrative goes on first, then it's easier for the government or the judge to, to say it's part of the crime, it's complicit, etc. So we see that they are going to.

They attack it first and maybe they will attack other kind of other layers after. And I'm trying to remember the other part of the questions but again, oh yeah, about national security actually as as I said, the decree, this kind of old decree is not very enforced, so we don't have a lot of precedents yet, but and the Durov case, it's not about national security, but about general criminal, how is it in English? But major criminal offenses.

But you were talking about the going dark and all the attempts going on at the European level or France. It's always national security that is that is that is. Putting put first by, by the government and then we have, we cannot do anything towards that because it it's the excuse for all the exemptions and all the attempts.

And so right now, the tension I was talking about between the ANSI and the government, it's holding, and encryption is still preserved, but we don't know what will happen in the next few years or months coming.

**Daniel Kahn Gillmor - ACLU:** I want to say, Greg, I wanted to mention one other thing. And your question is about, these bills that are being proposed that might end up making it challenging to meet the goal of the bill without removing encryption from a service.

And in the US, some of those bills have explicit carve outs that say nothing in this bill shall be construed to require you to remove encrypted communication. And yet, when you read the plain language of the bill, I don't know how you would do that without removing the end-to-end encryption.

And so it really is a question of like, how do we...? The folks who are drafting the bills are aware, which is good. That's a better situation than we've been in the past, that they're aware that they don't want these negative side effects. But I don't know how to read the bills clearly or who's going to be interpreting those bills, when push comes to shove.

**Greg Nojeim - CDT:** Yeah, it's a real problem. It's a problem in the U. S., problem in Europe, problem all over the world. Listen, we're at time, and we're going to have to wrap up. I will say this though we'll be following the Durov case at the Global Encryption Coalition.

If there are significant developments, Noémie, keep us posted and we'll keep the whole world concerned about encryption posted. I want to thank Dan and Noémie for joining us today and thank you all for signing in to listen in, and thanks to ISOC for doing the logistics for the Global Encryption Coalition for Global Encryption Day.

And I'd like to sign off and say goodbye to everyone.

**Noémie Levain - la Quadrature du Net:** Bye.

**Greg Nojeim - CDT:** Thanks all.