ICANN69 | Virtual Annual General - WHOIS Changes Under GDPR: Impact to End-Users and Public Safety
Wednesday, October 21, 2020 - 10:30 to 12:00 CEST

[This meeting is being recorded]

OZAN SAHIN: Thank you, and welcome to WHOIS changes Under GDPR: Impact to End Users and Public Safety plenary session. My name is Ozan Sahin, and I am the remote participation manager for this session. Please note that this session is being recorded and follows the ICANN Expected Standards of Behavior.

During this session questions or comments will only be read aloud if submitted in English within the Q&A pod. This feature can be accessed from the Zoom toolbar. I will read questions and comments aloud during the time set by the moderator of this session.

This session includes real-time transcription and interpretation. To view the real-time transcription, click on the "closed caption" button in the Zoom toolbar. Interpretation for this session will include Arabic, Chinese, English, French, Russian, and Spanish and will be conducted using both Zoom and the remote simultaneous interpretation platform operated by Congress Rental Network. Attendees are encouraged to download the Congress Rental Network app following instructions in the Zoom chat or from the meeting details document available on the meeting website package.

If you wish to speak please raise your hand in the Zoom room, and once the session facilitator calls upon your name, our technical support team will allow you to unmute your microphone. Please state your name for the record and the language you will speak if speaking a language other than English.

When speaking, be sure to mute all other devices, including the Congress Rental Network application. Please also speak clearly and at a reasonable pace to allow for accurate interpretation.

I would like to highlight that remote participants are not able to click on the microphone button and unmute themselves during this meeting without assistance from the technical support team.

For all participants in this session you may make comments in the chat. To do so please use the drop-down menu in the chat pod and select "respond to all panelists and attendees." This will allow everyone to view your comment.

Please note that private chats are only possible among panelists in the Zoom webinar format, and a message sent by a panelist or a standard attendee to another standard attendee will also be seen by the session's hosts, co-hosts and other panelists.

With that, I will hand the floor over to Jonathan Zuck.

JONATHAN ZUCK: Thanks. This is Jonathan Zuck, the vice-chair of the At-Large Advisory Committee. And as many of you know, the At-Large has sort of taken on DNS abuse and other related issues as a kind of campaign issue for the year, but I feel like a lot of these conversations have been kind of repetitive and haven't gone to anyplace specific. And a lot of that is a result of a lack of data. There's just a lot of rhetoric from all sides that makes a rational conversation about these topics very difficult.

And we've often seen within the ICANN context that sometimes predictions that are made in the heat of passion about a new policy don't come to fruition; that some other outcome takes place. For example, when the new gTLD program was first being proposed, it was suggested by Sony in a credential hearing that they would invest $12 million in defensive registrations, and they didn't end up doing that. They ended up finding another way to deal with protecting their trademark across these new gTLDs.

And similarly with the enforcement of the GDPR and the consequent wake-up call of the ICANN community, there was a scramble -- right? -- that led to the implementation of a temporary specification, the formation of an expedited PDP Working Group on how ICANN would comply with the GDPR regulation. And as a result, there's been a dramatic change to the data that's available publicly via the WHOIS system, and a new sort of system was put in place in which people needed to request information from contracted parties.

And so over the course of the EPDP process, for better or for worse there have been sort of the data managers and the data requestors that have become these two significant parties in those discussions.

And so the idea behind this plenary is to bring those parties together and to have a discussion about what's really taking place during this interim period. In other words, what level of data requests are being made and how are they being handled. It seems like we're often being surprised that the numbers are smaller than we think they are; that there weren't that many requests or there weren't that many complaints to contract compliance, et cetera. And so starting from a baseline of facts feels like a better place to be as we try to have conversations about registrants' data and its use.

It could very well be that the parties that were primarily concerned about access to registrant data have found alternative ways to get that information in order to enforce trademarks, to do law enforcement and consumer protection. And so it's trying to get at where we stand now, a couple of years later, in terms of that data, the need for it, its availability, the efficiency with which it can be gotten by the requestors from the contracted parties, et cetera. And that's what we're hoping to have as a conversation as part of this plenary, is really just a fact-finding mission about where things stand today, what's the status quo.

So hopefully we'll try to make a minimal amount of sort of ideological discussion and really maximize our discussion about data and the facts about what the status quo looks like.

To get the conversation kicked off, we're going to talk to -- get some perspectives from one of the requestor communities, if you will, which is law enforcement and consumer protection. And to that end, I'm going to give ten minutes to Laureen Kapin of the FTC and to Gabriel Andrews to talk about the law enforcement perspective, the need for this data, alternatives that have presented themselves, and what the process has looked like over the past couple of years.

So with that, I hand it over to you, Laureen.

Thanks. And you need to unmute.

LAUREEN KAPIN: It's still early for me, so a special welcome to everyone who is in a challenging time zone. And I'm sure the people who aren't, you're very grateful.

My name is Laureen Kapin, and I am here to give you a consumer protection end-user perspective on how the public uses WHOIS.

Can we go to the next slide, please.

I am an attorney if the Federal Trade Commission. I'm in the Office of International Affairs of Consumer Protection, and I've focused on these issues, as has my agency, for a number of years. But the views you're about to hear, they're mine. They don't reflect the official position of the FTC which speaks through its commissioners. So you're hearing from me, Senior Attorney at the Federal Trade Commission.

Next slide, please.

And I'm also co-chair of the Public Safety Working Group, who has been advocating on these issues for quite some time.

So the Federal Trade Commission has a wonderful resource where consumers and the public, not just in the United States but around the world, can file complaints when they have fallen victim or are concerned about a deceptive practice, fraud, or a scam. And that is called our Consumer Sentinel Database. And that database collects hundreds of thousands of complaints each year and has many contributors from all over the world.

And not surprisingly, when we look at those complaints, we can get a little bit of a photograph of how the public, Joe and Jane public who are going online to buy stuff, to meet people, to get information, how the public uses WHOIS, because the references to WHOIS are right in their complaints.

So what I did is I looked at a slice of those complaints, particularly after the changes to the WHOIS system went into effect. And when I say "changes," I mean those changes that masked certain information, particularly contact information for the registrant, the person responsible. And here's what I found. The end-users use WHOIS for a variety of purposes. But essentially they're looking for indicia of reliability. They want to look at the WHOIS records to perform due diligence also to follow up on suspicious or malicious conduct. They want to find out who's responsible. Sometimes they want to try and contact them. And sometimes I know from reading these complaints that they are investigating something mid-scam, i.e., they are on the phone with someone trying to figure out if they're being scammed or not. And they are going to their computer and looking at the domain that may have led them to this phone call.

Consumers had noted in these post-WHOIS changes that there is redacted or missing information in the record. And they may assume that the business is dishonest because of that lack of information. And that assumption may or may not be correct. And, by the way, the FTC receives these complaints. They don't verify the complaints. They just receive them and use them as a data point.

So folks have noted that details may be hidden and that that is interfering with their due diligence effort. For example, one person complained that there was no data for a public utility company. So you can see from this word cloud the ways that different people are using this, and these are terms that I found in the complaint -- in the complaints that I reviewed.

To give you a flavor, because we're trying to be pithy here and only have a few more -- a short time left. But to give you a flavor -- next slide, please -- of the types of scams that folks are using the WHOIS to investigate: Counterfeit goods, romance scams, puppy scams. You would be amazed how many puppy scams there are out there!

Next slide, please.

Invention scams, phishing techniques. And in the age of COVID, we also have coronavirus phishing scams. Tech support scams, government imposter scams, fake checks, job scams, a whole variety.

I also want to emphasize that folks don't just use the contact information in the WHOIS record. And to that extent, folks are fortunate because there still is some useful information there, such as when the domain was created and where it was created. So that's just a flavor for the way the end-user uses the WHOIS data to protect themselves essentially, and there is some frustration noted in these complaints that certain information is not available for that purpose.

And I'm going to pass the baton over to my colleague Gabe now.

GABRIEL ANDREWS: Okay. So next slide for me, then.

When I speak, I am speaking anecdotally on behalf of law enforcement. And I note that despite the plea for data, it is tremendously difficult to get good numbers from law enforcements about the times they're flustered by imperfect WHOIS access.

Further, law enforcement will tend to conflate multiple issues together. They might not always know better. But whether it's GDPR or the California Consumer Privacy Act or privacy and proxy services, in the end, all that really matters to the cop or to the investigator or the public safety official is that they're trying to get access to data and the data is not there for them.

So to talk about one of these issues is to talk about all of them from the cop's point of view.

Next slide, please.

I'd like to drill down into how long it takes to get access to data. And it matters. It also has different durations, different time lines, depending on the circumstances.

So it used to be that you could do a public source lookup and get back the registrant information in about ten seconds, right? So that's what many cops are accustomed to based off of their past investigative experience.

If they don't get that data, they might and probably usually won't even know that they can approach a registrar to get access to unredacted data if it was redacted for GDPR purposes. If there is not a privacy/proxy service in place and they do know somehow they can reach out, the responses have been various. Some registrars will respond directly to law enforcement requests for unredacted information, and we appreciate that.

Some will only respond to local law enforcement, meaning the same nation as the requested agency. And if you aren't that same nation, you're sort of out of luck at that point.

Some will ask for legal process.

For the benefit of translators, if you hear me say "legal process," I mean a court order, a subpoena, something along those lines.

And the time line for those increase as you might expect. If a registrar is responding voluntarily, it might not be ten seconds anymore but it still may be hours, maybe days. If you are talking legal process, you're talking days to two weeks on average is what I would expect to obtain, serve, and receive response to legal process.

If you're not in the same jurisdiction and you require legal process, you're probably out of luck. But you could theoretically, if you are a signatory to the Mutual Legal Assistance Treaty, file a MLAT request and get data back in six months.

Next slide, please.

So when we talk about impact, I wanted to call out one of our most impacted processes, our most -- one of our most impacted responsibilities and that is of victim notification. And the example here shows a business email compromise example, which is one of the most prolific criminal scams on the Internet today. We have an estimated $23 billion lost to this scheme as of 2019, last year. The numbers seem to double every year. I wouldn't be surprised if it approaches 50 billion by this year.

In this example, you see the bad guy is impersonating a CEO with a ceo@example.com domain that he registered. This is a look-alike domain, sometimes called homoglyph, where it is specifically targeted to a victim. He will send out an email asking for a wire transfer. That's how the schemes work. If he's successful millions of dollars go out the door. We as investigators in the past would do a reverse DNS search on that registrant of the bad domain and see many other domains that they've registered. And we can probably infer from most of those who the actual victims were because they're look-alike domains, right? If we can do this quickly enough, if we can move really fast, we then might be able to do further DNS queries on those victims and identify contact information for them and let them know in realtime that they are being actively targeted by a bad guy.

Now, even if it's a small delay in conducting those lookups because there are multiple lookups throughout this process, you are adversely impacting our ability to conduct these critical victim notifications to the extent that I don't think that these are being done anymore. Not because we aren't trying but because the very first step of obtaining all these additional potential victim domains, that requires legal process which will now require days or weeks.

We can still try this. I just really wanted to highlight this is one repercussion in the real world that comes from even relatively minor delays, going from seconds to minutes to days to weeks. It has tremendous downstream consequences. And I note that I am at time and time is precious, so I'm going to turn it over to the next panelist.

JONATHAN ZUCK: Thanks, Gabriel. And so next we are going to hear from the cybersecurity research folks. Greg Aaron and Lyman Chapin, go ahead and take it away.

GREG AARON: Hi, this is Greg Aaron.

Next slide, please.

Lyman and I recently did some research about phishing and tried to capture a lot of information about how much of it is taking place, where it's taking place, and so forth.

(No audio)

That yielded almost 300,000 phishing URLs, and those were in on 99,000 plus domain names. We then found out where those were hosted. We looked at the time of the events and found out what registrars, hosting providers were involved.

What we find is that phishing is actually fairly concentrated. It tends to cluster in places in certain TLDs. Certain hosting providers tend to have a lot more than others. If you want to go to the URL there, you can see the results of the study.

One of the things we do see is that phishing domains are used quickly. Almost -- Most of them are used within 14 days of domain creation, some of them, a lot of them within just three days of creation.

We also saw that phishing is a bigger problem than is reported. Every time you add a new source of data, you find out about new phishing events that the others didn't know about.

There are also evasion techniques that the criminals use.

So when you're looking at this data, you can figure out maybe what the floor is of the problem, but you can't establish the upper limit of what's going on.

One of the ways we know about how much phishing there is by how much is reported and block listed, and it -- trying to find this stuff is -- we're finding, is sometimes difficult. A lot of these sources overlapped by a very small amount. And we're also not seeing phishing in certain parts of the world. There is a conspicuous lack of data about phishing in places like China and Russia because of the reporting.

So one of those factors that does affect our ability to find the phishing is a lack of WHOIS information. There are two problems. Next slide.

Of course when you're trying to figure out how big a member is, depends on what you're measuring and how you're measuring. Now, Google, for example, is interesting in their measurements because they can actually see how much phishing they're blocking in the Chrome browser. So that's one very interesting measure. This slide is from their Safe Browsing Program, and the red shows the number of phishing sites they have been blocking. It's interesting because they have a consistent method over a long period of time.

What you see is the phishing is going up. At the same time, malware has been going down. Not necessarily unusual. The amount of cybercrime and where it is tends to shift and change over time. One of the reasons the malware is going down is because there have been some botnets that have taken down. It's also because criminals are less interested in running some kinds of banking malware. Instead, they've shifted to other kinds of crime, including the business email compromise scams that Gabe just described.

So when you're going to try to understand how much cybercrime there is, it depends on what you measure, how you measure, and you also need to look at the biggest picture. And if you don't measure some things, you simply don't find out about them.

Next slide, please.

Now, why do we need the WHOIS information? Well, we need the information because we do want to find out about things like when a domain name was registered and the registrars that it was registered at. That's the nonsensitive information. As we saw, registration date really matters.

One of the problems we encounter right now is rate limiting. That means registry operators and registrars only allowing you to do a certain number of queries within a certain period of time. The ICANN SSAC wrote a paper about that. It prevents us from getting the nonsensitive information that would allow us to see and probably detect more phishing attacks.

Also, people who are trying to fight the issue look, or used to look, at the contact information in the registration record. And that was important because criminals very often, as you would imagine, fake their information. They don't give accurate contact information. And it's possible to run checks on that, and if it's inaccurate, it is a gauge of bad faith on the part of the registrant.

It also allowed us to see if a certain party had registered more than one domain name, and you can do some lookups and compare information. Not so useful anymore in the post-GDPR world.

But what we saw in our report confirmed something that we've known for a long time, which is when criminals register one domain name they very often register a batch, and one thing we're seeing is those batches are not being caught as well as before. In some cases we can see long sequences of domain names, and a few of them were detected and blocklisted, but you can also see which ones were missed.

So next slide, please.

One of the things we also look at is the length of a phishing attack. This is some really great data that was put together by people at PayPal, Google, and Arizona State University. It was a really seminal study done this year. And those companies have some great insight because they can see what people are clicking on and they can track things from the first visit at a particular phishing site through the last visits, and then if it was a phish involving PayPal, they could see how the people got victimized and how many of them lost money out of their accounts, and so forth.

And this data was pretty consistent with other studies, including some I have done, but it shows us the phishing attack is short.

By the time you get your first visit to the time that the phish is kind of detected, perhaps, by a party, about eight hours elapses, and the entire phishing attack usually takes place over about 17 or 18 hours. So by the time the phishing attack is usually detected, the majority of the damage has been done. The majority of the victims have come to the site, and those who are going to actually lose money out of the scam have already fallen victim.

So next slide, please.

One of the things we also found is that about 60% of the domains used in phishing attacks are registered by the phishers.

Domains used for phishing fall into two categories. One, the phishers just go and buy domain names and then they use those to launch their fake sites. Phishers can also use domain names that they've broken into the hosting, so they're actually doing phishing on somebody else's domain name, an innocent party.

What we want to do as responders is we want to get those kinds of sites taken care of at the hosting provider, keep up the rest of the content, and prevent any collateral damage from happening to that innocent registrant.

However, domain names that are registered by phishers, those can just be suspended without any kind of collateral damage.

We found, through our methodology, about 60% of the domain names fall under this maliciously registered category.

A team from SIDN Labs and AFNIC -- those are the .NL and. FR registry operators -- created a separate system. There was a little bit of overlap in their methodologies. They created a very elaborate system, and they found 57%. So we were fairly close in the percentages, and they did some very good work that I thought was very interesting.

So next slide. So I think some of the take-aways are these. What we are finding is a lot of abuse registrations, we're having a hard time finding now. One of the reasons is that we don't have some of the data that was previously available and that's kind of an obvious conclusion.

In some ways, the contact data is something that distinguishes one domain name from another. It's an indicator of bad faith. And obviously who registered it or who purportedly registered it is an obviously important piece of information.

Now, the good news, if there is any, is that the registrars and the registry operators still have access to that data. They can see it even when no one else can.

And because a lot of the phishing is done by the phishers themselves who are registering these domain names, there's an opportunity for the registrars and the registry operators to continue to leverage that data. What we see, though, is that there is continuous phishing over and over again in certain TLDs and in certain registrars.

As far as the EPDP, one of the results was that we're going to have a target turnaround time for requests for data. Cybersecurity requests like for phishing requests are provisioned for in the GDPR itself. These are termed as legitimate interests for requesting the data.

However, that five-day turnaround, and then maybe it might go to ten, is going to be generally ineffective because the phishing attacks, less, less -- are lasting less than a day.

So the data through the SSAD system might come fast and it might come slow, and the slow requests aren't going to help the immediate problem.

So phishing is certainly an excellent candidate test case for automation. That something that the implementation team is going to have to look at. But if it can be routinized, then the SSAD system may actually be able to provide some useful data for responding to phishing and reducing victimization.

Thanks.

JONATHAN ZUCK: Thanks, Greg.

I guess we don't have Mark on the call yet. Is that right?

>> That is correct.

JONATHAN ZUCK: Okay. Then I would like to just go ahead and go to Milton so we can get to discussion because there's obviously a pretty lively discussion taking place. So let's get through these initial presentations and get the conversation going.

So, Milton, please go ahead.

MILTON MUELLER: Greetings, everybody. I'm Milton Mueller. I'm a professor at Georgia Institute of Technology in the United States. And, by the way, everybody on this panel is from the United States. Isn't that interesting?

In fact, the WHOIS debate has been kind of really focused on these differences between Europe and the United States over privacy law.

Can I go to the next slide, please.

So something you haven't heard very much about yet is why I'm on this panel, and I'm actually talking about the rights and interests of the registrant, the person who registers the domain name. And it shouldn't be too hard to understand why people who register domains have an interest in redacting certain personal information, sensitive personal information. And under many privacy laws, they actually have a legal right, as well as an interest in shielding that data.

In fact, our own Federal Trade Commission, which Laureen works for, has a lot of information about how you should not make information like your email address and other personally identifiable information like your telephone number easily available on online where it can be copied and used by anybody. And, of course, all we have really done with the enforcement of GDPR on to WHOIS is to use that common sensical notion that criminals and abusers can misuse open PII. And it's generally not a good idea to make your email and physical address available randomly to anyone and everyone on the Internet.

Now, despite that, in the existing WHOIS, of course, there's still quite a bit of information: Registrant name, the country, in some cases even the state will still be there and city. And we hope that we have set up new efficient methods to disclose redacted data in a way that will be faster.

It's curious to me why the At-Large has not been more interested in the rights of the domain name registrant. I know they're supposed to represent users. And I would like to know, you know, what was the position of the European At-Large structures on WHOIS. Because we certainly didn't hear any support for GDPR compliance from ALAC during the EPDP process.

Next slide, please.

Now, I really liked Jonathan's introduction to the panel, can we actually try to talk about facts here. So it's not easy to get conclusive information about what has happened. but we keep our minds on the fact that we're not talking about whether phishing is bad or whether -- how it works, so much as we're talking about how do these things work before and after the redaction of data because of our compliance with the GDPR.

So if you look at the Google statistics that Greg was showing and you look from December 15th to May 2018, which is the period -- basically the 17-month period before the redactions went into place, and you look at the 18-month or 17-month period after it went into place, with respect to malware sites, you see a decline before and after. Although the decline afterwards was obviously more large.

And if you look at phishing sites, you see very large increases both before and after of the implementation of the redactions.

And I've also looked at some spam data, although it's very hard to find long-term spam data. And, again, you don't see any linkage between the redaction of the data in 2018 and the size and scope of the problem. It's simply impossible to establish any kind of a statistical correlation between the redactions and the kinds of changes in the problem.

So I think, you know, the case that you would make based on data between redaction and our cybercrime problems is an extremely weak one.

It isn't because it isn't obviously helpful in some cases for law enforcement agencies to have quick access to this data. Obviously, it is. It's also the fact that quick access is a threat vector, part of the cause of the problem. And it's also the fact that more and more phishing and more and more abusive registrations, the criminals have learned to fake the information and they have come up with very clever ways of cross-referencing and getting false identity information in there without, you know, it being easily detectable by people who are looking at the WHOIS data.

As a final note on this phishing problem, let me say that when I'm teaching cybersecurity to students at Georgia Tech, we do an exercise in which we have teams of five students develop a phish email and send it to their instructors and see if they can fool them. And one of the things they discovered, the students discovered, is phishing domains are frequently detected by various algorithms among hosting companies, among web people, the browser manufacturers using things like how quickly was it registered and how recent is the domain and does it match certain strings. And maybe about half of those students discover that they -- their phishing domain is blocked even before they can complete their assignment and send it to me.

Next slide, please.

So again, it's not like we have shut off access to this information entirely. We do have established in the new policy process a centralized and standardized method for making disclosure requests. And I think we have to understand, and we can't ignore this, that this is all about compliance. This is not optional; okay, folks? We have to comply with the law. What we've done through laborious effort in the EPDP is to come up with a disclosure mechanism that is compliant with GDPR, which means many requests simply have to be reviewed to ascertain whether there is a legitimate interest and whether the requestor is legitimate, and so on.

So I'll leave it at that, and I look forward to robust discussion with the other panelists and with the audience.

Thank you for listening.

JONATHAN ZUCK: Thanks very much, Milton. This is Jonathan Zuck again here for the record. And I want to reiterate something that Milton said which is this is something that's happened and it had to do with compliance with the law. And so as we discuss this going forward, I think we want to look at what the world looks like, you know, under that law, not relitigate whether or not the law was good or anything like that, but instead, what the sort of data flow relationship has been between requestors and keepers of data. That's really the idea. Not to have the same conversation over again that the EPDP had for two years, but just to look back at what the process has been like since and what that relationship looks like.

To speak to that, I think Owen will be ideal. They just compiled a report on recent requests for data. I don't remember how far back it was. There is a webinar that's worth checking out. I'm sure Owen will point us to that and give us a little bit of a prÈcis of it here and talk a little bit from the data-holder side of the equation of what it has looked like since the implementation of the temp spec and what the past couple of years have looked like.

Owen, please take it away.

OWEN SMIGELSKI: Thanks, Jonathan.

Let's see. I'm showing video is on but I'm not showing up on the screen, or can people see me?

OZAN SAHIN: Hi, Owen. Yes, we can see you.

JONATHAN ZUCK: Yes, we can see and hear you.

OWEN SMIGELSKI: Okay; Great. Used to seeing myself but not the -- All right. Next slide.

So I am Owen Smigelski. I am with the registrar Namecheap. I'm also a vice-chair for policy of the Registrar Stakeholder Group. And the material I'm going to be presenting to you is a condensed version of a webinar that the registries and registrars put together in September. There is a link to the webinar, the presentation, as well as the recordings on the GNSO calendar. And I put the link in the slides here so that everyone could see that and go take a look. So I do invite you to go take a look and review that because there's a lot more information that's there.

I participated in that webinar along with three colleagues who put together the information that I'm now going to present: Alan Woods from the registry Donuts, Beth Bacon, PIR, the operator of .org, and Sarah Wild from Tucows registrar. So I've got to give all the credit to them for most of the material I'm about to present here.

Next slide, please.

So I think something that is lost in a lot of these discussions is that GDPR and data protection is nothing new. The roots of this is traced back to the end of World War II, and the concern there was during that period, personal information of people was used to profile and target numerous groups by states and other actors. That included names, religions, ethic origin, sexual orientation and other factors. and so after the horrors of that time, the interest of privacy in protecting personal data took a very high importance, and that has continued forward to this day. That's why data protection of data subjects is such an important issue and why it's something that just can't be overlooked because some people perceive that they are inconvenienced on occasion. So this was incorporated in the Universal Declaration of Human Rights in 1948. There became some more treaties and agreements, and the world's first national data protection law was in Sweden in 1973, and there were dozens more that were in place before the creation of ICANN in 1998.

Next slide, please.

So there are seven principles that are present in all the European data protection laws, and they should all be read with the protection of the data subject and not necessarily to third parties in there. So I won't go through them here, you know, but some of them are you need to have a limited purpose for gathering this information. You need to not take more data than is necessary. You need to make sure that it is stored for a certain period of time. It needs to be done in a secure manner. And there needs to be accountability for that data.

Prior to the effective date of the GDPR, the unrestricted access to registration data via WHOIS violated many of these principles.

Next slide, please.

So these are just some overview highlights of some issues here or some points. You know, GDPR is not new. You know, there were some slight changes to it to increase liability, but what was in place through GDPR was present in Europe as well as other countries and treaties for decades beforehand.

WHOIS never went dark. It's still there. It just complies with the law. And I know it's been repeated several times now in this webinar that WHOIS data is needed to stop reports. That's not the best way to do that. The best way is to report to a contracted party, either a registrar or registry or directly to a hosting provider. Those are the ones who can take care of it. You want to do an analysis afterwards to see who was doing what and how to prevent it, then that can be done afterwards when the limited time for a phish attack to stop it is done.

Reports and presentations do nothing to fix the problem. We need to have it reported to us in order to be able to take action.

And again, all of these data protection laws, including the CCPA in California and Brazil has a privacy law and other states which are continuing to pop up, confer rights to data subjects. It does not provide any right to the third party to access that data nor does it create an obligation to disclose that data.

Unredacted WHOIS data prior provided attack vectors that the ICANN community had been dealing with for well over ten years. Domain hijacking, spam, phishing, phone scams, fake renewal notices. All the things that we have been talking about for a decade-plus are things that can be addressed and resolved by protecting registration data from complete access by everyone.

Also, again, as we've heard time and again, overall abuse of domain names is not going up. It's going down. And there was no overall increase during the COVID-19 pandemic.

Next, please.

So I'm just putting this up here as an outline. For those who are interested in providing data requests, this is kind of the minimum and best information that someone can provide to a registrar or registry when making a data disclosure request. It's based upon the EPDP Phase 2 final report as well as best practices that were put together by the registrars and registries. And there's a link, direct link to this at the Registrar Stakeholder Group's website which I put in there. But it just gives some basic minimum information that a contracted party will need to review in order to conduct a balancing test on whether or not there should be disclosure. And without this information, that will delay the process.

And, yes, registrars and registries receive complaints without a domain name or what legal right the requestor is trying to claim or what data elements they want. And that delays the process. So you just need something to be complete for the registrar or registry to be able to cooperate and make the, you know, disclosure decision faster.

Next slide, please.

So now I'm going to just do an overview of some information that was collated for the presentation we did, was data provided voluntarily by some registrars and registries. It represents small, medium and large registrars and registries and several geographic regions of the world. So there was a wide range of data, so some registrars reported as few as 30 and others as much as 3400 requests. Registries had lower, and the initial post-GDPR numbers were higher but have kind of leveled off since then.

So some key takeaways are less than 1% of total domains under management were subject to requests, and they kind of varied based on what type of redaction, as the various contracted parties implemented and adjusted to the temp spec and other things there.

I would also like to highlight that under the SSAD, there will be a lot more metrics required by ICANN, which will also be reported to ICANN and then to the community. So we'll be able to get a lot better understanding, once there is an SSAD, on what types of disclosure requests are coming in, who is doing it, and what the results are, et cetera.

Next slide, please.

So here are some of the outcomes that we saw. So you can see from the registries about half the time they denied or redirected, and the registrars, about two-thirds of the time they denied or redirected.

So redirected means a registry saying please go contact a registrar or denied because of the unlawful basis. A balancing test there.

Some of the other reasons there while things were not necessarily disclosed is domain protected by a privacy service or the domain is not registered or with that registrar or registry.

Next slide, please.

What type of data was provided? A third of the time it was the registrant data, and two-thirds of the time it was the registrant admin and tech data. And generally when the data was not disclosed, the standard practice was to provide some sort of rationale and explanation. You know, often when there's a privacy/proxy service making a data disclosure request, it's not the proper avenue to do that. The privacy/proxy services have their own process and procedures in place to do that.

Next slide, please.

So some registrars did have some appeals that they'd received to denials of disclosure requests. Registries did not. You see the numbers for the registrars are very low. Often the requests come via an appeal would come over the wrong mechanism and would usually result in an educational outreach or an explanation of why it was denied in that particular case. And of note, none of the appeals overturned the disclosure decision or lack of it.

Next slide, please.

So here's some information about the types of requests that were provided. You see about three-quarters of them were from law enforcement -- excuse me, were IP requests, about 15% from law enforcements, and the rest were other, which includes security researchers, request of no domain (indiscernible) or again, domains that were not with the registrar or registry.

Next slide, please.

So of the requestors that we have here, I see that one -- there was one requestor for every four requests. So there's a lot of repeat requestors out there. And in fact, one specific requestor was the source of 45% of the requests, which is a significant portion of all the total request volume.

So I think that is -- one more slide, please.

This was the typical response time. It was less than three days overall. The registries were a bit faster than the registrars because often it would be a registry would redirect the requestor to the registrar who would be in a better position to either possess the data or to make that disclosure decision.

And so that brings me to the end here. I hope I didn't go through too fast. I wanted to make sure we had sufficient time for discussion afterwards.

Thank you.

JONATHAN ZUCK: Thanks, Owen. I know you had an awful lot to get through in a short time. So I appreciate you getting it through it quickly. That's very useful data.

OWEN SMIGELSKI: And please take a look at that webinar in he September. It was an hour and a half webinar so I had to condense quite a bit. There was a good discussion and a lot of information there as well, too. Thank you.

JONATHAN ZUCK: There definitely was. Maybe, staff, if you could look up the Zoom recording link for that and post it in the chat, that would be good. I think it's very good background for these conversations. And I appreciate the contracted parties having put that data together.

We're going to back up the slides, I guess, a little bit, staff, because Mark Svancarek has joined the call and we want to give him an opportunity to present briefly.

So, Mark, without further ado, take it away.

MARK SVANCAREK: Thanks, everyone. Can you hear me?

JONATHAN ZUCK: We can.

MARK SVANCAREK: Sorry. I had an alarm clock malfunction. What an amateur hour, huh?

Hi, I'm Mark Svancarek from Microsoft, and I'm here to give just a perspective of how we see cybercrime at Microsoft and what's happening with WHOIS and GDPR.

So I'll try to be fast so we can get to the -- (laughter) -- the conversation.

So I'm putting something in the chat. This is Microsoft's new Digital Defense Report. This is the first time we've done one. It's pretty comprehensive, and it tells how we see the current state of cybercrime.

So there is a lot of conversation about whether cybercrime has gone up or down lately. I'm not sure why this is a -- why this is a debate. It is -- it is going up. All sorts of cybercrime are going up. And so the defense against it remains a high priority and a lot of effort is going into it.

The WHOIS data set is one of the techniques that we use to address all sorts of crime, corporate, consumer fraud, anti-piracy, state actor threat assessment, more things than that.

I apologize.

Yes, I did not -- I did not submit slides. I'm sorry. When I previewed the slides ahead of time, I seemed like only Milton had submitted any. So I thought it would be just more conversations.

So -- sorry.

Anyway, the challenge that we have with WHOIS under GDPR right now is just that we have not really developed a system that enables us to access the data to the full extent that will be enabled under the regulation. And I think it would be interesting to debate this further in the group, but it really comes down to we have received a certain amount of legal information. And within the group, there was not consensus on what that legal feedback actually meant. And this is in regard to accuracy, necessity, and things like that.

And so I think if you were to look at that Webinar from September, go to about 34 minutes in the actual process that is put forward for balancing tests, I think you'll see that it differs a lot from the feedback that we received from Bird & Bird regarding what does "necessary" mean. And so I have some of this information here, if you would look at -- where is it? I'm sorry. I don't have my links ready. I thought I did. Basically -- I apologize. I am really sorry, folks.

I'll put these things into the chat in a minute. But basically it comes down to necessary -- I'm really going to have get my quote here.

We can move ahead.

Oh, dear. Oh, dear. Oh, dear. While I'm looking for the link, the point is we've heard such things as the existence of dispute resolutions, like UDRP, means that it would never be lawful to disclose data under WHOIS, for instance. That's not the case.

JONATHAN ZUCK: Hey, Mark. It's Jonathan.

MARK SVANCAREK: You know, I'll be back in a minute.

JONATHAN ZUCK: You don't need to have the links live. If there's just any big points you wanted to make, I guess that would be the place to go. But we can also, otherwise, just get going on the discussion.

MARK SVANCAREK: Let's get going on the discussion. And I will find these links momentarily.

But the point is that there have been a lot of assertions that SSAD could only be developed in a single way because of the legal feedback that we received. And that's not the reality. The reality is that we had additional options, and we have chosen not to pursue them.

And the path --

JONATHAN ZUCK: Thanks, Mark. I guess what we really want to focus on in this decision is not relitigating that, but actually looking at what these requests, timings have been, et cetera. That's why Owen's data was so useful.

I know David Taylor has compiled some data on the requester side.

But I guess what I'm trying to get at is given the fact that GDPR is a reality, given the fact that -- you know, that enforcement of it is a reality, implementation of the EPDP recommendations is a reality, are the communication channels working between data requesters and data holders, for lack of a better term?

I think that's the conversation we want to try to have, what that exchange has been like going forward. That's why Owen's data was really useful.

Because, you know, for example, one of the things that came up early on in the presentation was the idea, I think, that Gabriel mentioned, which is that by the time something is noticed -- a phishing scam is noticed, it's already over which would suggest that there isn't a fast enough time period for contracted parties to get back to you, you know, after a complaint, for example.

And so I think we want to start to have a real conversation about what's realistic in terms of what this data exchange can look like.

So -- let's see. Yeah, so one of the conversations that has come up quite a bit is that the DAAR data seems to suggest that DNS abuse at-large has gone down. Yet, there seems to be other data that it has gone up or it's gone up in different ways, et cetera.

Is there somebody that wants to take on that notion? This is from Luc Seufer who asked this question in the question pod. Why is there this dichotomy between those two -- you know, two different data sets? Why don't we have a definitive answer about what direction DNS abuse is going?

GREG AARON: Hi, Jonathan. This is Greg. I can talk to this because I designed and built the DAAR system.

So what DAAR does is it looks at data from a few different blocklists which contain domain names. And it looks at blocklists that cover certain categories of phenomenon like phishing and malware.

What we would normally expect is it would ebb and flow over time. If it decreases for a little while, it may increase again. That's kind of standard.

So it's measuring very specific things from very specific sources. One of the things we see, though, is that new techniques of evasion may decrease the number of domains you're seeing. We don't know the effect of having less WHOIS information available, what effect that's had on blocklisting efficiency. Although some sources have measured it and there's been some publication that shows that if it's harder to find the bad guys, you get fewer blocklisted domains. That's one of the possible effects.

So that doesn't mean that the amount of cybercrime has gone down. It just means you found fewer domains and you've found fewer on the lists you looked at.

When Owen says overall abuse of domain names is decreasing, that might be by one measure according to certain circumstances and certain sources.

Still, no matter how you measure it, it's a lot. The other thing to remind ourselves of is that the number of domain names on a given list is not a measure of the damage done or the risk involved. With business email compromise, for example, the amount of money being lost in each of those scams on average has been going up. So if you have the same number of domain names, the damage to the victims is greater.

So I think it really depends on what you're measuring and how. Other indicators say that it's going up. So DAAR is one thing -- doing one thing in a particular way. And I don't think it's probably indicative of the entire ecosystem. Thanks.

JONATHAN ZUCK: Thanks, Greg. Theo Geurts asked: What is the quality of the data when a registrar discloses data? Is it usable for investigations?

We heard from a number of folks that things were already headed south because of a lack of accuracy and privacy and proxy services, et cetera. Can you really -- I think as Milton asked: Can you really attribute the difficulties you're facing to the changes that have come as a result of compliance with

GDPR? That question is for, I think, folks in both cybersecurity research and law enforcement.

GABRIEL ANDREWS: Hi. This is Gabriel. If I can jump in and just add a small answer to this.

JONATHAN ZUCK: Please.

GABRIEL ANDREWS: I think the quality of the response is going to vary obviously, but it's always worth getting. And truly the only time that the response isn't worth anything is if it just comes back to a privacy/proxy service which will tell you nothing. But we find even if criminals lie about their registrant information or have used compromised payment credentials, et cetera, these are all data points. And you never know which data point is actually going to be key to breaking open investigations. So I would much rather take even fraudulent registrant data than have no data access. Although, obviously, the greater extent to which that data is authenticated at registration, the better for us and the worse for the criminals.

Thanks, Gabriel.

Stephanie Perrin posted a question: Do we have stats for the frequency of valid data being stolen and substituted for criminals' data? Historical data has already been scraped. Much is still valid.

GREG AARON: This is Greg. I can address that one. Hi, Stephanie.

JONATHAN ZUCK: Great, thank you.

GREG AARON: I mean, I've looked at the contact data for literally millions of domain names used abusively over the years. What I see is that criminals don't tend to pull the data of others and use it. They tend to just make up data. And some do a better job of that than others. But it's relatively rare in my personal experience to have seen just misappropriated data.

JONATHAN ZUCK: Okay. Thanks.

And I guess I'd ask, can you turn on your camera when you're speaking, too. We're trying to get more faces into these online meetings. So when it's -- when you're answering a question, it would be great if you can turn your camera on. I know it's a lot of clicking back and forth, but ideally people can see them.

Volker mentioned: Greg seems to be saying there's no benefit in taking domain names down when a report is received as the damage is already done. That seems counterintuitive.

GREG AARON: No. I think Volker misunderstands. One of the things you saw in that chart I showed is that, yeah, if you actually take down the domain, you will have an incremental benefit. Also, phishing is one of the types of cybercrime that is shortest in duration. So other problems you have a much greater benefit when you suspend the domain name that's registered by a criminal so it's very useful.

The question is certainly, though, there is a difference between mitigation and prevention. One of the things we have seen from the data is there are certain places where criminals go and register domain names. Their domains get suspended, and then they just register some more. We do have a problem with repeat activity. And it would be great if more of that repeat activity could be caught and prevented early.

So to suggest that, you know, suspending domain names is not worth anything, no, it's absolutely worth it.

Again, the name of the game here is to protect, you know, individuals who are being victimized.

MILTON MUELLER: Can I get in here, John?

JONATHAN ZUCK: Sure, Milton. Go ahead.

MILTON MUELLER: Again, I think we really need to focus on pre and post-WHOIS redaction. That's the issue here. I don't think it's entirely relevant to be saying that phishing is a problem. We all know that.

The question is: Has the battle against phishing or other forms of cybercrime, how much does it actually rely on open access to WHOIS data?

And I think that the criminals came up with fairly robust methods of avoiding detection and most of the real brakes that are put on phishing domains are coming from suspensions and from algorithms detecting patterns and quickly just blocking them. And it's not clear to me that the presence or absence of WHOIS data has anything to do with that. And there's -- again, looking at the data, we see no statistical correlation between pre- and post-WHOIS problems. So let's focus on that.

I don't think you can simply say we liked it when we had this access. But when you had that access to data, indiscriminate, open, phishing was still a problem. It was a very growing problem and growing at a faster rate than it is now.

So let's focus on, again, cause and effect, if we can.

JONATHAN ZUCK: Excellent question, Milton. Does somebody want to take that from law enforcement side or cybersecurity side?

GABRIEL ANDREWS: Well, I can add a comment that investigations are impacted adversely by the lack of that data. There's many ways why that occurs, but that's maybe a bigger conversation.

I wanted to call out this panel and my prior comments that our duties don't just involve the attribution side, however, but also sometimes involve the swift notification of potential victims. And that's a real-world example where we absolutely are impaired and that we are using not just subject identifiers within the DNS system but the identifiers associated with victims that are actively being targeted. And so assumingly valid data. But if it isn't swiftly available, then the important conversations that could happen telephonically to someone whose emails accounts are potentially compromised and being targeted right then, that day or the next day, they enable us to have those conversations. And if we can't, we can't and to the detriment to citizens globally.

JONATHAN ZUCK: Gabriel, are you suggesting that then the use of the data is more valuable to reach out to the innocent than it is to track down the criminals?

GABRIEL ANDREWS: I don't think I can place an evaluation. I can just say that I know they are used for both, if that's fair. I don't -- I have difficulty making broad, sweeping claims over what's happening most simply because I've tried to collect data and I've seen how difficult it is to get investigators to take time away from their busy days to report back. Like, I've tried 82 times to get registrant information and succeeded 42. Right? They don't track the failures. It's very difficult then to come back and provide the sort of facts that I know would be tremendously useful here.

But what I can say is that when I have been collecting these anecdotes, this is the one that I got that was most striking to me, was the frustration that was felt by some investigators who were trying to do the right thing, to provide notifications to people that would be harmed and they found they were stymied. And this isn't to say they couldn't somehow, some way maybe explore other avenues.

This is just saying that this is the swiftest method that used to work for them and it doesn't. And it's just something I wanted to bring light to.

And I'll let you take it forward.

JONATHAN ZUCK: Thanks. Gabriel.

Owen, I know that part of the presentation that happened recently by the contracted parties about data access laid out some groundwork for the best way to format requests to get them expedited, et cetera. Are there any examples or any data associated with data requesters doing it that way?

And is there a correlation then to greater likelihood of the data being provided in a more expeditious manner?

OWEN SMIGELSKI: Thanks, Jonathan. This is Owen Smigelski for the record. I can't really draw any conclusions from that. It was certainly a finite and not necessarily a comprehensive dataset, but the experience of the contracted parties was when they did have requests with additional information, they were able to process it quicker. They were able to conduct the proper balancing tests quicker. But just because you provide all of the information does not mean that it's going to pass that balancing test. Are there less intrusive means of pursuing it as opposed to just simply getting the data. There's a number of questions and factors in there that could apply.

It does certainly speed up the process. It can get you to a conclusion there. Most of the data showed most of the requests are for trademark infringement. And so that's generally not necessarily one of those urgent cases that needs to have a takedown of a botnet. There are other routes to go, such as a UDRP or URS or similar thing there which you don't need the data for. So that's a less intrusive one which would thus pass -- that would fail that balancing test because there are less intrusive means to do that.

JONATHAN ZUCK: Owen, do you think the balancing test is going to continue to be a completely case-by-case basis or is there going to be some way, for example, the people that have signed on to the DNS abuse framework to get together and come up with some sort of a decision tree that makes it a little less of a black box for the folks that are trying to get data from the contracted parties?

OWEN SMIGELSKI: Thanks, Jonathan. This is Owen again for the transcript.

I can't really say what's going to happen in the future. There's still a lot of ambiguity and uncertainty out there as to what and will not be allowed. Some of the guidance already is that, no, certain things can't necessarily be automated. And there is just so many unknowns with the data disclosure requests.

I know I saw some chat in there saying, well, the U.S. Congress is going to, you know -- should pass something to make WHOIS publicly available. But for a large registrar such as Namecheap where we've got millions of customers all over the entire world, it's not possible, necessarily, to say with 100 percent certainty that this is a person who is located outside of a jurisdiction, that's not subject to a data privacy thing, and disclosing that data would subject us to potential civil and criminal liability. So it's not something you can easily make a cookie cutter one-size-fits-all approach. Some registrars may be a smaller or are only focused on a certain region or have a different type of business model.

So I think as this evolves over time, and that is certainly built into the SSAC to evolve it and change it through the policy process, I think it will certainly evolve, but it's too early to predict how that would go.

Thanks.

JONATHAN ZUCK: Thanks, Owen. I guess on that same issue, Lori Schulman asked whether or not you'd be willing to discuss Namecheap's specific experience in terms of the number of requests that were received and how many resulted in disclosure of data.

OWEN SMIGELSKI: Hi, Jonathan. This is Owen again. That's not something I'm able to discuss right here. I don't have access to that data right now.

JONATHAN ZUCK: Great. Thanks.

So the -- I know there's been a conversation, I've been trying to watch all the question pod and the chat to try and sort of figure out what the community as a whole has been saying. I know that Mike Graham, if you're on, you made a specific question about a specific change that happened with the redaction. Is that something you're willing to turn on your microphone and share with us? Because it just scrolled past in the chat.

Don't mean to put you on the spot.

Yes, can you turn on your mic or can the staff allow Mike to turn on his microphone?

MICHAEL GRAHAM: Is it working now?

JONATHAN ZUCK: Yes, it is. Thank you.

MICHAEL GRAHAM: Sorry about that. Really quickly, I can only share a bit of the information, and that is in terms of effort and cost. And there are two different ways that it's had an effect. One is in just discovering information so that we can determine whether or not a particular domain name has been fraudulently registered and is being used or perhaps it may be registered by someone that has a relationship with our company and it's simply that they are inadvertently typo-squatting.

And certainly in the latter case, we understand there are a lot of people who get onto the Internet, are not sophisticated and may do something that, you know, may damage not only our ability to reach consumers and such but (indiscernible) their ability to do so and to be a good Internet citizen, but then in terms of just research and cost to companies, it is a tremendous expense, additional expense to find out that information. And in terms of the real abuse -- and this is abuse not necessarily phishing but in some cases in phishing for us and in other cases just out and out counterfeiting that goes on on the Internet. The cost of investigation has risen tremendously. And at some point, that's a cost that is suffered not only by us but also by consumers, both in a financial manner and also in their being able to trust what they find on the Internet. And that's something that really concerns us, that they're able to find what they're looking for and not be duped into one of these schemes that seems to be going on, you know, day in and day out.

JONATHAN ZUCK: Thanks, Michael.

The issue of cost is a complicated one, because obviously those in the data requestor community aren't always sensitive to costs being imposed on contracted parties, too. So, you know, in order to implement some of the things that are asked of them.

So if it's just a cost of doing business to comply with the law, then I think that's -- that's going to be a complicated balancing question as well.

Elizabeth --

MILTON MUELLER: Can I get in on that?

JONATHAN ZUCK: Yes, Milton. Go ahead.

MILTON MUELLER: Cost is really in some sense what this is all about because for 20 years, the requestors have not only had a free lunch, they have essentially been subsidized by the ICANN regime. So we basically present domain name registrants with a contract of adhesion that says you want a domain name, you are required, without your consent, without any say in the matter, to make your personally identifiable information globally accessible to everybody and anybody who wants it. And that imposed costs on registrants, and that subsidized the access of people, some of whom were hoovering up this information and selling it and making money on it.

And I think the -- what we've done is, with the SSAD is we have said, okay, the costs are going to be balanced in a way that is more just and more efficient. So if you're a big requestor, and we can all think of a couple of companies that are generating most of the requests, I thought Owen's data was actually very helpful about that, you know, you're the one that's generating the cost of the system. You are the cost causer, so to speak, and you should pay more. You should support the system either through a user-generated fee or some kind of tiered accreditation charge that would cover the cost of making this data available.

And if this data is going to be available as quickly as some people would like, obviously you're imposing huge costs on the contracted party who has to have somebody sitting around evaluating these requests. And again, you can avoid some of those costs by automating, but automating can also be illegal if you are not actually performing the proper kind of a check on the nature of the request.

So it is, indeed, as you say, a complex challenge, Jonathan, and I think that's -- in terms of the purposes of this panel, I think it would be good to have more awareness of the way costs are being distributed in a balanced way across different stakeholder groups.

JONATHAN ZUCK: Thanks, Milton.

Natalie Leroy asks: Most European registries offer a data release service compliant with GDPR if a requestor can provide evidence of a trademark registration. Is it known if gTLDs or other ccTLDs are thinking of adopting a similar model? This helps enforcement efforts tremendously.

Owen, you may be the only one able to address that question, even if you don't know the answer.

OWEN SMIGELSKI: I apologize. I was trying to follow the chat here. Which question was that?

JONATHAN ZUCK: Sorry, Natalie Leroy. It's at the very bottom of the question -- question pod.

OWEN SMIGELSKI: So I don't know -- thank you. This is Owen for the transcript.

I'm not sure if there are other gTLDs or ccTLDs that are adopting similar models, but, you know, again, as this moves forward, as we, you know, get into this SSAD, there may be a away of credentialing users that are for either a particular gTLD or something along those lines.

Again, with the EPDP Phase 2 report came out was the starting point. We were under some time pressures to get everything done, to put everything in there. There was a lot of participants inside and outside who wanted something done quicker than what we were doing, and so we did the best we could in the time constraints that we had.

So I think that could certainly be a suggestion moving forward as the SSAD model does evolve of putting something in there. I think if it's something that's agreed upon and complies with the laws, then that could certainly make (indiscernible) easier.

Thanks.

JONATHAN ZUCK: Thanks, Owen.

I hope that helps, Natalie. I think that's a much bigger question than we're ever going to figure out today.

Laureen has asked to respond to Milton. So Laureen, please go ahead. Or, staff, can you enable Laureen's microphone.

LAUREEN KAPIN: I think I'm unmuted already.

JONATHAN ZUCK: Okay; great.

LAUREEN KAPIN: Thanks. And I wanted to agree with some of the points that Milton makes about this information being a double-edged sword. And certainly it can be used for bad purposes. And, indeed, Milton, we see that in complaint data as well.

But on the other hand, the DNS is a public resource. And Milton used the example of things being hoovered up and used for malicious purposes and that being against the law, which there's no disagreement on.

But the GDPR doesn't protect the data of legal entities. And I'm looking forward to the ongoing policy development efforts in that regard, because the public does have a right to know the information of legal entities' information. And just by that change of allowing users to find out who is behind domains that are not individual entities, that would go a long way to helping the public and law enforcement in their investigations and due diligence efforts.

And, you know, just as we require certain information to be given for the use of public resources, whether it's a driver's license or a business license and some of that information is made publicly available, it should be done for the legal information associated with legal entities.

JONATHAN ZUCK: Thanks, Laureen.

There are more questions, and so the staff will collect them, and we'll try to find a way to write up answers. Unfortunately, we've run out of time. It's been a good conversation. It's always difficult to keep it focused. And -- but to answer Jeff's question about what the purpose of a plenary is, I'm not sure. But ideally, the more that we understand what the factual situation is before and after a change in ICANN policy, the better informed we are about what steps need to take place next. And I think that was the purpose of this discussion, was, to the extent possible, gain an understanding of what this change to the status quo has resulted in in terms of the flow of data and the availability of the information necessary for consumer protection in cybersecurity research.

So hopefully this was a bit of a fact-finding mission. There's clearly a lot more fact finding that needs to take place. There's a lot of questions left in the pod. We'll do see what we can to address them, but we've run out of time today. It's 3:00 in the morning for me, so I've probably run out of witty things to say so I will just say thank you to all of the presenters and all the people that have come on board to discuss this. We'll take a look at the chat, et cetera, and use that as fuel for conversations going forward.

Thanks again so much for everyone. This meeting is adjourned.

[END OF TRANSCRIPT]