DEMOCRACY, NARRATIVE DISPUTES AND SECURITY CONFLICTS IN ENCRYPTION POLICIES

INTERVIEW WITH RIANA PFEFFERKORN

LAW AND TECNOLOGY RESEARCH
INSTITUTE OF RECIFE – IP.REC

PRESENTATION

The present interview was conducted by the Law and Technology Research Institute of Recife - IP.rec, an independent research and advocacy center focused on social, ethical and legal impacts related to technological development.

The Institute's work began in 2017 and, since then, its team has been involved in the elaboration of scientific studies, case analyzes, campaigns, events, and actions that contribute to the construction of knowledge and critical sense about the functioning of digital networks.

The interview with Riana Pfefferkorn was conducted by André Ramiro, director of the Law and Technology Research Institute of Recife - IP.rec, between June and August 2020.

Recife - Brazil, October 2020.

IP.rec
INSTITUTO DE PESQUISA EM
DIREITO & TECNOLOGIA DO RECIFE

RIANA PFEFFERKORN

Currently, Riana Pfefferkorn is one of the main voices in the defense of encryption and in the analysis of surveillance policies that put at risk network security and fundamental rights. She is Associate Director of Surveillance and Cybersecurity at the Stanford University's CIS - Center for Internet and Society, where she investigates public policies and practices of the U.S. government that seek to decrypt data and communications or influence, through technical, legislative or judicial means, the architecture of platforms and services with regard to encryption.

Riana Pfefferkorn has been a strong opponent of anti-encryption proposals by U.S. government law enforcement. She has published analysis, white papers, reports and participated in public hearings in the scope of bills and judicial cases on topics ranging from proposals for backdoors, exploitation of vulnerabilities in applications and Internet services by law enforcement agencies and guarantees of fundamental rights within criminal investigations.

The themes that orbit encryption policies, as discussed in the interview, cover the central role that technological security currently assumes for the global economy and for the resilience of connected networks. Questions about the legislative and law enforcement approach, when it comes to technology policy, were also addressed, as well as the centrality of strong encryption to the exercise of political and fundamentally democratic rights. And, for sure, much more. Good reading.

INTERVIEW

Question: *Riana, thank you so much for accepting our invitation. Your view on this matter is a reference for decision makers, service providers, and encryption advocates in a variety of regions. We think your experience is very valuable for us to contextualize, from a geopolitical perspective, the debates that are taking place in Brazil and Latin America, also considering the long time dispute around encryption in the U.S.*

So let's start with the basics on this matter. Encryption is at the front line of electronic information security development for at least half a century. With the proliferation of Internet services and applications, alongside with the exponential rise in number of users and devices, it is, like never before, a cornerstone for network security and trust. At the same time, freedom of expression, as well as the exercise of a broad range of political rights in a connected reality, relies considerably on the privacy provided by encrypted protocols. Thus, we can assume that the encryption is directly related to democracy nowadays. Nevertheless, we see public policies in some countries trying to weaken encryption security in the name of investigative and surveillance powers. Of course there is a range of layers in the political science towards encryption policies, but do you think those policies are being proposed because of a lack of technical literacy, or there is a conscious security choice being made by those state actors? How do you see this scenario?

Riana Pfefferkorn: Thank you for this excellent summary of the situation. I believe these policies have several motivations. Many law enforcement officers and policymakers likely do not have the technical literacy to understand how encryption works or the risks of weakening it, just as you suggest. Anytime lawmakers turn their attention to technology, lack of technical understanding can be expected to be an issue. However, some lawmakers have staff members who are highly technically literate and can explain the technology and the risks to them. Likewise, law enforcement agencies may also have members of their staff who are technically competent and whose job it is to try to unlock phones, decrypt data, etc. So while lack of technical literacy is surely an issue, it is not the only explanation for why policymakers and members of law enforcement continue to make policy proposals to weaken encryption.

For those who do understand the technical reasons not to weaken encryption, yet make those proposals anyway, I think there may be several motivations. One is that they understand the risks of weakening encryption, and believe that the trade-off is worthwhile. They know that weakening encryption puts everyone's data at risk, and that "a backdoor for the good guys" will also be discovered and exploited by the bad guys. However, when they weigh that expected downside against the expected benefits of weakening encryption, in terms of detecting and investigating criminal activity and gathering evidence, they decide that they are OK with that trade-off.

Members of law enforcement in particular might be OK with that trade-off, because their job is fighting crime.

Policymakers have to think more broadly -- not just about crime, but about the economy, about national security, about people's fundamental rights -- all things that encryption protects

But also, every policy choice involves trade-offs; some will win and some will lose. Policymakers' job in crafting policy means they are always thinking about trade-offs and coming to hard decisions about trade-offs. And meanwhile they are also always under pressure to get re-elected, which influences where they come out on these policy decisions. If they believe they have a better chance of getting re-elected if they are "tough on crime," then they may decide the downside of weakening encryption is acceptable, because they think that voting to weaken encryption will make them look tough on crime. (Never mind that weakening encryption will enable more crime, perhaps more than it prevents or solves.)

So, there may be policymakers out there who understand the risks, and they look at encryption as a "security vs. security" choice: making law enforcement investigations easier on the one hand, versus strengthening protections for national security information, economic security, individuals' safety (for example, to keep abusive spouses from accessing their phones), etc., on the other.

And perhaps one side of that "versus" is just more convincing. The kinds of crimes on one side may seem more important than the kinds of crimes on the other. For example, "we cannot get into the phone of this murder victim, or this terror suspect" sounds absolutely terrible, while perhaps "encryption is necessary to protect people's banking information" might just not seem as important when compared to a murder. I think when the police can tell stories about really terrible crimes that they can somehow tie to encrypted devices or encrypted messages, that is very persuasive. So some of what's going on in these policy choices might be that policymakers understand the security trade-offs, but law enforcement tells more persuasive stories.

And finally, I think that among some law enforcement officers and some policymakers alike, they really do not believe that people should have privacy, and they really do believe that the police should have a huge amount of power. Just this week, there was a new bill introduced in the U.S. Senate that would basically make strong encryption illegal. One of the sponsors, Senator Tom Cotton, recently published an op-ed in the New York Times, the top U.S. newspaper, which said that the military should be sent in to quell the protests that have been going on in the U.S. for weeks to protest police brutality and systemic racism. To him, peaceful protesters deserve to be treated like enemies on the field of war! It is no surprise that someone like that would support a policy to make strong encryption illegal.

To him, protesters and people who exercise their constitutional rights are criminals, and the police and the military are the heroes.

> *Someonelike that, who favors a police state, does not care about the security trade-offs of weakening encryption. He cares about keeping citizens from having real privacy and about giving more power to the police*

Q: *When you talk about the Senator's actions - and I would like to come back later on the intersections between backdoors and social inequalities - I can't help to notice another similarity of your considerations with the Brazilian context in terms of punitivist agendas of both countries. With the election of a far-right wing president in both cases, these voices are louder than ever, and thus the criminal framing of political rights by those actors is reflected in tech policy. For instance, for the last three years, two of the last former Ministers of Justice, both related to the conservative sector and openly committed with being "tough on crime" (one of them now a Brazilian Supreme Court judge and another a former judge), have lobbied for backdoor bills within the parliament. Would it be possible to draw patterns between the backdoor crusade and a conservative tendency in public policies in the U.S. (and abroad)? Or it also appears within more progressive political perspectives?*

It's interesting when you talk about lawmakers turning their attention to technology. I would add that when it happens, the resulting policies, *including backdoor proposals, often appear in the rush and heat of social sensitivity. Otherwise, I believe, people wouldn't be likely to accept increasing surveillance at the cost of disrupting constitutional rights. It happened, for instance, with the Suzano episode in Brazil (a 2019 School shooting that turned attention to the dark web). The case will appear, e.g., as one of the reasons for a Brazilian bill that proposes the obligation of content and communications constant monitoring by service providers. How the San Bernardino and Pensacola episodes, for instance, were used as narrative resources for backdoor proposals? How are the authorities dealing with those kinds of crimes in terms of pushing the parliament towards interference on encryption?*

RP: I think what "conservatism" looks like in America now is much more far-right and extremist than what "conservatism" used to mean, under for example President Ronald Reagan in the 1980s. Some of the more "classic" conservative themes are (1) individual liberty and (2) for businesses to be free from government regulation. Those ideals would seem to translate into support for strong encryption, because strong encryption helps to preserve individual liberty (privacy, freedom of expression), and because regulations on encryption would restrict the businesses such as Facebook or Signal that offer it and harm their economic competitiveness overseas. Those traditional conservative values are why we have some Republican members of the U.S. Senate, such as Senator Mike Lee of Utah, who are pro-encryption. They are rare, but they exist!

And yet, there is another value of conservatism, both in America and I suspect elsewhere -- which is a strong police force, "law and order," generally a very paternalistic and ultimately violence-backed way of organizing society. This "law and order" slogan has been a theme of American conservatism ever since President Richard Nixon in the '70s, and it means that politicians on both sides of the aisle feel they must act "tough on crime." So, that kind of conservatism -- one that values the police's ability to intrude into people's lives in order to enforce the laws and keep public order -- is what we see at play in anti-encryption, pro-law enforcement stances.

That attitude is a hallmark of American conservatism. We see this in the newly-introduced "Lawful Access to Encrypted Data Act" bill that was sponsored by a group of Republican senators, with no Democratic co-sponsors. But, the "law and order," anti-encryption, pro-backdoor attitude can appear in what passes for "progressive" politics in America too, which means our Democratic party. As said, even many Democrats have traditionally been afraid to be seen as "soft on crime" -- though perhaps that is changing in a time of mass protests against police brutality and calls to put an end to the way we currently do policing in the U.S. That shift is largely driven by younger people. To keep up with popular opinion, the Democratic party may need to start acting less pro-police. Even so, the unpopular "EARN IT Act" bill was introduced by a bipartisan group of both Republican and Democratic senators. At least one of the co-sponsors, Senator Blumenthal, used to be the attorney general of his state, though -- so it is not so much of a surprise that he would co-sponsor that bill.

Overall, American politics has shifted to the right during the past 40 years. The Republican Party platform of 1980 would sound almost left-wing by today's standards. So overall it sounds very "left of center" for a politician to stand up and say, "Hey, privacy is a fundamental human right, and that means private communications that cannot be policed are also a fundamental right." I am hopeful that today's youth movement, the police protests, and the Black Lives Matter movement can help to swing public policy more to the left in the U.S. The people who have been hit the hardest by police surveillance in the U.S. are people who are Black, brown, poor, etc.

> *They understand firsthand how violent the "law and order" attitude is in its implementation, and they understand firsthand the value of secure private communications and devices*

If policymakers listen to them, and if they have to be responsive to those communities' concerns in order to win their votes, then maybe we will see a bit of a shift in this conservative attitude towards encryption. So far, though, it is really hard to find many politicians in the U.S. Congress who will stand up for encryption.

2 - The Attorney General (who is the head of the Department of Justice) and the Director of the FBI [Federal Bureau of Investigation] at the time of the Pensacola attack are not the same as the AG and FBI Director at the time of the San Bernardino attack.

But they all responded the same way, which was to use those attacks as rationales to argue in public for backdooring people's devices. But the Attorney General's and FBI Director's calls for encryption backdoors following the Pensacola attack did not get nearly as much popular or press attention as the San Bernardino episode did. I think that is because the FBI actually took Apple to court in the San Bernardino situation, but as far as we know, it did not do so with the Pensacola attack. In both cases, law enforcement was ultimately able to crack into the shooters' phones, which undermines their argument that backdoors are necessary. But the fact that law enforcement has these capabilities does not stop the A.G. or the FBI Director from calling for backdoors anyway.

I think it came as a surprise to the Department of Justice and the FBI that the San Bernardino terror attack did not cause the American public to uniformly and instantly take the side of the police and against Apple with regard to encrypted iPhones. There had been predictions by senior members of government that if a terror attack were to happen that could be blamed on encryption, then public attitude would become much more hostile to encryption. That didn't necessarily happen in public opinion after San Bernardino. Unfortunately I would say it did happen to some degree in Congress. Law enforcement agencies have the ear of congressmembers; average people who benefit from encryption do not, so congressmembers only listen to average people when they get a whole lot of phone calls or emails about a particular issue or bill, or when they think they need to do what average people want in order to get their vote, as I said before.

Anyway, shortly after the FBI was able to open the San Bernardino shooter's iPhone, in 2016, two senators, Dianne Feinstein (a Democrat) and Richard Burr (a Republican) introduced a bill that would have penalized smartphone manufacturers that did not build in a backdoor to permit law enforcement access upon receipt of a court order. That bill didn't go anywhere. But I think that the San Bernardino attack and the Pensacola attack were both motivating factors for the current anti-encryption legislation that we see pending in the Senate now.

With that said, I think terrorism by Islamist extremists does not necessarily scare the American public now as much as it used to, nearly 2 decades after the 9/11 attacks, as our "War on Terror" drags on endlessly forever. While there have been terrorist episodes such as San Bernardino, Pensacola, etc.,

A lot of the terrorism we have seen in recent years in the U.S. has been committed by American-born white supremacists. I think that fact is pretty awkward for the Attorney General and the FBI, because they can't play on nationalism, racism, xenophobia, Islamophobia as ways to convince the public that encryption is bad because terrorists use it. So we don't hear them talk about terrorism as much anymore, except in instances like Pensacola.

Now, since sometime in 2019, it is all about child sexual abuse online. This has been an ongoing problem for as long as there has been an Internet; there is no "9/11 of child sex abuse". It is not a shocking individual incident the way San Bernardino or Pensacola were. But terrorism is rare, whereas online child sex abuse imagery is a problem continually. That is something that federal law enforcement has used to strengthen their calls for backdoors. Instead of saying "we should backdoor encryption because of a rare problem" (terror attacks), law enforcement can say "here is an ongoing problem."

Plus, child abuse is something that everybody despises, no matter what their political leanings. It is a bipartisan issue. So now we see the AG and the FBI focusing much more heavily on child abuse instead of terrorism as the reason for backdoor proposals. Honestly, it is a surprise to me that it took so long for them to use child abuse as the rationale. I wonder why they didn't do so earlier.

With that said, I forget if I mentioned it before, but my experience of traveling to Brazil and other countries, and being involved in other countries' encryption debates, has been that there will always be some kind of crime that the government will use to rationalize its call for encryption backdoors.

> *For Brazil, it has been Car Wash, corruption, and elections. Here in the U.S., it has been terrorism and child abuse. The goal everywhere is the same: encryption backdoors*

It is only the reasoning that varies. The people who want backdoors will figure out whatever reason they think will get public opinion -- or, more importantly, lawmakers' opinion -- on their side, and that is what they will use. Once terrorism stopped being so influential on the American public, suddenly it was child abuse that backdoor advocates were focusing on. Even if Car Wash is always ongoing in the background, a special event such as an election can be used as the occasion to call for backdoors in WhatsApp. It is simply variations on the same tune.

Q: *It's interesting because when the crack is made possible by a contracted service, as those offered by Cellebrite or Grayshift, it seems to me that there is an additional cost, in terms of due process, for law enforcement agencies and, maybe, they lose some of the scalability potential (in other words: mass surveillance power) compared to the possibility of a systemic use of backdoors. But talking about due process and cracking lawfulness, is the debate, on some level, moving gradually towards government hacking practices?*

How can we analyze those practices policywise and in relation with human rights protections, encryption, and, ultimately, with the risks to information security as a whole?

RP: Yes, I agree that the use of Cellebrite/Grayshift devices -- instead of backdoors -- means that law enforcement is constrained to only crack into phones in specific cases. We could call this "tailored surveillance" rather than "mass surveillance." And when we are talking about Cellebrite & Grayshift devices, we are talking about equipment to crack into a particular smartphone, which requires law enforcement to have possession of the device. But the other side of "government hacking" is remote hacking -- where law enforcement (or the companies they contract with) uses an exploit to gain remote access to the target. The hack could be of a phone, as when NSO Group (on contract to various world governments) has hacked people's phones, using its own Pegasus software, or, in some instances, using a WhatsApp vuln. Or it could be of a web browser, as in the instances when, in order to uncover the user's true IP address or other identifying information, U.S. law enforcement has exploited a flaw in the Tor browser, hacking thousands of people's browsers via a "watering hole" attack[1] on visitors to a server that the police had seized, which was running a Tor Hidden Service for child sexual abuse imagery.

So there is some part of the debate that is about government hacking, which some experts and commentators consider to be a preferable alternative to mandatory backdoors, because there will always be flaws in software/hardware and because the tailored use of such flaws is less damaging to privacy, security, and other interests than a mandatory backdoor, which, as you say, opens the possibility of systemic mass surveillance. And yet, as I have written, government hacking comes with its own set of security risks, not to mention the impact on human rights when governments hack their own citizens, as the NSO Group saga has revealed. But

> *the practice of government hacking has gotten out ahead of legal restrictions on law enforcement use of this tool. The technology has moved faster than the policy, as is often the case when it comes to new technologies*

[1] An attack in which a website is modified, for malicious purposes, while the attacker waits for the victims to enter and thus infect them with a malware or exploit their information.

UN Special Rapporteur for Freedom of expression David Kaye has called for a global moratorium on the use of malware by governments, precisely because there is such widespread use without a lot of legal restriction -- and often in secret, with governments denying any involvement when, say, NSO Group campaigns against human rights activists or journalists or dissidents are uncovered.

In the U.S. we have the "Vulnerabilities Equities Process," which the federal government uses to decide whether or not to disclose a vulnerability that it has learned about. If disclosed, the vendor would patch the vuln and then the government could no longer use it offensively. This is a useful process to have in place, and I hope other governments adopt something similar. But my worry is still that these processes are not taking account of all the different stakeholders, especially human rights. Governments will tend to prioritize their own people's rights over those of others, and to prioritize national security, and I am afraid that human rights may not be taken as seriously as it should be in these discussions. We have international human rights frameworks in place that governments should bring into play when regulating the use of hacking by law enforcement.

Q: *I think you raise some facts that involve, fundamentally, encryption geopolitics between States and the private sector as well as between different governments that are related to international networks for surveillance purposes. These cooperations are sometimes more subtle (and yet very eloquent), as statements by the G7, Five Eyes, or even between the U.S. and Brazil (the latter having held a "Going Dark" Symposium [sic] last year). It seems that while the U.S. has no success in passing a backdoor law, it engages and encourages other countries to do so. How do you see these international "soft power engines" around anti-encryption policies, especially after you covering for years the policymaking in the U.S.?*

I have no specific knowledge of whether US policymakers and law enforcement officials have actually met with their counterparts from other countries and actively encouraged them to pass a backdoor law. However, I would not be surprised to learn that there has been such action, since, as you mention, we have seen "joint statements" on encryption that the US has joined. I think the "soft power" of the US may work in multiple ways. A difficulty here is that the US government is not one monolithic entity, and different parts of it have had very different opinions of encryption. While US federal law enforcement agencies are anti-encryption, the intelligence agencies are very dead-set against encryption backdoors because they see how the risks outweigh the benefits. Also, you may recall that the US State Department's "Bureau of Human Rights, Democracy and Labor" helped to fund Tor.

Historically the US State Department has tried to help promote democracy around the world as part of the US's exercise of soft power, and you can see how funding censorship-resistant technologies plays into that.

So here we have multiple parts of the US government whose interests are not all aligned when it comes to how to exercise US soft power on the encryption issue. But those parts are not all on equal footing right now. Under the current administration, the US has lost much of its standing in the world as a beacon of democracy. The State Department has practically been gutted, so it exerts less influence. That leaves the US intelligence agencies and law enforcement agencies, whose approaches to encryption are in tension. Understandably, the intelligence agencies are not usually out there holding press conferences. I don't know how they exercise soft power, but between them and the law enforcement agencies, it's obvious that the latter are the louder voice, at least when it comes to encryption.

With law enforcement's voice dominating, and the State Department's reduced to a whisper, the US is no longer setting an example of democratic values, and we have abdicated much of our moral standing to object whenever other countries pass laws -- such as backdoor laws -- that are inconsistent with democratic freedoms. The US's waning influence abroad also means that other countries can be the ones to set the example for the world, whether that example is good or bad. So

> *When Australia passed their anti-encryption law in 2018* (modeling it on the UK's 2016 "Snooper's Charter"), *they could say "we are a democracy, so this is a democratic law." And now, every other country -- whether it's the US, or China -- can point to Australia and say, "look, they're a democracy and they passed a backdoor law, so that must mean backdoor laws are OK"*

The utter abdication of US leadership on the global stage over the last 4 years seems to me to be a net negative for the rest of the world, even though on this one particular issue of encryption, the DOJ is probably happy with that outcome. Now, it looks more normal and acceptable to introduce a backdoor bill here: the Lawful Access to Encrypted Data Act bill introduced in the US Senate in June. The DOJ will now be able to say "of course this law is OK, it's just like laws passed by our close allies, Australia and the UK." In the past, you'd think it would be embarrassing for the United States government (which of course is very self-important and egotistical) to imitate what other countries are doing instead of being the leader. But it seems it is the policy of the United States not to be a leader anymore.

Q: *Riana, finally, I would like to get back to the social value of encryption for democracy. As you mentioned, the people who have been more targeted by police surveillance are those who are the victims of historical and systemic inequalities, like politically misrepresented sectors, such as the black movement, and also ethnic minorities or political dissidents. It has been well documented the* *illegal wiretapping culture and profiling of organizations and individuals, such as journalists and activists, by governments around the globe, even those considered democratic. Is it correct to say, in your opinion, that there are intersections between the mass surveillance rationale and the will to prevent any substantial social change in the status quo by eavesdropping on social movements? Where do you think encryption is historically placed in the fight for human rights? And at last, would you be able to make any predictions for this scenario in the near future?*

RP: I believe that eavesdropping on social movements is a tactic that governments, at least in the U.S., have deployed for decades as a way to monitor what they consider a threat to the state. Ultimately the state exists not to protect and serve its own populace, but instead to protect itself and perpetuate and extend its own power. Any popular movement for social change is, as you say, a threat to the status quo of the state's existence, the form it takes, and the scope of its powers. So yes, I believe that mass surveillance takes place in part in order for the state to keep tabs on these potential "threats."

> *I believe this is part of why governments hate encryption so much: because it gives more power to the populace and takes power away from the state, and makes it harder for the state to spy on the populace*

We can see even now, with popular protests in the U.S., that members of the government -- from law enforcement officials to even the presumptive Democratic presidential nominee -- equate political movements (such as Black Lives Matter, antifascism, and anarchism) with criminality and terrorism. In their view, there is no difference, and thus, if backdoors for encryption are necessary to keep tabs on criminals and terrorists, it thus makes sense that the government also wants encryption backdoors in order to monitor these political factions that pose a threat to the status quo.

For all these reasons, I believe that encryption is a tool unprecedented in modern history for helping fight for human rights. By threatening encryption, governments are threatening human rights, and I am sure that they are very well aware of this and are still deliberately proceeding with their anti-encryption agendas. We need strong encryption in conjunction with other tools that have proved highly useful: a big part of the global population now has a video camera in their pocket, and there is a huge amount of storage space in the cloud that is accessible for free. Storage is no longer expensive, recording video and photos is no longer hard; all these tools have been democratized. That helps to document and preserve evidence of human rights violations. And the existence of free, global communications platforms has also made it easier for people who are fighting for human rights to contact each other, organize, share their experiences, and share tips with each other -- whereas previously phone calls even to another part of the country were expensive, much less another country, and "snail mail" is very slow.

But of course, many of these tools for protecting human rights -- including encrypted messaging apps and devices -- exist because private-sector companies provide them. We depend on these companies to keep providing those tools, which means we are vulnerable to their decisionmaking and policies -- whether they create those policies on their own, or to comply with local laws (such as encryption backdoor laws). Even when small nonprofit organizations create and produce tools -- remember, Signal is made by a nonprofit -- we are still at risk of losing them because it is so easy for nonprofit orgs to lose funding, lose momentum, and stop supporting the tools they create. We have seen this happen with tools for documenting human rights violations. It could happen with encryption tools as well.

In the future I do believe that governments around the world that are enemies of strong encryption will make advances in terms of passing laws to weaken encryption, and I predict that the (mostly American) companies that provide strongly encrypted products and services will bend under pressure and comply with those laws. That will not mean the technology goes away, but it will be harder to find, and people who need the protection of encryption will have to be more intentional about seeking out and downloading those tools. It won't be easy because companies like Apple and Google will kick apps out of their app stores, on a country-by-country basis, that do not comply with applicable laws. And anyone who does seek out and download those tools, outside of the app stores, then may be at greater risk of being noticed and targeted by the state. There will be risks to you if you no longer seek out and use strong encryption, and there will be risks if you still do.

So I do not think the future looks particularly bright for encryption on the level of global law and policymaking. But

> *I do believe in people, and in the power of people. We will find ways to protect ourselves and our communities even if governments grow even more hostile to us*

And in the meantime, I am continuing to do what I can to try to protect encryption from bad laws and bad policies.

IP.rec

INSTITUTO DE PESQUISA EM
DIREITO & TECNOLOGIA DO RECIFE

htts://ip.rec.br

https://www.facebook.com/InstitutoIP.rec/

https://www.instagram.com/ip.rec

https://twitter.com/institutoiprec