COMMITTEE ON THE JUDICIARY,
U.S. HOUSE OF REPRESENTATIVES,
WASHINGTON, D.C.

INTERVIEW OF: ALEXANDER STAMOS

June 23, 2023

Washington, D.C.

The interview in the above matter was held in room 2237, Rayburn House Office Building, commencing at 9:30 a.m.

Present: Representative Jordan

Appearances:

For the COMMITTEE ON THE JUDICIARY:

[redacted]

For the SUBCOMMITTEE ON THE CONSTITUTION AND LIMITED GOVERNMENT:

[redacted]

For ALEXANDER STAMOS:

JOHN B. BELLINGER, III, ESQ.
CALEB THOMPSON, ESQ.
ARNOLD & PORTER KAYE SCHOLER, LLP
601 Massachusetts Ave, NW
Washington, DC 20001

[redacted]. We'll go on the record.

Good morning. This is a transcribed interview of Mr. Alex Stamos. Chairman Jordan has requested this interview as part of the committee's investigation of how and the extent to which the executive branch has coerced and colluded with companies and other intermediaries to censor speech.

Would the witness please state your name for the record?

Mr. Stamos. Alexander Stamos.

[redacted]. We encourage witnesses who appear before the committee to freely consult with counsel if they so choose, and it is my understanding that you are appearing today with counsel. Is that correct?

Mr. Stamos. Yes.

[redacted]. Could counsel please state your name for the record?

Mr. Bellinger. John Bellinger, Arnold & Porter.

Mr. Thompson. Caleb Thompson, Arnold & Porter.

[redacted] Thank you.

On behalf of the committee, I want to thank you for appearing here today to answer our questions. The chairman also appreciates your willingness to appear voluntarily.

My name is [redacted], and I am with Chairman Jordan's staff.

I will now have everyone else in the room who is with the committee introduce themselves as well.

[redacted] [redacted] with Chairman Jordan's staff.

[redacted] [redacted], Chairman Jordan's staff.

[redacted] [redacted], chief oversight counsel for the House Judiciary

Democratic staff.

[redacted] [redacted], House Judiciary Democratic staff.

[redacted] [redacted], House Judiciary Democratic staff.

[redacted] [redacted], House Judiciary Democratic staff.

[redacted] [redacted], House Judiciary Democratic staff.

[redacted] [redacted], Mr. Jordan's staff.

[redacted] [redacted], Chairman Jordan's staff.

[redacted] Thank you.

I would now like to go over the ground rules and guidelines that we will follow during today's interview. Our questioning will proceed in rounds. The majority will ask questions first for 1 hour, and then the minority will have an opportunity to ask questions for an equal period of time if they so choose.

We will alternate back and forth until there are no more questions and the interview is over. Typically we take a break at the end of each hour, but if you would like to take a break apart from that, please just let us know.

As you can see, there's an official court reporter taking down everything we say to make a written record, so we ask that you give verbal responses to all questions.

Do you understand that?

Mr. Stamos. I do.

[redacted]. So the court reporter can take down a clear record, we will do our best to limit the number of people directing questions at you during any given hour to just those people on the staff whose turn it is.

Please try and speak clearly so the court reporter can understand and so the folks down at the end of the cable can hear you as well. It is important that we don't talk over one another or interrupt each other if we can help that, and that goes for everybody present at today's interview.

We want you to answer our questions in the most complete and truthful manner as possible, so we'll take our time. If you have any questions or if you do not understand one of our questions, please just let us know. Our questions will cover a wide range of topics so if you need clarification at any point just ask.

If you honestly don't know the answer to a question or do not remember, it is best not to guess. Please give us your best recollection, and it is okay to tell us if you learned information from someone else. Just indicate how you came to know the information. If there are things you don't know or can't remember, just say so and please inform us who, to the best of your knowledge, might be able to article.

You should also understand that by law you are required to answer questions from Congress truthfully.

Do you understand that?

Mr. Stamos. Yes.

[redacted]. This also applies to questions posed by congressional staff in an interview.

Do you understand this?

Mr. Stamos. Yes.

[redacted]. Witnesses that knowing provide false testimony could be subject to criminal prosecution for making false statements under 18, U.S.C., Section 1001.

Do you understand this?

Mr. Stamos. Yes.

[redacted]. Is there any reason you are unable to provide truthful answers to today's questions?

Mr. Stamos. No.

[redacted]. Finally, I would like to make note that the content of what we discuss here today is confidential. We ask that you not speak about what we discuss in this interview to any outside individuals to preserve the integrity of our investigation.

For that same reason, the marked exhibits that we will use today will remain with the court reporters, and we will collect any copies of the exhibits at the end of the interview.

Okay. That's the end of my preamble.

Do my colleagues from the minority have anything?

[redacted] We would just like to thank the witness for flying out from California to join us today.

[redacted] Thank you.

Mr. Stamos I understand you have an opening statement. You may proceed.

Mr. Stamos. I do. Thank you.

Good morning. I'm glad to have this opportunity to describe the work of the Stanford Internet Observatory and to address misperceptions about its participation in the Election Integrity Partnership and the Virality Project.

The Stanford Internet Observatory studies misuses of the internet with the goals of publishing research, suggesting technical and policy mitigations, and educating the next generation of cyber specialists. I'm the founder and the director of the observatory and a lecturer in the computer science department at Stanford.

To that end, I teach courses in cybersecurity and online safety at Stanford, along with supervising our research efforts. Our research includes work on child safety, online promotion of self-harm, generative AI, and influence campaigns by China, Iran, Russia, and many other countries. I'm visiting Washington this week to brief government officials on our latest projects, a study of large commercial operations selling child sexual abuse materials on Instagram, and our upcoming work on how generative AI will impact child safety work.

Let me briefly describe the Election Integrity Project and the Virality Project, both of which have been grossly mischaracterized.

In the summer of 2020, SIO organized a group of four institutions in forming the Election Integrity Partnership. The primary goals of the EIP were to document, in real-time, the most widespread online narratives about the functioning of the election, to provide a basis for further academic research of online misinformation dynamics and responses, and to provide local and State election officials with a window into what was happening online in their jurisdictions.

The EIP had about 100 contributors from four institutions. About half of the overall workforce came from Stanford, and 42 of our 50 contributors were student research assistants.

The majority of those students were undergraduates, mostly ages 18 to 23, studying computer science, political science, and other subjects. To be clear, the vast majority of the analysis for both the EIP and VP was performed by student researchers.

The EIP operated transparently and openly, publishing numerous blog posts, holding regular video briefings, and documenting our work in a 274-page final report and multiple peer-reviewed articles. As part of our work, the EIP invited multiple groups, including the Republican National Committee, for example, to submit reports about potentially false or misleading social media posts around the operation of the election for us to include in the work, although in that case the RNC did not respond to our invitation.

One of the groups that did provide reports to the EIP was the Elections Infrastructure Information Sharing Analysis Center, or EI-ISAC. EI-ISAC was created in 2018 to help State and local election officials with cybersecurity issues. It is operated by the nonprofit Center for Internet Security and offers a switchboard operation for reports of security issues to be raised by the thousands of local and State officials who run elections in the U.S. The vast majority of these officials do not have the capacity or expertise to manage complex cyber issues by themselves.

To be clear, at no time did the EIP censor speech or have access to backend platform systems or data outside of public content. The EIP did not take down posts or apply labels and had no power to do so. The EIP did not create targeting lists or blacklists of accounts, and the list of accounts included in our reports as the top spreaders of false information were generated by our academic analysis, which, importantly, occurred after the election. When content clearly violated the policies of social media platforms, we could refer it to the companies so they could make their own determinations.

Many of these referrals related to false statements around the time, place, or manner of voting or accounts falsely claiming to be run by election authorities. SIO personnel flagged false statements that could be interpreted as supporting candidates of both major political parties, not solely false statements supporting Republican candidates.

I'll give you an example of how the system worked. On October 3, 2020, a member of the Kentucky State Board of Elections sent an email to the EI-ISAC team reporting a Facebook page that was pretending to be run by the Board of Elections and that was asking citizens to report ballot irregularities.

The EI-ISAC team opened a ticket in the EIP's tracking system to report the potential issue to EIP.

A student researcher at Stanford was assigned the ticket and quickly found a related website and Twitter account. He archived those accounts for further study.

The student determined that the registration information for the website matched that of an owner of an online marketing firm who had supported a Democratic candidate for Senate in Kentucky. The candidate had lost in the primary and blamed, without evidence, vote-by-mail. The website asked for personal data while misrepresenting itself as run by the Board of Elections.

The EIP team then reported the accounts to the relevant social media platforms and the URL to the Google Safe Browsing list. In this case the social media platforms removed the accounts for impersonation.

The team then replied to EI-ISAC with the details of our findings so they could be relayed back to the Kentucky Board of Elections.

During the 2020 election cycle, the EIP studied and documented several attempts by foreign actors to influence the U.S. election. This included for-profit actors operating out of North Macedonia, as well as amplification of domestic narratives by foreign propaganda outlets belonging to Russia and the People's Republic of China.

In October of 2022, the EIP partnered with Twitter in an analysis of six networks of fake accounts tempting to influence the midterm election on behalf of Iranian and Chinese interests. These networks generally pushed progressive ideas such as Medicare for All and attacked Republican candidates. Despite the conventional wisdom, different American adversaries clearly do intend to interfere in our democratic processes in ways that harm both major parties.

After the conclusion of the 2020 election, the surprise announcement of the first COVID-19 vaccines made it clear that the next historical event to play out online would be the testing and distribution of these vaccines. We added new organizations, built relationships with medical professionals, and created the Virality Project to study the most widespread rumors and narratives regarding the effectiveness and safety of COVID vaccines.

The goal of the Virality Project was not to identify misinformation, as we knew that the scientific consensus was still rapidly developing, but to study the most widespread narratives regarding the effectiveness and safety of vaccines. The primary, outputs of the VP were its weekly reports, all of which are still available on VP's public website. As stated on the website, our goal was to help guide public health messaging that is responsive to online conversations.

As with EIP, no government agencies had any special access to VP's internal research systems, and the VP operated openly and transparently, releasing weekly reports, blog posts, and a 230-page final report.

Neither the EIP 2020 or VP received any public funding. SIO's sole source of government funds is a single National Science Foundation grant funded after the completion of both of those projects.

Previous testimony to this committee has included some very serious false and misleading accusations about our work and I'm glad to have the opportunities to address some of them.

On March 9, Michael Shellenberger testified that the EIP report censored 22 million tweets with misinformation labels. Mr. Taibbi made a similar claim in a Twitter thread tied to his testimony. This is false. The EIP had no power to apply misinformation labels to any tweets. The 22 million tweet number was EIP's estimate, calculated after the project completed, of how many tweets overall mentioned the rumors or narratives we studied.

In a Twitter thread tied to Matt Taibbi's testimony, he then claimed that after the 2020 election, when EIP was renamed the Virality Project, the Stanford lab was onboarded to Twitter's Jira ticketing system, absorbing this government proxy into

Twitter infrastructure, with a capability of taking in an incredible 50 million tweets a day.

There were two falsehoods here. The SIO and EIP have never had access so any Twitter ticketing systems. The 50 million tweet number is, in fact, Twitter's estimate of the number of tweets made every day related to COVID-19.

Mr. Taibbi claimed that, in one remarkable email, the Virality Project recommends that multiple platforms take action even against stories of true vaccine side effects and true posts which could fuel hesitancy.

This is false. The misleading fraction of the email Mr. Taibbi released was part of a question sent to multiple companies from students to see which kinds of vaccine narratives the companies were interested in to be notified about. The content from these notifications were then put into the public weekly reports.

I'm glad to be able to dispel these and other false statements about our work, and I'm looking forward to your questions.

Thank you for the time.

[redacted] Thank you.

The clock now reads 9:43 a.m.

My colleague, [redacted], will begin with questioning.

EXAMINATION

BY [redacted]:

Q Thank you again for being here.

Can you state your full name?

A Alexander Stamos.

Q Mr. Stamos --

A You can call me Alex, please.

Q Alex, thank you.

What is your current place of employment?

A I am the director of the Stanford Internet Observatory at Stanford University.

Q And what is the Stanford Internet Observatory?

A It is a research program as part of the Cyber Policy Center at Stanford, which is a joint project of the Freeman Spogli Institute and the Stanford Law School.

Q And when did you become director of the Stanford Internet Observatory?

A I came to Stanford in August of 2018, and then we started the observatory as a new program in early 2019.

Q I'm sorry? 2019?

A In 2019, yeah.

Q And did you become director when the program was started?

A Yes. I was the original director, yes.

Q Starting with college, what is your educational background?

A I have a degree in electrical engineering computer science from the University of California, Berkeley.

Q Any other degrees?

A No.

Q Starting with after college, what is your employment history?

A My first job after college was with a company called LoudCloud, which was a cloud computing company, before it was a profitable business. That company was sold to EDS, and so I went and worked at a company called At Stake, which was a security consultancy. At Stake was purchased by Symantec, a large security company. And at that moment some friends and I decided to start our first company together called iSEC Partners.

We operated that company until 2010, at which point we sold it to NCC Group

PLC, a large British multinational security company. I stayed there for a little bit as the CTO of the new combined company. And then I was the chief information security officer at Yahoo. Then after leaving Yahoo in 2015, I became the chief security officer of Facebook, and that was a job I held until the fall of 2018 when I came to Stanford.

Q What were your responsibilities at Facebook?

A So chief security officer has responsibilities that really fall into two totally different categories. The first was kind of the traditional cybersecurity responsibility at Facebook.

Facebook at the time had something like 2 billion users, millions and millions of computers, and 17 data centers around the world. And so the core part of the responsibility was securing those systems and user data from attack.

As you can imagine, Facebook was -- had a very high threat profile, so we dealt with some of the worst attackers in the world trying to get access to user data or to our intellectual property.

The other side was in support of what is generally called the trust and safety mission in Silicon Valley, which is preventing the platform from being used to cause harm. Now, trust and safety, actually most of that belongs in other parts of Facebook, but as CSO I had the investigation teams that did kind of the really high-end problems. So I had a child safety investigation team that was the team of last resort if there were child safety issues.

I built a counterterrorism team so that -- you know, when I started, one of the biggest issues going on was the use of the platform by ISIS. So we built a new counterterrorism investigations team specifically around ISIS, but then expanding out to other kind of extremist groups who were using the platform to cause harm.

We also had a threat intelligence team whose job it was to investigate governments trying to manipulate the platform, and that would be both them using the platform to cause direct cyber attacks as well as things like disinformation and such.

Q Before we get any further, can you -- are you familiar with the terms "misinformation," "disinformation," and "malinformation"?

A I am, yes.

Q What is your understanding of the difference between those three terms?

A So the problem is that these words are used colloquially in different ways at different times. We try to be very careful with EIP just to make sure that we're all on the same page. So we actually have an index here.

By the way, if you guys want the nice paper copy, we can leave you --

Mr. Bellinger. We brought you some swag.

Mr. Stamos. I'm happy to sign that if you want.

So if you don't mind, I'll read from the definitions, which is what we tried to use for these projects.

Misinformation is information that is false but not necessarily intentionally false. Misinformation is at times used as an umbrella category for false rumors, disinformation, and other types of false and misleading information.

This is page 247 of EIP report. Disinformation is false or misleading information that is purposefully seeded or spread for an objective; e.g., a political or financial objective.

This goes on, but effectively the big difference here is misinformation is something that might be untrue but either the speaker doesn't know it's untrue or is not spreading it maliciously, where as disinformation they know something is untrue and then they're spreading it.

Malinformation is a term I try not to use because it doesn't really have any kind of reasonable academic definition.

BY [redacted]:

Q In your experience, is malinformation used by government agencies?

A I am sure there are people who work for the government who have used the term "malinformation." Again, that's not my favorite term.

Q And when it is used by -- we'll stick with government agencies -- what is the most common definition?

A I mean, the mal comes from harm -- they're trying to utilize the same framing as malware, which is software that causes harm. So I expect they mean information that causes harm.

Q Which would seem to overlap with disinformation?

A Not necessarily. I mean, disinformation -- the definition is things that the speaker knows to be untrue that they're spreading for a purpose. I think if you're saying malinformation, the overlap would be if it was actually harmful that it was being spread. Again, that's why I don't like the word "malinformation." I don't think it really means anything.

Q Can malinformation be truthful?

A Again, I don't use the term "malinformation." Disinformation can be based upon a kernel of truth, where then the kernel of truth is used to tell a story that is not true, and that's actually an extremely common disinformation tactic.

Q When you've heard government agencies use the term "malinformation," have they ever used it with the meaning that malinformation includes truthful information?

A I can't think of an exact -- a situation where somebody has defined it well enough for me to know what they meant. If they meant including truthful information, it's possible.

Q Okay. You mentioned in your opening statement you're here briefing government partners. Is that right?

A Yes.

Q If --

Mr. Bellinger. And Congress.

Mr. Stamos. And Members of Congress, yes?

BY [redacted]:

Q Great. And I suspect this is not your first time doing so?

A It is not.

Q When government partners use a term like "malinformation," is there an effort to clarify what they mean by that?

A I've never corrected somebody's use of malinformation. I see it as a term that tries to encompass this entire field of trying to study misleading things said online. But I'm not going to go correct somebody, no. Again, it's not my preference to use it.

Q We'll use the terms "misinformation" and "disinformation" as you've defined them, but if at any point you intend to use them differently, just let us know.

A Sure.

Q You mentioned that Facebook is part of the second half of the trust and safety mission that you have played a role in. That included efforts related to disinformation? Is that correct?

A It did. That effort did not start until after the 2016 election.

Q Okay. And can you say a bit more about what that effort looked like in your role at Facebook?

A Sure. So, after the 2016 election, there were a lot of discussions of -- we knew that a number of untrue things or incorrect stories were being spread on Facebook. The term at the time that everybody used was "fake news," which as we all know is a term that doesn't mean anything anymore, but people were talking about fake news on Facebook. And there was a project that started in early 2017 based upon me going to the executives at Facebook and briefing them on the possibility that some of the fake news had been spread by government actors.

And our reason for believing that was that earlier in 2016, we had detected -- we had a threat intelligence team that are people who are dedicated to different threat actors, so we had a China team, we had an Iran team, we had a Russia team. And the Russia team had been following actors that we knew to be working for APT28, which is the hacking team that is part of the GRU, which is the main intelligence directorate of the Kremlin. We don't really have an equivalent, something between NSA and DIA in the U.S.

And so we had observed GRU actors using Facebook for -- to map out people who are working for a number of Democratic groups, including the DNC and the Clinton campaign, I believe maybe the DSCC, because what we knew is that the initial targeting and surveillance of individuals of what we call the kill chain of the steps that an attacker takes to take over somebody's account often started on Facebook because everybody had a Facebook account. It's a great way to map out these networks.

And so we saw these GRU agents doing that work, and then we notified the FBI of that. I'm not sure what happened to that tip. That's a whole other discussion that perhaps got dropped on somebody's desk somewhere. As you know, there was an intrusion into a number of systems, none of which those intrusions happened on Facebook, but then later what we saw was the creation of fake accounts by GRU agents by same infrastructure that were then used to spread information that had been stolen from the DNC server, from Podesta's Gmail account, the other kinds of things that had been targeted by the Russians that summer.

And so we had taken action against that, but we were unaware at the time of what we later figured out, which was that there's a large completely separate Russian campaign to try and influence the platform being run from private institutions. So after the election we talked to the senior executives that we need to look into this fake news thing, and so a project was spun up in early 2017, of which I was one of the leaders. And through that project and then a subsequent one, we eventually found all of the activity by the Internet Research Agency and some other private institutions, mostly run by Yevgeny Prigozhin -- I can give you the spelling of that later, ma'am -- to influence the platform. And that's all information that was then released somewhat famously, infamously, I believe, in September of 2017.

Q With respect to both the 2017 project and, just more broadly, efforts related to disinformation on Facebook, did that include any involvement with revising Facebook's content moderation policies?

A Yes. After the discovery of all of the IRA activity, one of the things we figured out was a great deal of it did not violate any of Facebook policies. This is because the kind of professional trolls knew exactly what our rules were and would go up to the line without violating them. And one of the things we did not have a policy on was using hundreds or thousands of fake accounts to pretend to be people who you weren't.

And so coming out of that, one of the policies we created was the Coordinated Inauthentic Behavior policy, which, effectively, you can call it like a RICO for online manipulation, that you're not allowed to have a conspiracy to create lots of fake accounts and then push any information, whether or not it turns out to be true or false, that the activity of the group lying about who they are, that it is that itself that is manipulative and a kind of platform manipulation.

So that became the basis of our takedown of a number of Russian groups and then eventually Chinese, Iranian, and I think continues to be one of the base policies that Facebook uses in this area.

Q During your time at Facebook and with the development of this Coordinated Inauthentic Behavior policy, is it fair to say it was actor and behavior based?

A Yeah. So it sounds like you're listening to our podcast. I appreciate that.

Yeah, so there are three -- for the whole group, there are really three kinds of policies that you have in content policy: actor based, who's the speaker; behavior based, what are they doing; content based, what they're saying.

And, yes, that is a policy that was really about -- mostly about behavior, somewhat about actors. There were separate policies that effectively -- if you belong to searching groups that have been determined to be manipulating the platform, you're not allowed on. And so effectively the Internet Research Agency was declared persona non grata on Facebook. And so even like the personal Instagram accounts -- Russians love Instagram, it turns out. This is actually an interesting thing for us in the investigation. A bunch of them went to a wedding together, and so we were able to partially map out the IRA network because they had tagged all of their coworkers in a wedding photo.

And so we actually took down all of those accounts, because if you had any relationship to Prigozhin's kind of troll farm ecosystem that you were no longer allowed on the platform. The CIB is really more, with the B in there, behavior based, the behavior of that group.

Q So the CIB, is it not content based?

A As of the -- the initial intention was for it to be about the behavior, the overall behavior of trying to lie about who you are. I cannot speak as to the exact definition of CIB now because a lot has happened in the last 5, 6 years, and so it's quite possible that the CIB policy has changed to have more content components.

Q In 2018, before you left Facebook, you mentioned CIB as one of the content moderation policies. Was there a section of the content moderation policies that was content based?

A Most of the content moderation policies are content based.

Q And did you work on any of those policies?

A I don't -- that was not a core responsibility of the CSO. I specifically worked on CIB because it was my threat intel team that was leading the investigation into the Russian activity. I normally was not consulted on content policies, so I don't recall any other ones. It's possible I might have had input in, say, a terrorism policy since we did have the terrorism investigations. I had child safety investigations. I don't remember a significant child safety policy that changed. So I can't recall any other policies, other than CIB, where I had at least a significant input.

Q Do you recall any content moderation policies related to misinformation before you left in 2018?

A I am sure there were policies around misinformation, but I don't recall exactly what they were when I left. Again, that was not my core function. The CSO doesn't do a lot of policy work. There's an entire policy organization whose job it is to create those.

Q Do you recall the name of that team?

A Should be platform policy is when I left. I'm not sure what they're called now.

Q Okay.

A Facebook likes to reorganize the whole company about every 6 months.

Q Do you recall who the director of that team was when you left?

A Monika Bickert.

Q And just as a point of clarification, you used the term "disinformation." Initially, to your recollection, there was no efforts in your role at Facebook related to misinformation? It's not a primary responsibility. Is that fair?

A My primary responsibility related to these areas of specifically government groups who were manipulating platform, since as the runner of the threat intelligence team, which most of our work was about direct cyber, we were already studying these groups, the GRU, SVR of Russia, many states of security, People's Liberation Army of the PRC.

So my responsibility here was on the government side. It is possible I was probably in meetings about misinformation that was not government tied, but in that 2017 time frame really the big focus was on governments and then also what was the troll farms. So there's a lot of fake news that was just effectively spam. That was really being handled by other folks, but that was the other -- kind of the majority volume of the things of just straight untrue stories that were being pushed, were being pushed by groups of people who were doing it for economic purposes.

Q So you leave Facebook, and Stanford is your next place of employment. Is that right?

A That's right.

Q Yeah. And why did you leave Facebook?

A There was a reorganization where a bunch of my people were taken away and split up to two different groups. That was happening at the end of 2017, and so I didn't feel comfortable being the CSO and the face of the company. I was the one that came here to Congress to brief on anything. I was the one who had to go to Brussels. And any country that wanted to yell at us, I was the guy that got yelled at.

And I didn't feel comfortable doing that if I didn't have the appropriate team and oversight to be able to follow through, and so I told the company I wanted to leave. And we effectively made a deal where I stayed for most of 2018 to leave the team in a good place and then especially to work on the 2018 midterms to see through most of the work that was being happened. And then I left before the quarter started. The trigger was the quarter was starting at Stanford, and so I wanted to teach my class full time.

Q Were you teaching part time earlier?

A I had taught one class when I was at Facebook. I had started what is now called the Hack Lab, which is an internet cybersecurity class for non CS majors, so I actually have a lot of lawyers and political science students. You might have some of my students on your staff one day. And I had started that class when I was still at Facebook, and it was just going to be much easier to make the transition before the quarter started.

Q Okay. And you mentioned that you served kind of as the public face for the company at Facebook --

A Yes.

Q -- and would be yelled at?

Would that include the U.S. Government as one of the entities you're referencing?

A Yes, definitely.

Q Okay. And the media as well?

A I would do media events and interviews on behalf of the company, yes.

Q Okay. Do you recall a time period where the yelling or criticism was higher than normal?

A During my entire time at Facebook, the company had lots of enemies in lots of places. But certainly in the U.S., after the 2016 election, things got much more heated.

Q And why do you think that is?

A I believe a lot -- there's a decent size of people who believe that Facebook is the reason that President Trump was elected in 2016, and they were angry about that.

Q By "people," would that include U.S. Government officials?

A It certainly included elected Members of Congress. There wasn't really anybody -- you know, the Obama administration only existed for a couple of months then after the election so, I don't recall any interactions with folks working for the executive branch. But there was a lot lots of pressure from Congress.

Q In your role at Facebook -- we'll stick with the -- when did you join Facebook? Sorry. We didn't cover that.

A 2015 I believe was the exact date.

Q Okay. During your tenure at Facebook, which Federal Government agencies did you interact with?

A So our primary contact was with the FBI. We'd work with the FBI National Security Division on all of the hacking issues that we deal with. So, say, either somebody tried to break into Facebook or we caught -- I'll give you an example. While I was there, we discovered that an Iranian group was pretending to be young staffers, had fake accounts pretending to be young staffers at the State Department and then were friending those other State Department employees, Hey, saw you in the cafeteria, would love to get coffee sometime, whatever, get the friendship, send them messages, and then were using that to see their friend lists and then possibly to plant malware on their computers.

So our team discovered this because we were running machine learning classifiers to look for malicious links and such, and we found malicious links being sent out. And once you looked, it was clearly a campaign against the State Department.

And so that was a situation in which we informed the FBI, and they put us in touch with the right people in the State Department, and then we provided our data for them to both remediate the problem and then perhaps for legal action, although we were able to trace it to Iran, so I'm not sure, but I don't think in that situation there has been any subsequent legal penalties applied.

Q Are you familiar with CISA, the government agency?

A Yes, I am.

Q And what does CISA stand for?

A It's the Cybersecurity and Infrastructure Security Agency. They like security so much they put it in there twice.

Q And do you recall when CISA was created?

A It was created during the Trump administration, I believe, in early 2019. I don't know the exact date.

Q Yeah. And so it would have been after you had left Facebook?

A It was after I had left Facebook, yeah. I believe the organization that was leading -- doing that kind of stuff was NPPD and DHS.

Q And what is NPPD?

A Other than sounding like a Soviet era spy agency, I think it's National Protection Program Director. It's something like that. But that was like the group in DHS that was doing defensive cyber -- well, there are lots of groups doing that, which is one of the reasons I think CISA was created was lots of people said cyber was their job.

Q Do you recall when you were at Facebook if you interacted as a function of your role at Facebook with this DHS subagency?

A Yes.

Q And what was the nature of your interactions?

A So the biggest interaction was I called together a meeting at Facebook I believe in the summer of 2018. I want to say June or July, but I don't know the exact date. I might be able to find it.

I think there was news reporting around it, so we could find out the date from that, in which representatives of the government who were working on protecting the 2018 election came to Facebook and met with representatives from the tech companies. So I was able to get Google and Microsoft and Snap and a couple of other companies represented there as well.

Q In addition to this subagency from DHS, FBI that you mentioned, which other Federal agencies did you interact with most frequently?

A We would interact with NSA, so we had contacts with folks at the NSA who were working on tracking specific government attackers, and so we would send information to them about that. And we occasionally would get cleared briefings on the kinds of things that we should be looking out for, as well as declassified, what are called TTPs, tools, techniques, procedures, definitions effectively what should you look out for.

If this Chinese group is going to hack you, this is you look out for. So we would get those briefings. Generally that was facilitated by the FBI, but I believe there were situations in which we'd brief them directly too.

Q Okay. Among these government agencies, was there a common understanding of what counted as critical infrastructure?

A My understanding is that critical infrastructure is defined by an executive order and so -- but that's not really my field, so I can't speak to exactly what's in that. But my understanding is the President defines what critical infrastructure is.

Q To your recollection, was election infrastructure added as part of the critical infrastructure at some point?

A I believe it was added near the end of the Obama administration, yes.

Q And in your role -- well, this would be -- yeah. In your role at Facebook, do you recall having any interactions with Federal agencies with respect to election infrastructure?

A Part of our work on protecting the election included us looking out for Facebook being used to attack election infrastructure. I know that sounds a little weird, but the reason is not that Facebook would actually run election systems, but if I was sitting in Beijing and you told me, "I want you to attack Cuyahoga County," I'd go after the people first. And that is generally how high-end attackers do their work is they go after individuals.

And so, as part of that, we were doing work in the run-up to 2018 to try to make sure that we were not used as a conduit to attack individuals who were running the election.

Q Okay. Do you recall which agencies you worked with on this issue?

A So the people who were there at that meeting and who were part of this working group were FBI, DHS. There might have been a White House representative -- I'm not sure -- and the EOP person from maybe like NSC. There probably was a representative from the intelligence community, but I don't recall exactly who was there.

[redacted]. Just quickly, when you said Members of Congress blamed Facebook for Trump winning the election, what were the specific accusations?

Mr. Stamos. I don't think I'm telling you anything new. You can just look at every night of MSNBC in November 2016. But, you know, the overall accusation was that fake news on Facebook influenced people I believe into voting for President Trump. That is the general gist of it.

And then eventually once we released our results, those accusations were much more specifically around Russia.

BY [redacted]:

Q Do you think those accusations were fair?

A I think that's very complicated. It is accurate that the Russian Federation ran multiple campaigns during the 2016 election to either raise the temperature in the American election and, in some cases, specifically to hurt Secretary Clinton. Do I think it is accurate to say without those campaigns Trump would not have been elected, that is a social science question that nobody has been able to answer, but I think people have jumped to that conclusion way too quickly.

Q You mentioned -- so you joined Stanford in 2018. Stanford Internet Observatory was created in 2019. Is that right?

A Yes.

Q And what was the purpose of creating the Stanford Internet Observatory?

A The goal was to create a group that would work on these trust and safety issues that had not really been explored in an academic context. So child safety online, counterterrorism, the kinds of things I worked at of preventing organized malicious use of the internet to cause harm was not a field that academia dealt with very well.

The example I continue to use is that when I was an undergraduate in the late 1990s, computer security was not considered a real part of computer science. There was no one to graduate class at Cal or at any major university. I had to take a graduate seminar.

People who did security were seen as kind of weird, not in the center of the CS world, and that that's where we are as of now in the kind of general trust and safety of understanding the misuse of technology outside of core packing.

And so the goal was to help organize that as an academic field, and we've done that through our own research. We've done that through creating spaces for research, so we run a journal, the Journal of Online Trust and Safety. We run an academic research conference, September 28, 29 at Stanford -- you guys are welcome. I'll set a ticket aside for you -- and through our own research and then through our teaching to try and teach classes that help educate students about this area and try to make the field more rigorous.

Q With respect to trust and safety -- and you mentioned a couple of examples, child abuse, terrorism -- would another example be mis- and disinformation?

A Yes. Mis- and disinformation would generally fall under the trust and safety umbrella at tech companies.

Q Okay. And with respect to SIO in particular and the research you're conducting, is there an element of SIO that focuses on mis- and disinformation?

A It does, and especially with a foreign element, we do a lot of work on trying to understand how foreign countries have manipulating information here in the United States.

Q You mentioned within Facebook there was at least an attempt to make a division between kind of actor, behavior based issues, as opposed to content, you know, related issues. In your academic research, is there a similar delineation?

A When we do our work, we try to talk about things being actor, behavior based, content based. You will see when we talk about policies, we make that specific, but I'm not exactly sure what you're getting at there.

Q Sure. So one subject area might be looking at actor, behavior base, so if it's, you know, a foreign state sponsoring fake accounts --

A Yeah.

Q -- that seems to be content agnostic?

A Right.

Q But is the research that is primarily looking at content based?

A So I think it matters what we're doing. So I actually have a great example here. I think Caleb has copies if you guys want.

This is an exploration we did of overall Chinese capabilities in this space, and you'll see we talk about the actors, so we talk about what groups within the Communist Party and the People's Republic do disinformation work and information warfare.

We talk about their behavior of how they do it, and then we obviously talk about the content of the kinds of things, what are the tropes they're pushing, what are the ideas they're pushing.

So I see from an academic perspective if you're trying to study what is going on with Chinese misinformation, for example, you would be doing an incomplete job if you didn't look at all three of those things.

Q As part of your research, do you look at issues that are purely content based as opposed to -- or does it always incorporate actor and behavior as well?

A I mean, there's certainly situations in which an area of content would be interesting to us, but I expect our goal then would be to explore what actors were pushing it. You know, just saying this is content is not as interesting without understanding who is the one who's the speaker or the amplifier and how they're doing that.

Q Do you recall in 2018, before you left Facebook, there's -- you mentioned the section CIB and ultimately behavior based. To the extent there was an actor-based element to it, do you recall if there was difficulty in determining if the actor was domestic or foreign?

A There would definitely be situations in which it was difficult to determine who they were, especially after we released our results in 2017, because up to that point, I think these organizations, the Chinese, the Russian groups, and such, thought we weren't looking and, to a certain extent, they were accurate. And once we had shown we were able to map these out with the technical details that they left behind, then they had to improve their ops act, their operational security. And so certainly especially after that they would start to cover their tracks.

In the pure cyber space, this is called the attribution problem, and it's actually extremely hard. I, in fact, wrote a whole blog post that you can find -- I think that is still up -- for Facebook on how we approached attribution as a private entity versus, say, the intelligence community which has different kinds of standards.

Q Before you left Facebook and you're handling CIB-related issues, would the U.S. Government provide tips or reports of accounts or networks that they thought were potentially violating the terms of service?

A When I was there, they were providing reports for actual offensive cyber. That was a frequent part of our collaboration. There was -- for the 2016 election, none of the information we used to do our investigation into Russian interference came from the government. It was all generated internally.

After our announcements in, like, 2018, I believe, and maybe right before I left, there was the first tip for a group that was doing it. And my feeling at the time was that there was nobody in the FBI or the intelligence community tracking the information warfare actors in these countries in the same way they were tracking kind of the cyber warfare actors.

Q Do you recall who that tip came from?

A I don't. It was most likely the FBI. They were the ones who would relay. If, say, SVR was spreading malware on Facebook, it would come from the FBI, and they would relay it on behalf of whatever agency might have figured that out.

Q Are you familiar with the Foreign Influence Task Force?

A I've heard that term for the different groups in the government who work together on foreign influence, yeah.

Q Okay. Have you had interactions with that task force?

A We've -- I've had interactions with people who are probably part of the task force, FBI agents and such.

Q Are you familiar with the Global Engagement Center?

A Yes.

Q What is that?

A That is a group in the State Department that tracks and I think in some cases is counter messaging against foreign groups that are trying to influence global as well as domestic speech within the United States.

Q And do you recall when the GEC -- sorry for using that term -- was created?

A I don't know.

Q What's the nature of your interactions with the GEC?

A Now or --

Q Well, we'll start, did you have any while you were at Facebook?

A I don't recall any interaction with the GEC at Facebook.

Q Okay. Then since your time joining Stanford?

A During the Election Integrity Partnership, the GEC was able to send in tips for us of potential foreign actors operating to spread disinformation about the operation of the election.

Q Okay. Setting aside the EIP, do you recall any other interactions with GEC?

A It's possible. I mean, they're at conferences. We interact with, you know, groups of people who study foreign influence all the time. So I'm sure we've had a number of interactions with them.

Q You covered this partially in your opening statement, but can you say again, just at a high level, what is the Election Integrity Partnership?

A The Election Integrity Partnership was -- it doesn't really exist as of this moment -- well, we are finishing our 2022 report. Right now there's not an organized group doing this kind of gathering. But at the creation in 2020, it was a group of four institutions to study the narratives that were being spread around the operation of the election in 2020.

Q And can you say what those four institutions were again?

A So it was us at Stanford, the University of Washington's Center for an Informed Public, Graphika, and The Atlantic Council DFRLab.

Q And you said it was the University of Washington's Center for an Informed Public?

A Yes.

Q And what is that?

A That is a research group a lot like ours run by a number of professors, including Kate Starbird.

Q Okay. And what is Graphika?

A Graphika is a private company that makes tools to study manipulation of platforms with a specific focus on Twitter.

Q And what is DFRLab?

A They are a research group within The Atlantic Council that publishes a lot on foreign influence campaigns in the U.S.

Q Before EIP was created, had you worked with the Center for an Informed Public?

A Yes.

Q And what was the context of your previous work?

A We had a number of interactions. I don't know if we ever copublished, but we ran into them all the time. Kate Starbird is a very prominent member of the academic field studying this kind of stuff.

Q And before the creation of EIP, had you worked with Graphika before?

A We had had interactions with Graphika, and we had used their tools to do some of our research.

Q And by "we," you mean Stanford?

A Stanford, yes.

Q Had you worked with Graphika when you were at Facebook?

A I think we had conversations with Graphika. I don't remember exactly what the timing was of Graphika actually releasing their products. I'm not sure.

Q And prior to the formation of the EIP, had you worked previously with DFRLab?

A Yes. We, again, see them at conferences and such, and I think we had worked on some of the same reports on foreign influence campaigns. They had particular folks on Iran, so I think it might have been some of our Iran work.

Q And had you worked with DFRLab while you were at Facebook?

A We -- my team did certainly have a relationship with them. I'm not sure I had any direct relationships myself.

Q Do you recall what the nature of your team's relationship was with DFRLab?

A Our threat intel team would work with think tanks and nonprofits who worked on understanding foreign influence in attacks. So they would have those relationships with folks. I don't recall any specific projects together. A lot of that kind of -- the relationship with direct research projects working side by side occurred after I left.

Q Okay. Once CISA is created, 2018, 2019, before the formation of EIP, did you have any interactions with personnel at CISA?

A I'm sorry. Can you say the time frame again?

Q Sure. So from CISA's creation up until prior to the formation of EIP, did you have interactions with CISA?

A Yes.

Q What was the nature of your interactions?

A So we had invited -- we had CISA folks speak on campus multiple times, including Chris Krebs gave a talk to students and ran a recruiting event, because in those early day of CISA that was one of the things they were trying to do was to get some new blood. He, if I recall, was not super happy with some of the folks he had absorbed from the DHS Civil Service System, and he was looking for people with more -- younger folks with more cyber expertise. And so we had had those interactions with CISA. I'm sure there were other ones as well.

Q Who is Chris Krebs?

A Chris was the first director of CISA and is now my business partner in a consulting firm.

Q Okay. And what does your consulting firm do, just at a high level?

A We do cybersecurity consulting for large companies with a geopolitical focus.

Q Okay. Do you have any government clients?

A We do not do any government work, no. I don't know if you've ever filled out a GSA schedule, but it's not fun.

Q Do you know how long Mr. Krebs was director of CISA for?

A From its inception until he was very famously fired by tweet in either November or December of 2020.

Q Yeah. And when did you two form your consultant business?

A In January of 2021.

Q Do you recall who first came up with the idea for EIP?

A It was me.

Q Okay. And what was the motivation? What was the purpose you were hoping EIP would accomplish?

A So no matter what, we knew we were going to have to do some study around the 2020 election. This was clearly going to be an event that was going to play out massively on social media. And I was really afraid of foreign interference attempts being repeated against the 2020 election, not just this time from the Russians, but something that I had observed both at Facebook and then at Stanford is the publicity around what the Russians did in 2016 had caused lots and lots of countries to massively build up their capabilities. The biggest beneficiary there would be China. But really almost every country in the world now has some kind of capability to manipulate social media.

And so we were going to do some kind of study, and it was going to be a big thing. And so the goal was to spread the work across multiple institutions and be able to get help so that we didn't end up with three or four different groups repeating the same work, that we could work collaboratively, and then do our own academic research based on the data that we had gathered.

Q And if I just understood part of your answer correctly, you said the publicity -- is this following the 2016 election -- led foreign states to invest more?

A I think the publicity is one thing. In the China situation and particularly the other thing that really accelerated -- and this is something we actually talk about in that report -- that accelerated their capabilities was first the uprising in Hong Kong.

So the PRC and the Chinese Communist Party found themselves getting, honestly, their butts kicked by teenagers in Hong Kong, by young millennials who were much better, and they found themselves, like behind the ball of their ability to control the narrative about what was going on there. And the second was COVID. The Chinese had a very big focus on trying to control the narrative around the origins of COVID, China's responsibilities, the quality of their vaccines, all that kind of stuff.

And so between those two things, there was a big investment, from what we can see in our research, in Chinese abilities in the non-Chinese languages. They always had a massive capability in Mandarin and other Chinese languages, the important paper that's written by Jennifer Pan, who's a colleague of mine at Stanford. But their ability in English was actually quite poor, and there's a big acceleration post Hong Kong and then during COVID into creating a capability to manipulate the United States, manipulate people in Spanish, manipulate people in German, stuff like that.

Q Do you recall, or to the extent you have knowledge, of when it came to Russia's efforts to interfere in the 2016 election how strong their capabilities were with respect to influencing English-based networks?

A I mean, I could just -- I don't have -- there's no power ranking here. I can't give you, like, the AP Coaches Poll on who are the best disinformation actors, but the

Russians had two decent sent capabilities. The first was their capability in their intelligence agencies, specifically GRU, because they were able to pair up an information warfare capability with actual cyber operations. And so that's what made the GRU component really powerful is that they had the ability to actually break in and steal people's emails, steal documents, and to do technically advanced stuff and then use that to power their disinformation work.

On the other side with the troll farms, which had an ability to push stuff, but they weren't as technically advanced and were a little bit disorganized in their work, so I would say the capability the Russians had in 2016, while at the time was a big deal, was pretty weak compared to where a number of countries are now.

Q And when you left Facebook in 2018, was it your sense that the company was well prepared to handle issues related -- actually let me strike that real quick.

Are you familiar with the term "foreign maligned influence campaigns"?

A Yes.

Q And to your understanding, what does that phrase mean?

A Foreign means not American; malign meaning malicious, trying to cause harm; influence to try to change people's minds.

Q Okay. And so these examples with China and with Russia, you put those as types of -- consider those parts of foreign malign influence campaigns?

A Yes. I mean, I think each specific set of actions would be considered a campaign, yeah.

Q Okay. When you left Facebook in 2018, did you think the company was well prepared to handle foreign malign influence campaigns?

A The company was much better prepared than it was in 2016, in that there was a group working on this. There were people in threat intelligence whose job it was to specifically track the information worker actors and not just the offensive cyber actors, and there were policies like the CIB policy that actually covered it.

So, yes, I thought the company was in much better shape. It was very hard to know what was coming, so I'm not sure what I thought about -- I don't recall what my exact thought was of whether they were ready or not, but I knew they were in much better shape.

Q Okay. And with respect to, we'll say in 2020, summer of 2020, a few months before the election, do you recall what your understanding was as far as whether large social media companies like Facebook and Twitter were well prepared for foreign malign influence campaigns in the lead-up to the 2020 election?

A Yes, I think they were generally well prepared for that.

Q Okay. And what sort of changes do you think they adopted to be prepared?

A So they had teams that were specifically looking for it. They had policies to cover it. They had collaborations. There had been a long history of collaborating on cyber issues in Silicon Valley that really come out of 2009. There was a big People's Liberation Army attack against a big chunk of Silicon Valley called the Project Aurora Attacks. I actually got to help in the incident response for that. And that was like a huge deal. If you remember, that's when Google pulled out of China famously. They shut down their China operations. That was a big deal because it indicated that tech companies were playing at the same level as the defense industrial base, big banks, stuff like that.

And so that collaboration existed really on the offensive cyber operations, and they used some of the same kind of capabilities then to study and stop information warfare actors. So if one company found we have this group in Iran that is creating fake accounts that they could share, here are the email addresses, here are the phone numbers with another platform, and they could go find the similar aspects.

So there's that kind of collaboration that was happening. There were dedicated teams. I do think the companies were in better shape for 2020.

Q So going back then to, what was the goal with forming the EIP? What need were you looking to fill?

A So there are really three big gaps that existed that we wanted to fill that had not existed in 2016.

The first was to create a real-time historical record of what was happening. Lots of content on social media is ephemeral. It can be deleted by the actors. It can be deleted by the platforms. It kind of can get lost in the sands of time. And one of the things we found coming out of 2016 is there's no good historical record of what actually happened, and that's generated a lot of disagreement about the size and scope of these campaigns.

The second was to do academic analysis of how were the actors operating, how does information flow in these platforms, and what were the responses of the platforms, and the possible effectiveness of those responses.

And then the third was to provide a help to local and State election officials, who had really very little capability to stand up against dedicated information warfare actors by themselves, to help them understand what was going on in their own backyards.

[10:31 a.m.]

BY [redacted]:

Q For that third purpose, how did you gain this understanding?

A I'm sorry. What do you mean?

Q Sure. So the third purpose is to help State and local election officials. At what point did it come to your attention that State and local officials, based off your understanding, were ill-equipped to handle these kinds of issues?

A So, before 2020, I had been a part of a number of groups that had met with NASED, you know, the National Association of -- well, there's the National Association of Secretaries of State, and then there's a National Association of State Election Directors.

So, of the different groups that represent the local and States -- this is where you'd have Matt Warner and other kind of prominent secretaries of states talk about the things they were doing to protect in 2020. In those situations, they talked about their need for help.

I think America is the only advanced democracy in which we devolve our elections into thousands of localities. That has a lot of benefits of allowing local control and probably gives us security benefits in that it makes it very hard to steal an overall election because there's a huge diversity in systems and capabilities. But the flip side is that you end up with these local government officials having to stand up to state adversaries.

I live in San Mateo County in California. The people who run the elections are nice people, but the idea that they're going to protect their systems against the People's Liberation Army just doesn't make sense. If the People's Liberation Army Air Force flew over San Mateo County, that is not the San Mateo County Sheriff's Department's responsibility to have a SAM site, right? That's the Air Force.

And so a lot of this discussion was happening in the runup to the 2020 election about how centralized help could -- from the Federal Government, from other nonprofits and such -- could be provided to local and States on cyber issues. But it also became clear in those meetings that they had challenges around the disinformation side that were probably not going to be met.

Q Okay. And just to be clear, these meetings occurred once you were already at Stanford?

A Yes. Yes.

Q Okay. Do you recall when you started to meet with these types of groups?

A I don't have an exact recollection. I'm guessing in late 2019, early 2020.

Q Okay. And, when you were meeting with them, would it be with -- you mentioned nonprofits and the Federal Government. Were these meetings with representatives from nonprofits and the Federal Government?

A There were people from nonprofits and Federal Government at these events. NASED events, NAS events, and such.

Q Yeah. Which Federal agencies were involved?

A Well, certainly CISA, which I believe now existed at this time, Federal Elections Commission, EAC, the Election -- I think -- Assistance Commission is what that stands for. I believe those are the three that you would normally have from the government.

Q And do you recall who from CISA would attend these meetings?

A So you'd see Matt Masterson a lot. Krebs himself would come. Probably some other folks. I don't recall everybody.

Q Okay. Who is Mr. Masterson?

A Matt Masterson is probably the man who knows more about election security than any other living American. He has worked in elections at the local level, at the State level, at the Federal level. He worked for CISA. He was -- I don't know his exact title, but he was effectively kind of a special assistant to Krebs on election security in 2020.

After he left CISA, he came and spent a little bit of time with us to document everything he had learned and to do a report on what he had learned out of the 2020 election. Now he works at Microsoft, I think, in their group that supports election security.

Q Okay. Do you recall when in 2020 you first began considering the formation of EIP?

A Yeah. So, in the early summer of 2020, I had a conversation with one of my students who was interning at CISA. And, in that conversation, we talked about how there was no kind of support currently being offered on the disinformation side to local States.

And so we had already been planning at that moment to do some kind of study in the fall, but this is where it became clear of -- if we're going to put a group together to work together on the election, that another function that we could provide would be that support.

Q Okay. In addition to the student, who else did you consult with in the summer of 2020?

A Well, then we ended up sending emails to a number of stakeholders. Obviously, the other groups that were part of EIP. And then we had meetings with CISA to get their feedback.

Q Yeah. And who at CISA did you meet with?

A I don't recall exactly. I expect it was Matt Masterson, Brian Scully. Those were key people at CISA. And probably a variety of other people.

Q Who is Brian Scully?

A He was an important person at CISA. He's now at NSC. I don't know his exact title at CISA.

Q Okay. Did you consult with Chris Krebs in the summer of 2020?

A I probably did, yes.

Q Do you recall what sort of feedback anyone from CISA -- whether Mr. Krebs, Mr. Masterson, or Mr. Scully -- provided?

A I don't recall exactly what they said, but the outcome was that they introduced us to the Election Integrity -- Election Infrastructure ISAC people, and we built the relationship with the EI-ISAC to be able to relay these -- to introduce us to local and State partners and to relay the requests.

Q Okay. And what is EI-ISAC?

A The Election Infrastructure Information Sharing and Analysis Center.

Q Great. And we can stick with the acronym.

A Yeah. That's fine. Thank you.

Q And what does EI-ISAC do?

A So the ISACs are nonprofits that coordinate security inside of a sector, often a critical infrastructure sector. The ISACs have been around for a while, this idea. I believe the first ones were designated by an executive order. The canonical one that everybody uses as an example is FS-ISAC, the Financial Services ISAC, where you have thousands of banks -- big ones, small ones -- sharing real-time information about bad things happening, and then the big banks providing support to the little ones.

And so the idea of an ISAC is collective defense, that you're in better shape if one person gets an attack, that they tell all of their friends "I'm getting an attack from this IP address" or "I just saw this piece of malware or "I find this vulnerability in this product; we should get this fixed," that you work together in the ISAC to get that kind of support.

So the EI-ISAC is a similar thing. I believe the central management of it is by the Center for Internet Security, which is a nonprofit that actually runs the kind of coordination, but most of the work is then done by the members themselves who are sharing with one another.

Q Okay.

BY [redacted]:

Q The student you mentioned, was that an undergraduate student that was interning at CISA while --

A Yes. We had four students who were working at CISA. Three of them were new interns. One had had a preexisting relationship. All of them, I believe, at the time were undergraduates.

Q And they were interning for the summer? Or what was the duration of the --

A For the summer. One of them, again, had a preexisting relationship because he had done lots of work in hacking. He had actually hacked the Pentagon as part of a program and did some other stuff like that. So he had a relationship that, I think, postdated the summer. But three of them were there just for the summer.

BY [redacted]:

Q Okay. Do you know who funds CIS?

A So I can't speak to all of their funding. I know they get government grants.

Q Okay. Do you know which government agencies provide the grants?

A Relative to this, I believe they get a grant to run EI-ISAC from DHS.

Q Okay. And do you know if that's true for all of the ISACs? You mentioned there were multiple.

A Which ones get government-funded, I'm not sure.

Q Okay. By DHS, is it your understanding that CISA in particular provides the grants to CIS?

A I can't speak to who the grant holder is.

Q Okay.

A I believe the EI-ISACs predate CISA. So I'm not sure how that would affect it.

Q Okay. Did you ever interact with the EI-ISAC while you were at Facebook?

A It's possible. I don't recall. It's possible they had a representative at our meeting, but I don't -- it's possible.

One of the projects we did at Facebook is we tried to gather up the Facebook accounts of all the key election officials because we wanted to -- this is something that we had done first for the German and French elections, which occurred right after the U.S. elections, in which the German equivalent of CISA helped gather up all of the key people who were running the German election so we could mark their accounts as being high-risk.

So, if a bad guy takes over your Facebook account -- it happens every day -- nobody is going to notice. But, if the bad guy takes over the Facebook account of the key technical person patching systems for a swing State, that's something we want to know.

And so we had done a bunch of work that summer to identify those thousands of people who might be targeted as part of a campaign so that we could -- we push notifications for them to turn on two-factor. We force them to change their passwords if their passwords were weak. And then we had special monitoring so if a bad thing happened to that account, it would get locked and a human being would look instead of just allowing them to deal with it themselves.

And so it's possible we worked with EI-ISAC on that, but I don't recall exactly who our contact was for that.

Q A couple answers earlier when talking about the different ISACs, you referred to critical infrastructure. Did you mean to refer to critical infrastructure as used by the executive order you referenced earlier in the hour?

A My understanding is the initial ISACs were created by executive order tied to the critical infrastructure sectors. So there's a national health. There's a power generation, you know -- maybe it's called energy ISAC.

But there's ISACs -- aviation -- for critical infrastructure sectors. I believe there's ISACs outside of those, too, but that's the original idea.

Q And you mentioned that election infrastructure was added to critical infrastructure at some point in the Obama administration?

A That's my understanding, yeah.

Q Do you know if EI-ISAC was created after that change occurred?

A I am not an expert in the history of the EI-ISAC. I believe it preexisted, but I'm not totally sure.

Q Okay. And the Center for Internet Security, other than its operation or helping facilitate the EI-ISAC, had you other interactions with CIS at your role at Stanford before the formation of EIP?

A It's possible, but I don't recall any specific ones.

Q Okay. What about during your role at Facebook?

A Again, it's possible, but I don't recall.

Q What was the reason for consulting with the individuals you did at CISA before the formation of EIP?

A We were offering to them that, if they got reports from their local and State partners, that that's something that we would like to have; one, because we were trying to make the most complete historic and academic record of what was going on, and that we could then provide support through our own exploration of these issues and communicate back to them.

Q So does CISA have any role to play with EI-ISAC?

A I can't speak to the exact relationship between CISA and EI-ISAC?

Q But it's your understanding that there was some relationship between the two?

A My understanding is that they were working together to help local and State officials, that a core challenge of CISA is that they have responsibility for helping secure the election but no real power to do so. And so they need to be a service provider, and that EI-ISAC was one of the tools for which they could provide a service to these local and State election officials so that they're not totally by themselves while securing the election.

[redacted]. Okay. Can we go off the record, please?

[Recess,]

[redacted]. We can go back on the record. It's 10:53 in the morning.

EXAMINATION

BY [redacted]:

Q Mr. Stamos, good morning again.

I want to ask a couple questions based on the prior hour. I don't think we ever got a definition of the term "election infrastructure." What's the definition of that term?

A As I would use it, it would be the systems that are actually used in the -- all the different parts of election, from the registration systems, to the poll books, to obviously the systems that print ballots, scan, if appropriate, ballots, tabulate the results, all the way through the ways in which the results are then announced to the public or sent to the media, which is a part that people often forget about because that last part is actually quite critical.

Q You say systems. Does systems mean machines? Software programs? What does systems mean?

A All of the above. Computers, specialized hardware, software, firmware, all the different components that go into supporting the election, as well as -- I would define it including the normal IT systems of election -- you know, I said San Mateo County. So the Windows desktops of San Mateo County would be part of that infrastructure.

Q So is it fair to say that it's really the technical things that make elections work?

A Yes. I think that's accurate.

Q Okay. I want to turn to -- I think we talked a little bit earlier about the purpose of the Stanford Internet Observatory. I just want to talk a little bit more about the SIO.

And I'm sorry. The Stanford Internet Observatory is sometimes abbreviated as SIO, correct?

A Yes.

Q So I'm going to use that phrase going forward.

A Sounds good.

[redacted]. So I want to introduce Exhibit -- I think this is our first exhibit, actually -- exhibit 1, a printout from the about section from the SIO website.

[Stamos Exhibit No. 1

Was marked for identification.]

BY [redacted]:

Q And I should say, we printed this off in reader view, so this is not exactly how it appears on the website. We couldn't get it to print appropriately just hitting control P.

Are you familiar with this?

A I mean, this looks like you got it from our website, yes.

Q Okay. And I want to read the third paragraph down into the record. It says: The Stanford Internet Observatory is a cross-disciplinary program of research, teaching and policy engagement for the study of abuse in current information technologies, with a focus on social media. Under the program direction of computer security expert Alex Stamos, the Observatory was created to learn about the abuse of the internet in real time, to develop a novel curriculum on trust and safety that is a first in computer science, and to translate our research discoveries into training and policy innovations for the public good.

Did I read that correctly?

A Yes.

Q Okay. What does "abuse of the internet" mean in this context?

A So, when we talk about abuse, that is misuse of technology to cause harm in a way that's technically correct. So that's what differentiates us from hacking or traditional cybersecurity, is that when you abuse an online system, you're using it in the way it's intended to be used, but the outcome is that something bad happens to somebody.

Q And so harm means something bad happening to somebody. Is that how you would describe it?

A Yes.

Q Okay. And the paragraph says that -- that I just read says that the SIO was established to, quote, learn about the abuse of the internet.

What does "learn about" mean in this context?

A So, as I was discussing with [redacted], one of my goals here was to help create a more stable academic basis for kind of assumptions that people have always made about things that happen online and the responses. We don't have, like, a good qualitative or quantitative basis to understand what kinds of things are going on, what are the actual harms, and then if the things that companies do -- whether they actually have any positive impact.

Q So is it fair to say that the SIO is primarily a research-focused entity?

A Yes.

Q Okay. And SIO -- you mentioned in the earlier hour a couple different areas that you've looked at. Is it fair to say that you're not focused solely on elections; you're focused on a wide variety of things that happen on the internet?

A That's right. We look at a number of things of different kinds of abuses. We do try to restrict ourselves to adversarial abuses. So where there's somebody who is actively doing something bad. But, within that space, we have a pretty wide variety.

Q And actively doing something bad, why is that important for you to restrict your focus to that?

A So there's a lot of people who study, is the internet bad for you? Are phones melting kids' brains? Totally legitimate area of study.

My colleague Jeff Hancock, who is now our faculty director, is a psychologist and has much more of a background in that. For my particular background, coming from a cybersecurity training and then working on specifically stopping people who are child abusers or stopping government agencies, I felt that my skill set was better applied to that area, to adversarial abuse.

Q Okay. And I want to look at a recent example of a type of abuse that SIO has looked at.

[redacted]. I want to introduce as exhibit 2 the key takeaways in the background section from a report entitled "Cross-Platform Dynamics of Self-Generated CSAM."

[Stamos Exhibit No. 2
Was marked for identification.]

BY [redacted]

Q This was written by yourself, David Thiel, and Renee DiResta, and it was published by the SIO on June 7, 2023.

A That's correct.

Q And you're familiar with this report?

A I helped write it, yes.

Q Okay. What is self-generated CSAM?

A So CSAM, child sexual abuse material, is the term of art we use in the industry to refer to child pornography. For a variety of reasons, child advocates do not want to use that term, so we say CSAM.

SG CSAM, self-generated, is content that was created by the child themselves with their consent, to the extent that a child can consent to anything. This is about specifically commercial SG CSAM.

So you can have the noncommercial, which is effectively teenagers sending each other naked photos of themselves and such. Sexting, I think, is what a teenager would say. I feel incredibly old saying that with air quotes.

This is specifically about the commercialization of that kind of technique.

Q Okay. And, on page 3, the first full paragraph on the top of page 3 says: After being alerted to specific hashtags and keywords commonly used in this community, SIO began an investigation to assess the scope and scale of the practice and to examine how platforms are succeeding or failing in detecting and suppressing SG CSAM. During this process, we identified hundreds of accounts dedicated to selling as well as likely buyers detected by social graph connections and public account metadata. These sellers and suspected buyer accounts were referred to the National Center for Missing and Exploited Children, or NCMEC, for further investigation.

Did I read that correctly?

A Yes.

Q Okay. What is the National Center for Missing and Exploited Children or NCMEC?

A NCMEC is the federally -- the congressionally designated recipient of all reports in the United States about child sexual abuse material. They are effectively the only people in the country who are legally allowed to hold on to this material. And so they are the clearinghouse that the tech companies work with if they ever find reports -- if they ever find bad stuff, they are legally required to send that to NCMEC.

Q So is this an example of an investigation -- or a study, I guess, I should say -- that SIO did that you researched various posts, various types of content online, and then certain ones were essentially flagged and submitted to NCMEC?

A Yes. That's right. So this was an academic study -- what you would call this is a descriptive white paper. We are now preparing the manuscript to be submitted to a peer-reviewed journal. That's a process that takes a year and a half, 2 years.

And one of the reasons we did this preprint specifically is because we thought the abuse was so bad that going public with it would help us motivate the companies and motivate law enforcement into taking action.

And then we also reported to NCMEC. I do not believe we have a legal obligation to do so. So I believe it's 18 U.S. Code 2258a that requires electronic communication service providers, of which we are not. But we thought the only ethical thing we could do in this case would be to hold ourselves to the same standards as Facebook or Twitter and such.

Q Okay. And so you found this problematic material, and you reported it to somebody who could potentially take action on it. Is that fair to say?

A That's right. Yeah. We briefed NCMEC. We provided them with our Maltega graphs and such with the data that we had gathered around this, and then I believe they did forward it on to the FBI.

Q Okay. We talked earlier about misinformation, disinformation -- I guess malinformation, although you said you don't use that term.

A I don't.

Q But do you recall that discussion generally?

A Yes.

Q You've been studying disinformation for a fairly long time. Is that fair to say?

A I would say that this has been an area of kind of -- organized disinformation has been an area I've been studying since the results of the 2016 Election and the investigation I helped run in 2017.

Q And by "organized disinformation," you mean disinformation spread by state actors?

A By any actor who is working to do so intentionally. So it's something that I have studied. I try not to call myself a disinformation expert. And certainly I'm not an expert in the overall kind of psychology of these issues. But I do know a lot about how people use platforms to spread disinformation.

Q Okay. In your experience -- and I'm sorry.

You said earlier you previously worked at Facebook, correct?

A Yes.

Q And you previously worked at Yahoo?

A That's right.

Q In your experience, both in your current role and based on your prior experience with social media companies, do social media companies have reason to be concerned about the spread of disinformation on their platforms?

A Yes.

Q Why is that?

A Social media companies exist to show ads to people. If you want to show ads to people, you have to have inventory. Inventory is somebody who is looking at their screen, and they're scrolling through, and they're reading all day. You have to have engagement.

What keeps people from wanting to use social media is if they feel it's a bad experience. And that could be an abuse that's really directed against them, or it could be that overall they feel like it is a -- that this is no longer a platform that they can trust.

And so I do think the platforms do have a responsibility for all trust and safety. There's an economic incentive to make it an experience that people want to have. And, for a lot of people, that includes not being intentionally lied to.

Q Okay. And so I just want to reemphasize what you said. The companies have an economic inventive to address disinformation on their platform?

A Yes.

Q And that's because people won't -- advertisers won't want to buy ads if people are wary of spending time on the platform?

A Yes. I think we actually have a really good example of this right now, which is -- Mr. Musk's takeover of Twitter has become almost a perfect experiment that we never could set up in social science of what happens when you seriously downgrade your trust and safety enforcement. The platform has had really a growth of bots, a growth of spam, probably a growth of organized disinformation actors, although we're still trying to work that out of exactly to quantify that. And they've lost at least two-thirds of their value according to some of the reports I've seen.

And so, you know, advertisers do not want to be on platforms that are controlled effectively by a government. Advertisers don't want to be on a platform where people are spreading lies or they're lying about who they are. And users don't want to use a platform if they don't believe the people interacting with them are real.

Q Thank you. And I want to talk about coordinated inauthentic behavior a bit as well. And I think you gave the definition earlier, but I didn't write it down.

Could you remind me what the definition of coordinated inauthentic behavior is?

A It is when a group of people work together to mislead users of a platform, generally about their identity. That's the core -- the definition, I think, at Facebook now is probably actually quite complex.

But, when we started this, it was really mostly about the identity. That you can't have 20 people in St. Petersburg pretend to be 500 Americans, that we needed some kind of policy that caught that behavior, even if the individual pieces of content posted by those 500 fake Americans -- that each individual piece did not violate policy.

Q Okay. And I think you used an example earlier from the 2016 Election of Yevgeny Prigozhin engaging or leading, I guess, an effort to conduct coordinated inauthentic behavior. Is that fair?

A That's right. Yes.

Q And Prigozhin - he's a Russian, correct?

A I am pretty sure he's a Russian citizen.

Q And he is also the head of the Wagner Group, correct?

A Yeah. I believe he owns Wagner Group, yes.

Q And what is the Wagner Group?

A That's a mercenary group. So he seems to have an ecosystem of both troll actors and then groups like Wagner, which are actual physical boots on the ground.

In one of the studies we did -- I don't think I have access to it, but we could pull it up on the website -- was looking specifically on his actions in Africa, which demonstrated that he would support certain dictators in Africa with both Wagner boots on the ground as well as with disinformation activity, and in return, he would get economic benefits from those countries.

Q Okay. And so, through your time with Facebook, you determined that Prigozhin -- who had supported African dictators and is involved in the war in Ukraine in 2016 -- conducted an coordinated inauthentic behavior attack on the United States, correct?

A Yes. We were able to isolate a rather large network of Internet Research Agency accounts, and we had very strong technical attribution to specifically the IRA.

Q And why was it of concern to Facebook that Prigozhin was conducting coordinated inauthentic behavior attacks on its platforms?

A So, for the company, allowing people to manipulate the platform in the long run is not going to be good business, for sure. I think also, personally, I'm an American. Most of the people who work on this are American. So we in particular felt not happy about a foreign actor influencing our democracy.

Q The research that you did to examine what took place on the platform, did anybody in the United States Government ask you to conduct that research?

A Nobody asked us to do it. There were a number of -- you know, in the runup to that, there were a number of people talking about Russian activity on the platform and who were, you know, blaming Facebook. So if you want to call that asking.

But certainly the specific project that started, which we called Project P -- P for propaganda -- in the start of 2017 was something that was triggered by me approaching Mark Zuckerberg and his executive staff saying I think we need to do this work.

Q Okay. And Facebook, you said, has now established policies on -- and I'm sorry. I keep saying coordinated inauthentic behavior. It's abbreviated CIB, correct?

A Yeah.

Q Facebook has now established policies on CIB, correct?

A Yes.

Q Did the government ask Facebook to establish those CIB policies?

A No.

Q Okay. And why did Facebook establish those policies?

A We did not want large groups of organized people -- working for governments or not -- manipulating the platform. And so we needed a policy that caught both the IRA activity, which was government-related, as well as the Macedonian troll farms and the other kinds of organized groups that we found manipulating the platform.

Q And, when you say you didn't want people or entities manipulating the platform, is that because of cybersecurity reasons?

A We didn't want it because, just like with other trust and safety issues, it would eventually drive people away if they thought they were being manipulated. And particularly the financially-motivated stuff was very widespread and was creating a really bad experience for people.

The eponymous Macedonian troll farms -- they're not all in Macedonia -- but there's, like, a famous example of these Macedonian teenagers who were able to set up entire fake news organizations. And that really is not in the long-term interest of the company.

Q Okay. And so the companies have a financial incentive to address CIB on their networks, correct?

A Yes.

Q Okay. There have been some claims made that, when the Russians or others engage in CIB activity, they're just engaging in free speech. Have you heard those claims?

A I mean, I've certainly heard there's lots of debate about what kind of rights do you have as a foreign speaker in American elections, for sure.

Q Do you have an opinion on that?

A I do. I think -- I'm not a First Amendment scholar, as I'm sure will be really obvious throughout the next several hours.

From my perspective, I think it's completely appropriate for foreign governments to have outlets who have speech in the United States. So I don't mind that Russia today exists. I don't mind that CGTN carries the stories of the Chinese Government and the Communist Party. But I think they need to be honest about who they are.

And, from my perspective, I don't think you have a free speech right to lie about who you are and to say, "I'm just a good ol' red-blooded American from Texas, and this is what I believe," when you're really working indirectly for the Russian Government.

Q And, from the social media company platforms' perspective, the social media companies are private entities, correct?

A Yes.

Q Okay. And so social media companies are not -- if social media companies have an economic interest in controlling what's on their platforms as a private entity, they have a right to do that, right?

A I mean, that is my understanding of the law, yes.

Q I want to return to the discussion about the Election Integrity Partnership. I'm going to refer to that as the EIP going forward.

[redacted]. I want to introduce a July 27, 2020, post from EIP. It's entitled, "Announcing the EIP." This is on the EIP website. This will be exhibit 3.

[Stamos Exhibit No. 3
Was marked for identification.]

BY [redacted]:

Q Have you seen this before?

A Yes. This looks like the initial announcement post from 2020.

Q Okay. And this is dated July 27, 2020. Do you see where it says that?

A Yes.

Q Okay. Is that a fair -- is July 27, 2020, approximately when the EIP was stood up?

A Yes.

Q Okay. You said in the earlier hour that, even before the EIP, you at SIO had been talking about ways to study the 2020 election, right?

A Yes.

Q Do you have an estimate on when you first started thinking about studying the 2020 election?

A Probably right when we started SIO in 2019. I mean, it was clearly going to be the next -- it was the next Presidential election after 2016. It was going to be the most important online information event of possibly our lifetimes.

Q Okay. And -- sorry. You said it was going to be possibly the most important information event of your lifetimes. Why did you feel that way?

A Because the 2016 election -- the activity that the Russians did, as I talked with [redacted], may or may not have had a real impact on the outcome. That's a very difficult question to ask -- answer. I'm sorry.

But the coverage of it meant that anything that was happening online would immediately be seen in the frame of foreign interference and that what the Russians had done was advertise out a capability that we knew lots of other countries would want to utilize. Like I said, China was specifically the country that reacted the most to what the Russians did and to their own internal problems to build up this capability.

So I believe I used the term multiple times that this could be the Super Bowl of disinformation and that it seemed likely there were going to be many different groups who were trying to manipulate the election.

Q And is it fair to say that, in your role as head of SIO, your interest in looking at the 2020 election was primarily academic in nature? It was primarily for research purposes?

A Yes.

Q Okay. We spoke earlier about CISA, the cybersecurity and internet security agency?

A Cybersecurity and Infrastructure Security Agency.

Q Thank you. And you said you had had some meetings with CISA around the time of the creation of the EIP?

A Yes.

Q Did CISA ever ask SIO to create the EIP?

A I don't recall if they ever asked us to do anything. The EIP was my idea, and we approached them with the proposal.

Q Okay. So it wasn't like the Department -- did anybody else at the Department of Homeland Security ask SIO to create the EIP?

A No. This was my idea.

Q Okay. Turning back to this -- what we've introduced as exhibit 3, at the bottom of the page, there's a line reading: We would like to thank the Knight Foundation and Craig Newmark Philanthropies for their support of this effort.

"This effort" refers to the EIP, correct?

A Yes.

Q Are you familiar with the Knight Foundation?

A Yes.

Q What is the Knight Foundation?

A They are a nonprofit that does a lot of grants to universities for research.

Q Are they affiliated with the government?

A I don't think so, no.

Q Are you familiar with Craig Newmark Philanthropies?

A Yes. That's a one-man nonprofit by which Craig Newmark is giving away his money.

Q And is that nonprofit affiliated with the government?

A I don't think so, no.

Q Okay. So both the Knight Foundation and Craig Newmark Philanthropies are private philanthropic organizations, right?

A Yes.

Q To the best of your knowledge, in its work in advance of the election -- so say through December of 2020 -- did EIP receive any funding from any government entity?

A SIO has only ever received one government grant, and that happened well after both the EIP and the Virality Project.

Q Okay.

A I can't speak as to every bit of money ever received by anybody who worked on EIP, of course. I can only speak to SIO.

Q But to the best of your knowledge, I should say.

A Best of my knowledge, no.

Q Okay. I want to look at the second paragraph of this post. It reads: The Election Integrity Partnership is a coalition of research entities focused on supporting real-time information exchange between the research community, election officials, government agencies, civil society organizations, and social media platforms.

We talked through in the prior hour what the coalition of entities was, but I want to talk about the real-time information exchange part of this. Do you recall what was meant by that?

A We built a database in which we could collect all of the examples we found in real time of disinformation during the election. And, in doing so, we took tips and then tried to provide services back to the local and State election officials. So we wanted to have a real-time exchange between folks, as we believe that that would support our academic mission and then also allow us to report out issues that we saw happening in real time.

Q The post continues: Our objective is to detect and mitigate the impact of attempts to prevent or deter people from voting or to delegitimize election results. This is not a fact-checking partnership to debunk misinformation. More generally, our objective explicitly excludes addressing comments that may be made about candidates' character or actions and is focused narrowly on content intended to suppress voting, reduce participation, confuse voters as to election processes, or delegitimize election results without evidence.

It's a long paragraph.

A Yes.

Q I want to go through each piece in turn.

To the extent that you recall, what did "content intended to suppress voting" refer to?

A So we are -- that is specifically situations in which you might have a post that threatens people, that lies to people about the nature -- or I'm sorry -- like, the time, the place, the mechanics of voting. Traditionally, you've had things like: The vote has been canceled. The vote has been delayed. The polls are closing early. We have at least one example in our database of a bomb threat.

And so that's what we mean. Things that you would lie about online to try to keep people from voting.

Q To the extent you recall, why did EIP choose to focus on content intended to suppress voting?

A So, in all of these situations, we were specifically focused on the operation of the election itself. In this case, there is a long history of disinformation to try to suppress voting. In fact, there was, I believe, even a prosecution of people who were sending text messages telling people the wrong information about when to vote, for example.

Q Okay. Is it fair to say that this focused on the time, place, and manner of voting?

A Yes. And, in fact, this is drawn from -- if you want to see in more detail, in the EIP report itself, we break down in detail kind of our scope and specifically in these four areas.

Q Okay. And I think we'll get to that in just a minute.

A Okay. Great. But I do believe we talked about time and place and such.

Q So, to the extent that you can recall, what did "content that would delegitimize election results without evidence" refer to?

A Right. So, in this case, we were looking for claims of the election being stolen or of being rigged in such that was not based upon an evidentiary basis.

Q Okay. Why was that something that EIP chose to include as part of its research?

A So, by the summer of 2020, it became clear that the kind of traditional outlines of election disinformation were going to be pushed. By that summer, President Trump had already started laying the groundwork to deny that he had lost the election.

Q And why was it of concern -- was it of concern to you if the election result might be delegitimized?

A Yes. We have -- we had a very long history of peaceful transfers of power in this country. That's one of the things that makes us the city on the hill, as Reagan might say. It's one of the things that makes us special.

And one of my fears, personally, has been that we will end up becoming a pseudo-democracy where people never believe the election. They always believe the election was stolen. I believe that that's actually something we're trending to on a bipartisan basis.

And one of the things we wanted to understand was, what were the lies that might be driving those beliefs during that year, and to come up with -- both for us to -- as it says here, in some cases to publish and to demonstrate what is being said, and then, kind of on a longer term, to understand how can we restore trust back in the voting system.

Q So your goal in looking at that was to assess how these narratives spread. Is that fair to say?

A It's to see what the narratives were, how they were spread, who spread them, and in what situations did specific features of different platforms -- we call those affordances. How would certain platform affordances affect this issue? That's actually one of the key things SIO works on.

Back to the child safety thing we were talking about, for example, it's -- what is it specifically about this platform that makes this abuse especially work here? And so those were all kinds of things that we wanted to study.

Q Okay. So, again, it was research-focused. Is that fair to say? You wanted to study how -- these affordances?

A Yes. And we have. And we have published our results, both in this big ol' report as well as in a number of peer-reviewed journals.

Q Okay. In your opening statement, you stated that part of the purpose of the EIP -- sorry, turning away from exhibit 3 -- was to provide local and State election officials with a window into what was happening online in their jurisdictions.

A Yes.

Q When you say "a window into what was happening online," is that with regards to both how the election operations might be impacted and also with regard to potential delegitimization of the results?

A Yes. For all of the issues within our scope, which is the function of the election itself -- if you were, again, Cuyahoga County or San Mateo County, if there was a claim going viral, that's something that we wanted you to know so that you could put out your own accurate information and respond however you thought was best.

Q Okay. So EIP conducted the bulk of its collecting of research data in the lead-up to the election, so from July 2020 to November 2020. Is that right?

A That's right. We ran for -- I would have to look at the exact date, but we ran for a bit after the election collecting responses to what happened, and then we shut down before the end of the year.

Q Okay. And then, after the election, EIP analyzed what it had collected. Is that fair to say?

A Yes. We spent much of the first half of 2021 taking all the data we had gathered, and then building our database and then building our analysis, which you see the results of here and those other papers.

Q And so EIP ultimately produced a report entitled "The Long Fuse," correct?

A That's right.

Q Okay. This was published in March 2021?

A That sounds correct. I'd have to look at the exact date, but March sounds about right.

Q Okay. And did you --

A I'm sorry. We have this one marked June.

Q Okay.

A So I think it probably was June.

Q Okay. Did you play a lead role in drafting the report?

A I played a role in helping coordinate. Lots of people worked on it. I'm not going to take credit for it.

Q Okay. But you were familiar with the report's contents?

A Yes. Of course.

Q And it's the product of your research? Research that you led?

A Research that I helped supervise, yes.

Q Okay.

A But to be fair, one, there's four organizations involved and, as you can see in here, lots of people working on this who provided both the input into it as well as did the writing of the report.

Q Okay.

[redacted]. I want to introduce as exhibit 4 -- and I know you have your own copy, but I want to introduce it into the record because I think it's hard to put this into the record -- as exhibit 4 the cover page and the executive summary from "The Long Fuse."

[Stamos Exhibit No. 4
Was marked for identification.]

BY [redacted]:

Q On page Roman numeral VI, there's a line reading "what we did" and followed by three goals. Do you see where it says that?

A Yes.

Q Okay. So I want to walk through each one of these goals in that first paragraph in order.

So the first goal -- it says: The EIP's primary goals were to, number one, identify mis- and disinformation before it went viral and during viral outbreaks.

What was the -- is that accurate that that was one of your goals?

A Yes.

Q Okay. What was the purpose of identifying mis- and disinformation?

A So both that we could, as it says here, share our own countermessaging and also to inform local and State officials of the kinds of things that were going viral and then in support of our academic research. Without identifying what was going viral, then there's no way you can do any research on what actually happened.

Q Okay. And I know that the report is almost 300 pages long, and it discusses in some detail how EIP went about identifying mis- and disinformation, but can you break it down into layman's terms what was done?

A Right. So we had monitoring groups of students who had a variety of different tasks that they were given, who worked in shifts during the day so that the shifts got more frequent and longer as we got closer and closer to the election. And they would be given specific tasks to look at the output of certain things.

On some platforms, we had automated systems that were taking API data and then surfacing -- these are the pieces of content that are starting to trend on the topic of the election. And so, for example, for Twitter, we had a dashboard of -- these were, like, the biggest tweets about the election overall, and they'd look and they would discard anything that actually had to do with the candidates.

So, to be absolutely clear, we did nothing around Donald Trump is bad/Joe Biden is good and vice-versa. Any claims about the candidates, about their kids, for example -- all that stuff was out of scope. So they would disregard anything like that.

But then, if there was a claim that fit within these four buckets of different kinds of potential disinformation, they could pull that down, open up a ticket, and start an investigation.

Q Okay. And so you mentioned the different types of -- the scope, essentially. And that's listed down below. So let's skip ahead down to that.

A Yeah.

Q The scope of what was considered mis- and disinformation for purposes of your investigation was fairly limited, right?

A Yes. It was only about the functioning of the election itself.

Q Okay. And so, in the bullet point section on page 6 -- or Roman numeral VI --

A Yes.

Q The first example is "procedural interference." Can you explain what you consider procedural interference to be?

A So it says here: Misinformation related to actual election procedures. So telling people -- you have to have a passport to vote would be an example of attempting to interfere procedurally by lying to people about something they have to do to vote.

Q Okay. And so it's a demonstrable falsehood about how a person can vote. Is that fair to say?

A Yes.

Q The next bullet is "participation interference." Is that right?

A Yes.

Q And what is your understanding of what participation interference is?

A So here, we define it as content that includes intimidation to personal safety or deterrence to participation in the election process.

So an example of that that we had in our database was saying: A bomb threat has been called into this precinct. Don't go. Don't go vote. There's a bomb threat.

And there was no bomb threat.

Q Okay. And so individuals, if they had heard that bomb threat, might have not gone to vote. Is that fair to say?

A Yes.

Q Okay. And so people effectively could have been disenfranchised by that information. Is that fair to say?

A That's right.

Q The next bullet is "fraud."

A Yes.

Q How did you define fraud for purposes of this project?

A So it says here content that encourages people to misrepresent themselves to affect the electoral process or to illegally cast or destroy ballots.

So it is effectively people calling on others to help them fraudulently throw the election.

Q Okay.

A So go get lots of ballots. Go, you know, mark your ballot up for your parents. Go request absentee ballots in places that you aren't allowed to. Those would be examples of fraud.

Q In your introductory statement, you used an example of an individual impersonating an election worker. Do you recall that?

A Yes.

Q Would that be considered fraud for the EIP's purposes?

A Yes. I think so.

Q Okay. And then the last bullet is "delegitimization of election results."

And I think we talked through it, but here it says: Content aiming to delegitimize election results on the basis of false or misleading claims.

That tracks with your definition, right?

A Yes. That's right.

Q Okay. So the second goal listed under "what we did" in that paragraph is: Share clear and accurate counter-messaging.

What does countermessaging mean here?

A So countermessaging would be providing accurate information to people. And the way we did that was both ourselves, mostly on our blog, of saying, "This is some claim that's going viral, and here's the truth that we could find," or by providing knowledge to those State officials -- local and State officials who then could do their own local messaging.

Q So, with respect to the State and locals first, would an example of that be, if there was a claim made about how long polls were open, and it was false, you would let the State or local know so they could put something on their website potentially to make it abundantly clear --

A Yes. And that's something that happened multiple times, where people shared the incorrect dates or times of voting so that they could then do their own tweet or their own post or go to the local media and say: Hey, tell people the polls are still open, for example.

Q Okay. And then you said, with respect to the EIP specifically, you might post things on your blog about inaccuracies. Is that right?

A Yes. Yes. We posted -- for narratives that got lots of traction or seemed to be really important, we would do our own write-ups of both analyzing how it was going as well as linking to any fact checks or any information we could find about the base truth.

Q Did you ever affirmatively create social media content for the platforms? In other words, would you create content for Facebook to counter a post that might be misleading?

A No. No. We had our own Twitter account where we'd speak as ourselves, but we did not create any content for the platforms.

Q Okay. And countermessaging, to be clear, it doesn't actually involve removing content, right? It's just pushing more information out that's accurate?

A That's correct, yes.

Q Okay. The third goal identified under "what we did" was to document the specific misinformation actors, transmission pathways, narrative evolutions, and information infrastructures that enable these narratives to propagate.

I am not a scientist. I'm not a data scientist, for sure. And I don't really understand what that language is. Can you explain what that means?

A Yeah. So this is overly flowery academic terms for -- first document the specific misinformation actors. So that is us creating a record of who was either speaking about things that were false or amplifying. The amplification actually became a big focus of our research afterwards. We learned some interesting things.

The second, "transmission pathways," how is this incorrect information moving?

"Narrative evolutions," how have things changed over time? We wrote both a blogpost and we have a couple examples in here that's, as the facts changed or as States were called, for example, the narrative changed.

Or "information infrastructures that enabled those narratives to propagate," that's back to when I was talking about the affordances. What is it about these platforms specifically that allows these things to grow?

Q Okay. And the very first word in this is "Document the specific misinformation."

A Yes.

Q Is it fair to say that by "document," this amounts to tracking or cataloging your findings?

A Yes. It was us looking to see what was going big and then archiving it and creating the database for our further study.

Q Okay. So, again, one of the major goals of the EIP was research-based. Is that fair?

A Yes. Absolutely. Both the research we did specifically in the EIP, and then to support further research because one of the things I saw coming out of 2016 -- when I got to Stanford, I talked to a lot of people about what happened in 2016. Real political scientists. I'm not a political scientist. But political scientists who study democracy. Frank Fukuyama. Larry Diamond.

And if you talk to them about what do you think this important question of, did 2016 change the results, what most of them will say is: We don't know because nobody was watching.

And so one of the things I wanted to change for 2020 is, if something big happened, either in the election or afterwards, that we had a real historical record that did not exist in 2016 that would allow both history to know what happened but then for us to do our own research and for our partners to do their own research.

Q Okay. And I want to turn to one, I think, outcome of that research in the key takeaways section on page -- Roman numeral VII.

A Yeah.

Q And I want to look at the first item on that page, which is: Misleading and false claims and narratives coalesced into the meta-narrative of a stolen election, which later propelled the January 6 insurrection.

Can you explain what's meant by a meta-narrative?

A So the report talks a lot about -- that you have -- one of the things that happened in 2020 is that the overall belief that the election was going to be stolen before anything had happened started to be laid by President Trump and some of his political allies throughout the summer and the fall of the year. So that's the meta-narrative, is the election is going to be stolen, and then immediately on election day and afterwards, the election has been stolen. The meta-narrative is supported by whatever evidence can pop up and can be utilized for that.

And so that's a lot of what we documented here, was -- if people are voting with Sharpies, that becomes a narrative that Sharpies are part of throwing the election. If people are voting with Dominion Voting Systems, that becomes part of the narrative.

And so the meta-narrative being stolen election was -- one of the things we talk about here is that once you prime people to believe through repetition over and over and over again the election is going to be stolen -- the election is going to be stolen -- then if they personally witness anything, then they will make it fit that meta-narrative.

And so that's a lot of what we talk about here. They get a Sharpie, and they vote, and they're like: Oh, man. It bled through. This must be part of the conspiracy.

And that's a lot of what we were trying to study here.

And one of our conclusions was that a lot of the narratives that came up were specifically targeted or -- I'm sorry -- were created by the meta-narrative becoming widespread among mostly supporters of President Trump.

Q Okay. Thank you for that.

Real fast, you referenced Sharpies. That's your reference to what's sometimes called Sharpiegate scandal. Is that right?

A That's right. We have a whole -- we have a blogpost about this and a big analysis because that was a great example of an observation a number of people made that then got fit into this meta-narrative. And then, as the night progressed, in particular when FOX News called Arizona, all of a sudden, the narrative changed to make it about Arizona, for example. So it was a really good kind of baseline for our study.

Q And the Sharpie -- the allegation -- just so the record is clear -- the allegation was that individuals were filling out ballots with the wrong pen, and it was making the ballot invalid. Is that right?

A Right. The allegation is, if you vote with a Sharpie, it bleeds through, and that that would make it not read correctly.

Our understanding is that the ballot manufacturers know that Sharpies bleed through, and so that's why there's not voting space on the other side of the ballot. They don't scan that. They don't count that. And, in fact, Sharpies are something that is requested by some of the ballot manufacturers because, unlike ballpoint pens, it doesn't smear off inside of the scanner and jam stuff up.

And so one of the things we document here is -- some of the first allegations around Sharpies actually came from people who seemed to be more progressive and from blue States of: Hey, what's going on here? I voted with a Sharpie. It bled through.

And then, as the night progressed -- and especially with Arizona because Maricopa County, for whatever reason, a lot of people were using Sharpies -- that as it progressed, then, all of a sudden, kind of a general thing that a number of people said got coalesced into this narrative that Sharpies were only being given to Republicans or in Republican districts, and therefore that was being used to invalidate all those ballots.

Q Okay. And the allegation about Sharpies invalidating the ballot, it's untrue, right? It's demonstrably false?

A To my best understanding, it's untrue, yes.

Q And you also referenced the Dominion theory. That's a reference to the

Dominion -- the theory that Dominion voting machines were switching votes. Is that right?

A That's right, yeah.

Q And that's also demonstrably untrue?

A To my best of my knowledge, it's untrue, yes.

Q Okay. So you used these examples and talked through how they coalesced into a meta-narrative. I want to look at a couple pages of your report that show the results of this meta-narrative.

A Yep.

[redacted]. I want to introduce pages 99 to 101, which concerns postelection violence. And this is exhibit 5.

[Stamos Exhibit No. 5
Was marked for identification.]

BY [redacted]:

Q So we've clipped the whole part, but I really want to look at page 99, which is the start of the second paragraph under the "during and postelection" heading.

It says: Violence-related posts became increasingly tied to claims of election theft or rigging and, at times, were part of increasing rhetoric that more generally referenced the idea of preparation for civil war.

A I'm sorry. I think I might be looking -- where exactly is it?

Q I'm sorry. It's the second paragraph.

A Okay. Yes. Yes.

Q It says: Violence-related posts became increasingly tied to claims of election theft or rigging and, at times, were part of increasing rhetoric that more generally referenced the idea of preparation for civil war.

Do you see where it says that?

A Yes.

Q So your team saw a spike in calls for violence after the election. Is that right?

A That's correct, yes.

Q And did you analyze how the narratives that were already creating the Sharpie, for example, the Dominion voting, fed into those calls for violence?

A Yes. That's a big focus of our report.

Q Okay. And what did you find?

A What we found is that the creation of all of these narratives, that were based, in some cases, on people's real experiences, were factual things that happened but were then turned into narratives that were not true about large conspiracies or the election being stolen.

It is the creation of all those narratives that gave people the feeling that something must have gone wrong. This must have been stolen. And that's what most likely led people to do things like call for civil war or call for violence.

Q So is it fair to say that your research actually showed that these preelection false claims actually ultimately fed into calls for violence postelection that potentially could have contributed to January 6?

A So I would be very careful of making, like, a strong causal claim here. That is not, like, the research question that we had here. But we did document the increasing popularity of these narratives and then, among the same people who seemed to believe the narratives, would have called for violence.

Q Okay. Thank you. And then, before I move on from the report, I want to turn to page 9 of the executive summary, which is key recommendations. And sorry.

That was the previous exhibit number. No. 4. And I want to look at the one for the Federal Government: For the Federal Government, EIP recommends the development of clear authorities for identifying and countering election-related mis- and disinformation, and creating clear standards for consistent disclosures of mis- and disinformation.

A Yes.

Q What does "disclosure" mean here?

[11:42 a.m.]

Mr. Stamos. I am sorry, I was on the second part. Create disclosures. Yes, it means for -- in this case for members of the Federal Government to say here is something that a trending, here is why it's not true. And we specifically refer to rumor control which was a CISA blog that was very effective of doing that during the election.

BY [redacted]:

Q And so the ideas is that the recommendation is that the government identify and make these things public, but there's no recommendation here that the government sensor or work with the social media companies to take any posts down. Right?

A No. We do not make that recommendation, nor do I think that would at all be appropriate.

Q And why, why would that not by appropriate?

A I don't think it's appropriate for the government to tell platforms to take content down.

Q Okay. And so there's no recommendation here that platforms take anything down the recommendation is that more information be pushed out?

A I mean in this case, we are not recommending that the Federal Government take content down at all, no.

Q Okay. I have about 10 minutes left so I want to turn to some kind of misconceptions that have been circulating around the EIP and what the EIP does. And you I think you touched on some of these in your opening statement. And actually, do you happen to have a written copy of your opening statement.

Mr. Thompson. I certainly may have another one.

Mr. Stamos. I have this one. I just kind of need it back, if you don't mind.

[redacted]. I wanted to -- okay. So we can do without it. I was going to introduce it into the record, but that's okay.

[redacted]. You can put it in the record.

Mr. Stamos. You can use it.

BY [redacted]:

Q Are you familiar with Matt Taibbi?

A Yes.

Q Who is Matt Taibbi?

A He is a journalist who testified in front of this committee.

Q Are you familiar with an individual named Michael Shellenberger?

A I am.

Q And who is he?

A Likewise he is a journalist and a Substacker he writes on Substack. And he testified in front of the committee.

Q Have these individuals made claims about the Election Integrity Partnership?

A Yes.

Q And I think -- and one that you referenced in here you claim that the EIP -- oh, I'm sorry, Mr. Taibbi claimed that the EIP has succeeded in getting nearly 22 million tweets labeled in the run-up to the 2020 vote. Are you familiar with that statement?

A Yes.

Q Is that accurate?

A That is absolutely false.

Q You look like you want to say more.

A I would be happy to explain.

Q Yeah, please do.

A So he was pulling out this 22 million number, which I believe comes from here in my statement, I believe I cite exactly where it comes from.

So we in our academic study and in our publications one of the things we have done is we have discussed the size of the overall conversation. And one of the things that we talked about was there was something on the order of 800 million tweets in that year about the election at all, about Trump and Biden and anything to do within the election and that there's 22 million of those were specifically about the narratives that we had identified.

So if you look in our report we talk about Dominion, Sharpiegate stuff like that. After this was all done, we went back and we looked at Twitter and we said, how many people were talking about these things? Those were not necessarily true or false, it's just people talking about Dominion Voting Systems, people talking about Trumpies.

And that was a number of the overall scope of the conversation. It had nothing to do with anything. We reported the platforms. That number had nothing to do except as part of our post facto analysis of the conversation that happened online.

Q I want to introduce pages 182 to 183 of The Long Fuse because I believe that's where this comes up.

A Okay.

[Stamos Exhibit No. 6
Was marked for identification.]

BY [redacted]:

Q So at the top it's not a full paragraph because it carries over from the prior page, but it describes the collection of information. It says, the collection resulted in 859 million total tweets. That's 800 million number you just referred to. Right?

A That is right, yes.

Q And in the middle of page 183 there's a paragraph reading in total our incident related tweet data included 5,888,771 tweets and retweets from ticket status IDs directly, 1,954,015 tweets and retweets collected first from ticket URLs and 14,914,478 keyword searches for a total of 21,893,364 tweets.

A Yes.

Q Correct?

A That is right.

Q So what does the reference to tickets mean in this paragraph?

A Right, so a ticket is an entry into our internal research database describing a narrative or incident. Yeah.

Q Okay. And so the ticket is the 21,897,364 number, that's the total number of tickets in your database. Correct?

A No.

Q Okay. What's that?

A So we had -- we had -- the actual number of tickets is elsewhere.

Q Oh, I'm sorry. I meant the total number of tweets in your database not the total number of --

A That is the total number -- so the University of Washington team, using their API access collected tweets that were related to the election at all. That it is the total number of tweets that then were related to the narratives that we identified.

Q Okay.

A In that massive database of everything that was said about the election.

Q And I'm sorry, you just referenced API data. For the record, what is API data?

A API means application programming interface. So that would be the mechanism in this situation in which the University of Washington was able to ask tweeter send us all you will of your public tweets about the election.

Q On March 17, 2023, SIO posted a blog post of some type of background on the SIO's project on social media. Are you familiar with that post?

A I don't have it memorized but I am familiar with it, yes.

[Stamos Exhibit No. 7
Was marked for identification.]

BY [redacted]:

Q And again, this is a blog post. I will refer to the page numbers as printed. But a blog post --

A All right.

Q Page 3 of this post as printed you address the 22 million claim. And it says that Stanford explains that that's false. And it says, in fact, EIP identified 2,890 unique tweet URLs and potential violation of Twitter stated policies. Does that number track your best recollection of how many tweets are identified in violation of policies?

A Yes.

Q Okay. So that's actually a bit over .01 percent of the entire data set. Is that right?

A That's correct, yes.

Q And what does the reference to Twitter stated policies means here?

A So we had during our operation in situations where there were egregious violations of the policies that the platforms have already put out which we then provided -- we both provided a public analysis and we had an internal tracker of the what the policy's were per platform. We could then refer to those to the platforms.

In which case they would get an email from us that would say saying something like we believe these five URLs might violate policies on fraud. And then the platforms themselves could make a determination themselves could make a determination of whether or not that was true.

Q Okay. So I want to emphasize that. You sent this information to the platforms. And after it left your hands, you had no control over what a platform did with it?

A That's right. They had to make the determination, it's the same as if you went into Twitter right now and you clicked and said report, it's essentially the same function.

Q And anybody can do that. Right? Anybody can go on Twitter and report a post? Right?

A Anybody can report a post. And I know there are, multiple organizations that email people. As somebody who comes from a platform, you get email all day, every day of things that people think should be taken down. In our case, we believed we were reporting things that were violative of their policies around election operations specifically. But people do it all the time for all kinds of reasons.

Q Okay. And it's the same thing with Facebook. Right? Once if you were to report something to Facebook as potentially in violation of their policies, once it left your hands it was up to Facebook to decide what to do with it. Right?

A That's correct, yes.

Q And you had no control over how Facebook applied its policies to particular posts. Correct?

A We had no control over what they did, no.

Q Okay. Mr. Taibbi testified that the EIP targeted more disinformation on the right than on the left by a factor of 10 to 1. Is that correct?

A No.

Q Could you explain?

A So I think what he is doing is misrepresenting our tables that show the size of various narratives and who the super spreaders were. And so we had no goal of targeting anybody or any political -- as I said, I am actually afraid of this becoming a bipartisan issue and we can talk more about how that might happen.

And so that was not part of our targeting, but in the end when we did our analysis then, as you might expect, the majority of disinformation around the election did come from conservatives, which is not a surprise because President Trump lost the election and he denied that the election was valid and so that motivated his supporters to be spreading those things. But that is a post facto analysis as part of our academic research into what happened in 2020.

Q Are you familiar with what's been referred to as the Hunter Biden laptop story?

A Yes, I am.

Q And this is a reference to an October 14, 2020, New York Post story about a laptop reportedly belonging to Hunter Biden. Correct?

A That's right.

Q Did EIP analyze the laptop as part of its work?

A No.

Q Is it fair to say that the laptop story was entirely outside the scope of your work?

A Yes. That kind of claim about the son of a candidate is completely out of scope for us. We had nothing to do with any decisions of any platforms made about

Hunter Biden nor does that show up anywhere in our database.

Q I think -- we can go off the record.

[Recess.]

BY [redacted]:

Q Mr. Stamos, I wanted to pick up briefly on -- touch on one of your answers from the previous round. You were asked a question about whether the government had ever requested EIP be created or something similar. And during that set of questioning you mentioned that there was "a lot of blaming" that went around to, like, Facebook and other social media companies. With respect to people that were blaming Facebook and others, would that include people in the government?

A So if we are talking about post 2016.

Q Yes.

A Yes. I mean, I think pretty famously you had a number of elected officials, President Obama being at the top of it and most Democratic House and Senate Members talking about fake news on Facebook being a determinative thing.

Q And you said you approached Mark Zuckerberg about your concerns and the need to address, coordinate inauthentic behavior?

A What I brought to him was this fake news problem that might have a foreign component and that we need to get ahold of it.

Q Okay. And as part of your discussions with Mr. Zuckerberg, did you note the public backlash that Facebook was receiving?

A I don't recall exactly what I said. I don't think I had to note for him the kind of public backlash that he was getting.

Q Do you think he was well aware?

A I think he was well aware, yes.

Q And do you recall if he was receptive to what you were presenting?

A He was. He was receptive. And he ordered XFN, cross functional working group to be put together specifically to look at possible foreign origins of the fake news crisis as we were discussing it at that time.

Q And to your understanding, what would the consequences have been if the company had failed to address this concern?

[redacted]. I'm sorry. Can we go off the record?

[Discussion off the record.]

BY [redacted]:

Q To repeat that previous question, to the extent you have a recollection, to your understanding were there consequences that Facebook would face if it failed to take action with respect to better countering foreign malign influence campaigns?

A I think in the long run it would have been worse for the platform to not do things because people would have lost trust in news worthiness. But in the short run being honest about it probably ended up creating more political pressure on them.

Q And what types of political pressure are you referencing?

A Well, I -- the pinnacle of this was Mark and Colin Stretch being called to do hearings and lots of blame that Russia controlled fake news, that Russia was larger. There were a lot of discussions like in the late '17 into 2018 of the idea that a huge amount of the content on the platform was controlled by Russia or came from Russian sources and have an overstatement. The stuff that we put out was factual and we thought kind of sober and then that got blown out of proportion in 2017, 2018.

Q And you referenced in an earlier answer that there was a sense, primarily by Democrats, that Facebook's failure to better counteract foreign malign influence campaigns, particularly from Russia, materially impacted the outcome of the 2016 election. Sitting here today, do you think that's still the case, that a large swath of the public still believes that?

A I don't have any survey data here. I think it has become less widespread of a belief. But certainly I am sure there are still Democrats who believe that minus the IRA campaign or the GRU campaign that Donald Trump would not have won.

Q And during your time at Facebook, do you recall what Monika Bickert's role was?

A She was the head of platform policy.

Q And do you understand what was her responsibilities?

A She ran the team that came up for -- what policies were going to be, the community standards they are called on Facebook and Facebook's other properties and then the interpretation of how those would actually be enforced which was actually the really important component here that is generally not public is how do you take a general statement against hate speech and then define that in really specific circumstances in dozens of languages around the world.

Q And when you were briefing Mr. Zuckerberg about your concerns and the need to better address foreign malign influence campaigns who else participated in those discussions?

A So it was a big room, it was certainly my boss, Colin Stretch, the general counsel, Sheryl Sandberg, the COO at the time, Chris Cox was the head of product. Probably Mike Schroepfer, who is the chief technology officer. Monika Bickert would have been in there. Elliot Schrage who is the head of policy, Joel Kaplan with a K was his deputy who ran policy in the D.C. team, probably some other folks from D.C. in policy who I don't recall.

Q And do you recall approximately when these meetings took place?

A This was in November and December of 2016 was the initial set of meetings. Obviously, as all the stuff progressed over 2017 we had regular updates on our findings and what to do about it and such.

Q I also want to touch upon briefly you had mentioned that EIP did not cover the Hunter Biden laptop story.

A That's right, yes.

Q Did you have a general familiarity with the story?

A From the media reports, yes.

Q Did anyone from the government contact you regarding the story in the days following the publication?

A I don't recall anybody in the government ever talking to me about the Hunter Biden laptop. Sorry.

Q Did anyone from Facebook contact you on the days following the story's publication?

A I had had regular contact with people at Facebook, I don't remember this being a topic. But I don't recall -- they certainly would not come to me for advice on something like that.

Q Do you recall anyone from Twitter contacting you in the days following the story's publication?

A Again, I was in regular contact with people at Twitter. I don't recall a specific conversation about the Biden laptop.

Q In the fall of 2020, with respect to content moderation, enforcement decision, would you ever be contacted by somebody at Facebook or Twitter?

A So they would often ask us for our feedback either on specific things that are happening. So, you know, especially on some of these foreign influence campaigns we would collaborate on the investigations. And around election policy we had a back and forth on sometimes they would ask us generally this has been the summer, well before the election, about what kind of policies issues to put in place. So we did have a kind of an ongoing conversation about that.

Q In these ongoing conversations, do you recall any that concerned whether social media platforms should develop policies with respect to potential hack and leak?

A We probably had those discussions, but our scope for EIP was specifically about the election infrastructure itself. So we would not have been given advice for anything outside of a hacking campaign that involved the election running, which is something you could consider possibly happening.

Q And just a point of clarification, if it involved EIP that would be relevant too, but also just in your position as a former Facebook executive and having expertise in the area. Is it your recollection that when the story, the Hunter Biden laptop story first broke that there were some who believed it was the product of a hack and leak that Russia was behind?

A Yeah. I mean that was a pretty widespread believe among people.

Q And during that time, do you recall anyone in media or otherwise asking for your expertise regarding whether Russia was behind this as a hack and leak operation?

A It's possible. I don't recall.

Q You don't have any specific recollections of anyone?

A No.

Q Do you recall familiarity with the statement that 51 former Intel officials released 5 days later?

A Yes, from the media.

Q Before that was released, did you have -- did any of the 51 former Intel officials contact you?

A I am pretty sure not, no. I don't have a recollection of that, but that seems highly unlikely. And I did not know anything about that letter until it came out.

Q If we could -- so if could turn your attention and get back to the summer of 2020, you're in the early days of forming EIP?

A Yeah.

Q Were there any potential partners who you reached out who declined to participate?

A Hmm. I don't recall any specific ones. It's possible.

Q How did you decide on having UW, Graphika and DFR Lab as Stanford's three partners?

A So UW had already been our closest academic partners. And their team was the one that was most aligned to the kind of work that we had done in the past. So they were just a natural fit. We won their academic institution especially for eventually we were going to be publishing peer reviewed work and that's not something that's of interest generally to non academic institutions.

Graphika was interesting because they made the software at the time that was the best at understanding networks of amplification on Twitter in particular. So answer to Graphika's data set there and having their analyst use it was going to be the interesting part. DFR Lab we contacted them because of their particular experience doing these foreign investigations. So Graphika, DFA Lab and us, less UW but we had in the past worked with Graphika and DFR Lab on our investigations of different foreign influence actors and such. So they were kind of natural partners since we had already done that work together.

Q And you mentioned that there were discussions with CISA prior to the formal formation of the EIP. Once EIP is formed, what role did CISA play?

A So CISA made the introduction to EI-ISAC and helped us know who the players were. We didn't -- we didn't know until our conversations with CISA that the central responsibility for the switchboard function of communicating with all the local and State officials was going to exist in the EI-ISAC so that was key role they played. They did not have access to our data nor could they report things to us directly. So EI-ISAC was our primary partner in being able to reach out to the local and States.

Q And when did you first learn that EI-ISAC existed?

A I don't recall.

Q Was it before you joined Stanford?

A I don't think it existed for long before I joined Stanford. So it's probably while I was at Stanford. I wouldn't have a recollection of the first time I ran into them.

Q You said CISA, you know, introduced you to EI-ISAC. Did you have familiarity at all with EI-ISAC before CISA --

A I don't recall. It's possible I'd run into them at, like, the NASS, the secretary of State events and such.

Q Yeah.

A But CISA didn't -- made the introduction to the people who were actually running this function.

Q And are those people at CIS, are they -- or are those people at CIS different than those ruining EI-ISAC?

A The people who run EI-ISAC are CIS employees is my understanding, who run the central function. There are thousands of members who then do all the work and create content and such. But the kind of coordination function my understanding is run by CIS.

Q Do you recall when CISA introduced the partnership to EI-ISAC?

A So it must have been in the June timeframe. I don't have an exact date.

Q And did you have an understanding of EI-ISAC before the formal formation of EIP?

A I don't recall my knowledge of EI-ISAC.

Q Did you have an understanding before you were intro -- before CISA introduced you to the EI-ISAC if there was some sort of switchboarding or reporting portal related to elections that existed?

A It probably came up in one of those earlier meetings with election officials. I don't recall the exact timing, though.

Q When you were first raising this issue, was the idea that EIP would provide a similar reporting function?

A So we had discussed at one point working directly with locals and States, but I think that became clear after we learned about EI-ISAC to be completely improbable because there were thousands of people. It was just not going to be with the time that we had something that we could possibly advertise out to them.

And so there was, like, a series of meetings in discussing how could we work best with all of these counties, all of these cities in some cases. And the outcome was that EI-ISAC already had these relationships, it could be the people that routed to us.

Q When the introduction was made between CISA and EI-ISAC, did you have an understanding of how familiar the folks at CISA were with EI-ISAC and how it operated?

A I mean, I don't recall a specific feeling about that. I -- it's pretty clear that they had been working with each other on building the switchboard functionality.

Q Do you recall if there was the switchboard functionality ahead of the 2018 U.S. midterms?

A If there was, I was not aware of it.

Q So you have contacted CISA, CISA introduces you to EI-ISAC. And we are still in the summer of 2020, to the best of your recollection?

A Okay.

Q What roles did CISA play, if any, after that?

A In the EIP they had no official role. They did not have the ability to report things directly to us. We would take things from EI-ISAC. I don't believe anything that EI-ISAC sent us came from CISA employees themselves. And they were not part of our day-to-day operations or our analysis. So they had very little role, if none in EIP.

Q Did CISA continue to meet with EIP partners during the summer of 2020?

A It's possible, we had meetings. We did a number of briefings for government partners about the kinds of things that we were seeing.

Q And happy to use whichever term you want, there's the EIP four partners and there are other external partners as well. You mentioned social media platforms --

A There were other --

Q -- some sort of engagement with EIP. Is that right?

A Yes. I think the term we used is stakeholders was people who we had some kind of communication with.

Q All right. And do you recall which social media platforms were some of the external stakeholders for EIP?

A So we list all of these in the report. I'm happy to go through them, if you want.

Q Would it include Facebook, Instagram, Twitter to your recollection?

A Yes, all three of those. Instagram and Facebook for the purposes of this would be the same, it would be the same people.

Q How did you decide which social media platforms to include?

A So we contacted the platforms that we thought would have the most -- that this content would be found on and that would be the most interesting for us to study. So in some cases we had had preexisting relationships such as with Facebook and Twitter. We had worked with them on these investigations of foreign influence campaigns and such. And some of the cases like for example Reddit we didn't really have much of a relationship with, and so we reached out to them to at least have the ability to report stuff to them.

Q So if I could just try to clarify a couple of the wes there. When with you say we worked with Facebook and Twitter, that's in reference to EIP. But when you referenced we earlier, working with Facebook and Twitter, is that Stanford?

A Okay. So the Stanford Internet Observatory had worked with Facebook and Twitter on foreign influence campaigns in the past.

Q Okay.

A So it that was the preexisting relationship we had. And then as part of EIP we reached out to a number companies that we had not had relationships with such as Reddit because we thought they would be of possible -- possibly targeted as part of campaigns. And we wanted to have the ability to report things to them.

Q Do you recall any social media platforms that declined the invitation to participate?

A I don't recall, but it's possible.

Q Okay. And in addition to the social media platforms, what other types of external stakeholders were there?

A So we had voting rights groups and other kind of NGOs who related to voting rights and voting suppression who had the ability to send us tips. They didn't have access to anything but they could send things in to us. They had an email address. Like I said, we reached out actually to the RNC to the general counsel's office and they did not take us up on our offer. But effectively we'd reach out to a bunch of groups saying, here's an email account that you could then email if you see anything going on.

Q You mentioned that reports can be submitted to EIP as you were setting up this operation and EI-ISAC was one of the primary entities that would be submitting reports. Is that correct?

A So we document this in here. Of the entities that submitted reports, EI-ISAC was by far the largest.

Q And do you know if every report that was submitted to EI-ISAC was then in some way forwarded or submitted to EIP?

A No, I am -- I am pretty sure that most of the reports that went to EI-ISAC were related to more standard cybersecurity issues. And so somebody is port scanning or I found malware or something, those are not forwarded to us. And I -- I can't speak as to what percentage of the things that related to disinformation were forwarded to us.

Q Who made the decision whether a report submitted to EI-ISAC would be submitted to EIP?

A I believe it was the CIS employees who were running the switchboard.

Q Yeah. Do you recall who was running the switchboard at CIS?

A I don't recall names of the people, but we could -- I could come back with that.

Q Yeah. Do you know who Aaron Wilson is?

A I believe he is CIS employee.

Q Do you know who Mike Garcia is?

A I don't know. I don't recall who he is.

Q You mentioned that the Global Engagement Center was one of the entities that can submit reports, tickets as well?

A Yes. They could send -- they could send emails in to us for us to open and to look into, yes.

Q Do you recall who at the GEC you interacted with?

A I don't- -- I mean, personally I had -- there was a meeting in which I believe the director of the GEC was at here in D.C. I don't recall her name. I -- I didn't have most of those conversations.

Q The meeting in D.C. that you just referenced, what was the purpose of that meeting?

A I believe it was to tell them about what was EIP was doing and telling them that they could send into us reports of foreign influence that they he saw, potential foreign influence.

Q Do you know who first connected GEC and EIP together?

A I believe that we had already had preexisting relationships with GEC because they had published in this area before the EIP.

Q In addition to CISA and GEC, do you recall any other Federal agencies that played either informal, like, external stakeholder role or otherwise consulted EIP?

A So the only groups that could and did report from the Federal Government report anything to us was the GEC, which is actually part of the government and then the EI-ISAC external, you know. And you'd have to give it your own determination of how much of the government that is. But those are the only two groups that did send anything in to us. We did do briefings for several our agencies and we had one ticket that we then sent out to the FBI.

Q Which other Federal agencies did EIP briefly?

A I did a briefing for General Nakasone then the director of NSA and Cyber Command.

Q And did these briefings -- when did they occur in the process? Is it pre-election?

A Pre-election, yes. Like in the late summer, early fall we did a briefing. He had come to campus and had heard us talk about our foreign work. And he asked me to brief his executive staff on our concerns and what kind of foreign influence who happen during the election.

Q And the FBI mentioned -- received the ticket. Did the FBI also receive briefings for the election?

A The FBI was part of that briefing, so I did it from the FBI office in -- in San Francisco because I just can't Zoom in to the NSA.

Q Do you recall who set up the meeting between you and the NSA?

A Elvis Chan had set up the -- so the meeting was set up because Nakasone had come to campus. Elvis was the facilitator who provided the space and participated, listened to the briefing in San Francisco.

Q Yeah. Did you know Mr. Chan before this meeting had occurred?

A I did.

Q And how did you know special agent Chan?

A Yeah, he runs the group in the San Francisco office of the FBI that handles high profile national security cyber attacks and so had I worked with him both at Yahoo. At Yahoo we had been attacked by the -- by contractors working for the Russian FSB.

And then at Facebook we had a number of attempted attacks, as well as manipulations of the platform to cause attacks by a variety of government agencies, foreign government agencies. And so Elvis was the primary contact for all of that because he ran the group that would investigate those kinds of foreign actions.

Q Do you recall anyone else from the FBI attending this meeting?

A There were some other people from his squad. I don't recall their names.

Q And so in addition to the NSA, FBI, do you recall any other entities that were present at the meeting?

A The -- it was a video conference. In the room were only FBI agents. The only people I knew of who were on the other link were NSA.

Q So you mentioned FBI, NSA, GEC and CISA. Were there any other government agencies that received a briefing from EIP?

A Not to my knowledge.

Q Did you -- in addition to this briefing that the FBI helped facilitate between EIP and NSA, did you have any other interactions with the FBI as a function of EIP's work?

A We did the preemptive briefing and we sent them one report related to Arabian action in the election and I believe that was our only interaction with them.

Q When EIP was organized, were there new EIP email addresses created for folks?

A No. We have a domain that has one working email address info@, which was a mailing list that went to three or four different people.

Q Okay. Do you know who those three or four people are?

A It was me, probably Elena Cryst or deputy director of SIO, Kate Starbird and I believe there's a comms person at UDOT, I forgot his name, who'd receive those emails. Because often that would be media requests and he would be the one who handled those.

Q So I think we started to touch upon this, but how would members of EIP communicate with one another?

A So there was some emailing of each other. We had very regular Zoom calls, you know, at least one or two times a week in the first days and then every day in the days right up to the election, right after the election. We could communicate over Slack channels and we -- but most of our kind of research communication happened within Jira, because that's where you would put content and you'd put any analysis into it.

Q And if you could say a bit more, what is Jira? What is a Jira ticket?

A So Jira is a popular product made by a company called Atlassian that is used by lots of company for issued tracking. It has a couple of ways you can use it. You can use it for, like, internal IT. It's used a lot for software defect management so finding bugs, tracking how you are fixing stuff or you can use it for work flow management. There's an on premise solution where you host it yourself or you do it in the cloud.

We had a cloud account. And so we created a database in Jira service desk, which is the version of Jira we used that EIP members had access to where we could create tickets that would identify lines of research attached to that evidence that we found and then have a conversation about what was going on.

Q And when reports are being submitted to EIP, EI-ISAC -- GEC also have the capability. Are they submitted via Jira or how do the reports get from outside the system into Jira?

A Right. So for those two organizations for EIP and GEC they had the ability to submit it directly. So the EI-ISAC people had an account they could log into where they could submit reports and then they could see the public components of their ticket. So there's a part of the ticket that was private just to us and the part that was public. They could see the public part of those tickets.

For GEC, we'd have to look again, but I believe it was somewhat of the similar, they would file something, they could see the things that they opened themselves or that we added them to specifically.

For the other organizations like NAACP, we just give them an email account, they could email us.

Q For GEC, when you say they would have access to a public portion of the ticket, by that you mean they are in the Jira system?

A Yes.

Q This is not an email notification, this is separate from that?

A So every user in Jira can change what notifications they want to get. So you can put in there to say if anybody ever mentions me in a tickets or if a ticket changes, I want to get an email. So that's an individual setting by each individual user.

So there could be emails generated for the ticket being created and there could have been emails generated for changes to the ticket. But that's really up to each individual user.

Q But to see the ticket itself you had to be invited to join?

A Right. You had to be logged in. You ha -- the account is Atlassian account, but we'd have to invite your account to have access.

Q Do you recall who at GEC had access to the GEC account?

A I don't recall who the exact person was.

Q Okay. Who at the GEC was most involved with EIP?

A I didn't have much of those conversations. I can't really -- I don't remember the exact names of the people.

Q Who at EIP had most of the conversations with GEC?

A GEC was probably either Renee Diresta or Elena Cryst.

Q And who is Ms. Diresta?

A She's our research director.

Q Besides GEC, which other agencies had access, direct access to the Jira ticketing system?

A So to be clear, no agencies had direct access to everything. They could only access the stuff that they gave to us or that we specifically tagged them in. And the only two agencies -- well, not agencies, one organization was EI-ISAC and then the only government agency would be the GEC.

Q Did CISA ever ask for access?

A I don't believe so.

Q Did the FBI ever ask for access?

A I don't believe so.

Q Did the NSA ever ask for access?

A Definitely they did not ask for access.

Q Following your meeting with the NSA that the FBI facilitated, did you receive any follow-up communications from the FBI regarding their interest in participating in EIP in any way?

A I don't recall our exact communications. I think it was known that the line of communication was open if we saw anything that was actually a significant legal problem or a foreign interference that they wanted to be notified of it.

Q Did the FBI and the NSA know that CISA consulted you at the beginning of EIP, had made the introduction between the EIP and EI-ISAC?

A I don't know what they knew. We -- most likely, by the time we briefed NSA, we probably briefed them on the EI-ISAC reporting initiative.

Q So in addition to EI-ISAC and GEC, you said there were other external stakeholders that would just email reports to EIP?

A Right. They could send in. And I believe we gave them so the -- a Jira database itself can have an email account so effectively you can email to that and the email will get entered into a ticket for somebody to go look at it.

Q Okay. Do you recall what those email addresses were?

A No.

Q Do you know when the domain name would be for those email addresses?

A It would most likely be under atlassian.net or atlassian.com. They were not things that we hosted. That's part of the basic functionality of Jira.

Q And would each organization get a specific email address or did the Jira ticketing system that EIP was using have its own email address?

A I don't recall how we set it up.

Q With respect to choosing the different options to using the Jira system, who at EIP played the primary role in that?

A I am sorry. What do you mean choosing the different options?

Q You said Atlassian provides Jira --

A Yes.

Q In a couple of instances now we talked about different options that may or may not be available. In terms of deciding how to set up the ticketing system, who at EIP was playing a primary role in that?

A So the choice of Jira was mine. It's kind of the default choice of any situation in which you want to do cloud based ticketing. It's extremely widely used across the tech industry. Of the people who did the setup, there's a variety of people doing that. There's two students especially who did lots of work, [redacted] [redacted] [redacted]. And I guess he wouldn't be for EIP, for later [redacted] did a lot of work on the Jira configuration.

Q And then once a ticket is received, who has the ability to comment or make any provisions on the ticket?

A Right. So a comment could have been entered by any of the, like, of the inner members of the EIP. Right. So analysts from us, UW, Graphika and Atlantic Council those are the people who could hack, could see all the tickets and could comment on any of them. Although in general you'd only comment on ones if it was your time to do so, if you were on call and it was your responsibility to do so.

The -- there's a pop -- there are different kinds of comments called public comments, which could be seen by either EI-ISAC or GEC if they had either we had tagged them specifically or they had submitted the tickets or we could add tech companies. So if we said, I want Twitter to see something, then you would add -- you would add Twitter to the ticket and then you'd fill out a public comment that would say Twitter, here's something you should look at.

Q And when Twitter is added to the comment, can Twitter see who first submitted the ticket?

A I am not sure. That's a good question.

Q During this time, did CISA at any point have access, the ability to see what was on a Jira ticket, either with access to public comments on Jira or receiving email notifications from Jira?

A I don't believe so.

Q With respect to when social media companies mentioned Twitter in the previous example, who is making the decision at EIP whether to tag a social media platform?

A So that would have been usually a conversation between the tier one and tier two analysts. So the tier one analysts were mostly undergraduates, the tier two were undergraduate students and post docs mostly. There were some undergraduates who operated in tier two. And so the would be a -- the tier one analyst's job was to find content to do the initial analysis to archive it, to open the ticket. And then at the could say, I think this needs to go to -- this looks like it is violating this policy or this is developing and they could tag in the tier two analyst who was on call to go make that determination.

Q What was your role in EIP once it's been operationalized?

A So there was a manager role that was above tier two for any escalations or questions and so I would occasionally take manager shifts.

Q Who else served IP the manager role?

A Kate Starbird, Elena Cryst, Renee Diresta. I think maybe one other person. It might have been Mike Coffield from the University of Washington, Camille Francois from Graphika, maybe Graham Bookie, I don't remember, but he was the leader from the DFR side.

Q When you are serving in this manager position and you are handling issues that have been escalated from tier two, what sorts of issues might be escalated from tier two to manager?

A So if something required -- if there is thoughts that this was something that was going really wide and we might want a write up about it, that would go to a manager to say yes, I think this deserves a --

So, for example the Sharpiegate was a great example of, like, this is becoming a big issue. And we made a decision let's write more about this. If they believed that there was a need for something really immediate -- so if there's a possible threat of violence, for example.

So we had a couple of threats of violence. We had that bomb threat as I talked about. So those are the kinds of things we would -- wanted them to escalate to a manager. Generally though it was the tier two analysts had -- the students had a lot of flexibility here and what steps they are going to take. This is for if they thought something was a corner case or if something seemed extremely urgent --

Q To your recollection, the decision whether to add Twitter, Facebook another external partner was made at the tier two level?

A I believe that's generally where it's made, yes.

Q Do you recall what criteria was used to determine whether a social media platform should be tagged or not?

A So the general criteria was it had to be obviously violative of the policies.

Q And at tier 2, when a person is making this determination, is it one person, is it multiple people?

A There might have been a conversation between different people or one person could have made it by themselves.

Q How big was EIP as --

A I think a little --

Q -- in 2020, I should say?

A A little over 100 people.

Q And of the 100, how many served in tier two?

A That's a great -- I'm not sure. I'd have to go look.

Q Do you know who at EI-ISAC was the individual or individuals who had access to Jira tickets that EI-ISAC was submitting?

A I don't. I believe they had a shift system themselves as well so that the person changed.

Q And is it your understanding that those individuals would have been employees of CIS?

A I believe they were. I am not sure.

Q Do you know if CIS was in contact with CISA regarding CIS's involvement in EIP?

A It's possible, but I can't speak as to CIS's relationship to CISA.

[Stamos Exhibit No. 8
Was marked for identification.]

BY [redacted]:

Q And this is some of the archived data from the Jira ticketing system that's been produced for the committee. There are many, many rows that its produced in Excel. Two rows have been pulled for exhibit 1 and --

[redacted]. Is this 8?

[redacted]. Exhibit 8, yes.

BY [redacted]:

Q So to be clear, this is an archived data version of what were Jira tickets. Is that consistent with your understanding?

A So yes -- what we turned over to the committee was an Excel spreadsheet that we exported from when we were done with the project we didn't need a live database anymore, we needed that the data in a way that we could do the analysis that you see in here and in our papers and so we downloaded the database as an Excel spreadsheet.

Q With respect to each of these columns, if you could help walk me through with respect to whether and how each column would appear that Jira ticket when it's first being addressed, when the system is still operational and it is in real-time. There are a couple that appear to be pretty self-explanatory who it is assigned to, who the reporter is.

If I call your attention to -- this is on the front page about middle of the way there. CIS misinformation reporting, do you know what that's in reference to?

A So that means that this ticket came through EI-ISAC from the CIS team.

Q Okay. And so when there are references to a CIS misinformation portal in other contexts, does that to you understanding refer to EI-ISAC?

A So if there is a portal that CIS was running, that would be different than this. That would be something that they would see. They would have then had to manually go and put it into our system, if that's what you mean.

Q Not quite. To your knowledge, was CIS operating a misinformation reporting portal separate from EI-ISAC?

A I --

Q Both independent of EI-ISAC.

A I know people could report to them. I am not sure exactly what the functions were. So it's possible they had a portal that was separate, yes. But they were not -- we did not have a portal on behalf of CIS to be clear.

Q Understood.

A Okay.

Q Great. To your understanding, and recognizing you were not at CIS at any time --

A No.

Q -- that is CIS could both receive reports and that was separate than the switchboarding function that EI-ISAC operated, that CIS operated. Is that what you are saying?

A I -- I don't know. I know CIS could get reports on behalf of the EI-ISAC and then they could choose to put them into our database. But I don't know exactly how you would communicate with EI-ISAC on the other side.

Q Gotcha. But to your understanding, when CIS misinformation reporting appears in the EIP system that is in reference to something that was submitted to EI-ISAC and that CIS decided to then submit to EIP. Is that correct?

A Yes. That's right.

Q Flip the page, backside of the first page, there's a column called description. And then there are a couple of examples beneath it. And for the top one it looks like there's been an email that was copy and pasted and it's from what appears to be a State official and sent to misinformation@cisecurity.org. To your understanding, is this an example of a report, this email I should say, not the fact that it has been copied and pasted, is this email an example of something that has been submitted via EI-ISAC by a State official or via a different reporting portal available to CIS?

A I -- this is obviously an email that belongs to CIS. Whether or not this is officially part of the EI-ISAC, I don't know.

Q Okay. So if there was a difference between the two, by the time it gets to EIP that to your understanding that distinction is not made?

A We would not know that difference.

Q Okay.

A And I'm not sure what reporting CIS would take outside of their EI-ISAC, but that's something you'd have to ask them.

[12:49 p.m.]

BY [redacted]:

Q All right. With respect to when a ticket is created, can we walk through -- you know, what is the first thing that happens? Is this type of description included on the ticket initially?

A Right. So when filling out the form to create a ticket, the CIS people, at least in this case -- and this is, I think, common with a number of the EI-ISAC tickets -- copy and paste it in whatever report they got into the description. And then they could fill out probably a couple of these other fields.

You know, all the times would be automatically generated. But, for example, priority based upon their definition of priority, those are probably the only ones they filled out themselves.

Q And when an EIP analyst -- we'll start with a tier 1 analyst -- sees this ticket -- first off, are tickets assigned randomly? You mentioned there were shifts. But when someone starts their shift, do they get to pick and choose which tickets they work on?

A Right. So in the different shifts, we had different assignments, effectively desks. This was COVID so people were generally not together. They were working from their dorm rooms or home and -- but they would have a specific thing they were responsible for.

So probably somebody -- I don't recall the exact assignments, but I expect that we had somebody assigned just to incoming. So if a new ticket was created based upon the shift, it would go in as effectively unseen, and they would have the queue open of tickets that had yet to be addressed, which is generally how ticketing systems work.

Q And when an analyst then takes on a ticket -- and we'll use these two as an example -- they would see the email that had been copied and pasted as a submission by CIS. Is that right?

A Yes.

Q If I could have you flip it over. This would be the front half of page 2, there's a column referring to fact checking.

A Yes.

Q Do you know who in EIP -- or first off, let me back up.

Is it someone within EIP who is responsible for filling out the fact-checking aspect?

A Yes. This is part of our checklist of things for tier 1 analysts to do was you can see it says archive URLs. So one of the first things they do is archive the content. As I said, one of our core things was to try to have a historical database here for further study. So they'd archive it in case it got taken down or deleted.

And then one of the things in the checklist was if a factual statement was being made, whether or not there were any other -- any fact checks or any other news stories to reference on that factual assertion.

Q If I could have you flip one more page, and it starts with the columns -- there's a comment column, and then comment 1, and it starts column 2, column 3, so on.

A Right.

Q Can you walk me through as far as what this would look like on the Jira ticket as opposed to what we're seeing in the archive data?

A Right. So in the Jira ticket, you would have -- the body of the ticket would have the initial email as we talked -- so the summary up top, so just a description. As you can see here, it says CIS dash. So my understanding is that reflects their internal database for CIS of their tracking number.

The description -- the issue key is just a monotonically generated integer of counting up ticket by ticket as it's created automatically by the system. So a bunch of these fields you would see there in the body, and then at the bottom people could comment.

And so what you're seeing there is it's like Reddit or Facebook or any other place with a common field is somebody could comment, respond, respond. And so these columns represent those comments in order.

Q Okay. And who can comment?

A So there are two kinds of comments. There were public and private comments. Private comments could only be EIP members. Public could have been comments that were made by EI-ISAC or GEC or one of the tech companies if they had been added to the ticket.

Since in this situation the ticket had been reported by CIS, the CIS people had access to those fields automatically.

Q And since it had been submitted by CIS, does CIS have access to these private comments that you referenced earlier?

A I don't believe so.

Q So even the entity submitting the ticket doesn't have access to those?

A That was -- the intention was they should not have access to that.

Q In this archived format, are you able to tell which comments are public and which are private?

A No. You have to kind of infer it by what is being said.

Q Okay. If there were -- to your recollection, were there instances where there were multiple tech companies copied, so, like, say, both Twitter and Facebook would be on a ticket?

A Yes. We actually document this in our report where we talk about -- so if you look at 38, page 38 in the main report, we talk about which tickets were -- which companies were tagged. And as you can see, it's over 100 percent, because you would have companies -- multiple companies that could be tagged on the same ticket since the ticket was about a narrative, not necessarily a single piece of content.

Q And when two companies are tagged, with the understanding that there's these private comments that they can't see but the public ones that are seen, if Twitter posts a comment and both Twitter and Facebook are tagged, can Facebook see what Twitter commented?

A I don't recall what they could see. It's possible. I'm not sure.

Q If I could have you turn to -- keep flipping until you get to column 5, please -- comment 5, that column.

A I see it.

Q Great. There's a comment -- there's some text before it, but the language starts: "We heard back from Twitter through CISA with this response: Our team concluded that the tweet was not in violation of our Civic Integrity Policy."

Do you know what role CISA is playing that is referenced here?

A So I expect this comment was from EI-ISAC. I can only assume based upon what I see here. I have no other knowledge of what role CISA was playing.

Q Okay. So with the understanding that -- so it doesn't seem like this comment came from you. But based off your experience in EIP and seeing this Jira ticketing system, do you know whether CIS was working with EI-ISAC?

A I know CIS has a relationship with -- or CISA has a relationship with CIS. I don't know exactly what that was like.

Q Do you recall any discussions with the social media companies whether they had the understanding that CISA was working with the EI-ISAC?

A I don't recall that being something they'd discuss, and I'm not sure why they would discuss that with me.

Q If I could have you keep flipping until we get to comment 11, that column.

A Uh-huh.

Q There's, again, like a string of letters and numbers, but the text starts: "Thanks EIP. We have kept the election official updated on the steps you took. We also received confirmation from Facebook (by way of CISA) that Facebook took action on this case."

Same question. Do you know what role CISA is playing here?

A No. I expect that this -- since this says "Thanks EIP" and we have kept the election official updated, that this was posted by the EI-ISAC team. They're referencing CISA, but I don't know exactly the relationship between the EI-ISAC and CISA.

Q But it is your understanding -- I mean, CISA introduced EIP to EI-ISAC. Is that right?

A Yes. I know that, obviously, the EI-ISAC was operating with CISA's blessing to run a switchboard, but what specific role was being played in this is outside of our knowledge.

Q Do you recall if -- let me strike that.

Throughout the 2020 election that the EIP is operating in, would you make public posts from time to time regarding decisions that EIP was making?

A I wouldn't say they're about decisions we were making, but we did public posts about the narratives we found.

Q And do you know if -- actually not do you know.

Do you recall any interactions with officials at CISA regarding the narratives that you were finding?

A It's possible we briefed them. I don't recall any specific conversations.

Q Okay. If you were to brief CISA, what form of communication might that be?

A Well, I expect we would have e-mailed them if we wanted to have a meeting with them.

Q Okay. And who at CISA was your primary point of contact during the fall of 2020?

A Probably Matt Masterson or Brian Scully you could say.

Q Was there a time where you briefed the tech companies on what EIP is when you were first inviting them?

A Yes.

Q And when that briefing occurred, had you already made the decision to have EI-ISAC as an external partner?

A I don't recall the order in there.

Q Okay. Do you recall a time where external stakeholders were brought together for a briefing, including tech companies and the EI-ISAC?

A We did lots of briefings. It's quite possible it happened, yes.

Q Do you know with the Jira ticketing system, could someone download a ticket ever? Is that a function that was available?

A As the administrators, we could download full spreadsheets. It's -- I don't know exactly what configuration we had on individual tickets. Certainly you could always print a ticket. So if you wanted to have a record yourself, you could always generate a PDF.

Q Okay. Again, with respect to the commenting system, I'd asked about Twitter and Facebook and whether -- if Twitter comments, can Facebook see it. Same question, but with respect to if GEC is the one that submitted the ticket and is able to see what's going on, do you recall instances where GEC was on a ticket with Twitter and Facebook as well -- Twitter or Facebook?

A It's likely. We've turned over all of those tickets, so it should be obvious from the organizations field. So if that was true, you would have GEC as well as Facebook and/or Twitter tagged in organizations.

Q And to your recollection, same dynamic or same question as the Twitter/Facebook one. If GEC commented, could -- and both GEC and Facebook were tagged, could Facebook see GEC's comment?

A I don't recall. I know that the company should have been able to see the initial description. So if GEC put in something in the initial description, the companies would have seen that, but I'm not sure about the comments, what they would have seen.

Q Okay. At what point in time -- so, obviously, it's operational through at least the election of 2020. At what point in time did the Jira ticketing system -- was it no longer operated and then you switched to this archived version of the data?

A Well, we stopped our collection a couple of weeks after -- we've got the exact date in here -- of the election, so that's when we stopped changing it. And so probably some point early in 2021 when we were changing the project from -- so it says right here, you know, we started data cleanup in -- around the end of December, so that's when we would have had to export and start to do all of the work necessary to do the analysis. So there's an operational timeline on page 3. So I'm guessing it would have been in the end of December, beginning of January.

Q Do you know if this archival process was automatic?

[redacted]. Oh, [redacted].

[redacted]. We've got 30 more seconds.

A Okay. We manually went in and said we wanted to export the spreadsheet, if that's what you mean.

BY [redacted]:

Q Okay. So it was not an automatic process, just a point of clarification?

A We had to -- we had to say we want to export.

Q Yeah. And did you have to go to Atlassian to do that, or is it just an option as a user to do that?

A If you were an admin, you could just go and click a button in Jira to say export everything.

Mr. [redacted]. Okay. Could we go off the record, please?

[Recess.]

Ms. [redacted]. Okay. It is 1:48. We can go back on the record.

BY [redacted]:

Q Mr. Stamos, I want to start by talking through some comments that were made in the prior hour before the break.

A Okay.

Q There was some discussion about an NSA briefing.

Do you recall that?

A Yes.

Q And you said that that was a briefing for a General Nakasone. Correct?

A And his staff.

Q And his staff?

A Yes.

Q A virtual briefing?

A Yes.

Q Okay. And did they request that briefing?

A General Nakasone did.

Q And why -- what's your understanding of why he requested that briefing?

A He had come to Stanford and had visited a number of people, and we -- as part of that visit, I went in with some of my colleagues from SIO, and we gave him an overview of a bunch of our work, and he said -- and it included, you know, the work we were doing to get ready for the election. And he said something along the lines of we'd love to hear from you of what kind of concerns you have for interference in the fall.

Q Okay. Were there -- the concern was specifically foreign influence campaigns. Correct?

A That's right, yes.

Q Okay. So did he -- during that meeting, to the extent you recall, was it primarily you providing a presentation about what you were seeing?

A It was me doing a presentation about the capabilities of various actors that we had been tracking and some of the things we were concerned about them doing from -- at the time and still, one of the things we talk a lot about is kind of hybrid warfare.

So one of our big concerns was if you were one of these high-end government groups, similar like PLA, GRU, not the Russian troll farms, but like the high-end guys, you could attack election infrastructure.

Third, in the chaos, it's really hard to actually change votes. It's not that hard to make things break. And then break things and then use that as a basis of a disinformation attack to say that the election is being stolen, something is going on.

And so we talked a lot about that kind of stuff and what we would be looking for and the threat posed by various adversaries in that area.

Q Okay. Thank you for that.

And so the focus was completely on foreign interference. Right?

A Yes.

Q And it wasn't about -- well, withdraw. Strike that.

A He specifically asked us to brief on foreign interference.

Q Okay.

A And knowing that the NSA is not allowed to operate domestically, I would have never talked about domestic actors.

Q All right. There was some discussion in the earlier hour -- actually a fair amount of discussion on CISA. And I want to take a step back and talk through what CISA, is, what it does, what its role is.

I think you were asked, maybe actually in the first hour, when CISA was created. Do you remember that?

A Yes.

Q And I think you said you thought it was 2018, but you weren't sure?

A Yes.

[redacted]. So I want to introduce the printout from Congress.gov, which is the reflection of the bill that created CISA. This will be exhibit number 9.

[Stamos Exhibit No. 9
Was marked for identification.]

BY [redacted]:

Q And this was bill number H.R. 3359, Cybersecurity and Infrastructure Security Agency Act of 2018. And if you see up at the top, it says: "Latest action: 11/16/2018 became Public Law No. 115-278."

Do you see where it says that?

A Yes.

Q Okay. And then if you look up above that, it says the bill's sponsor was Representative Michael McCaul, Republican of Texas.

Do you see where it says that?

A Yes.

Q Okay. And looking down further, I want to start at -- we'll start at the bottom of the actions and work -- it's in reverse chronological order.

So the bill was introduced in the House on 7/24/2017?

A Yes.

Q Do you recall which party was in control of the House in 2017?

A I believe it was the Republican Party.

Q Okay. And then it was discharged -- it was reported by the Committee on Homeland Security on 12/11/17 and then discharged by a number of other House committees on that same day.

Do you see where it says that?

A Yes.

Q And so one of the committees that discharged it was the Committee on Oversight and Government. Do you see that it says that?

A Yes.

Q Are you aware that Mr. Jordan was a member of that committee in 2017?

A I was not aware.

Q Okay. And then later that day, on 12/11/17, it says it was passed and agreed to in the House on suspension.

Are you familiar with what the term on suspension -- on the motion to suspend the rules and pass the bill means?

A I mean, I believe that's when it's basically unanimous and people say they don't want to slow things down, so nobody objects and, therefore, it passes.

Q Okay. So in December of 2017, this passed the House, essentially a Republican House -- Republican-led House essentially unanimously in December. Correct?

A Yes.

Q Okay. Then it went over to the Senate. Do you know which party was in control of the Senate in 2018?

A I believe it was also the Republican Party.

Q Okay. So it passed through the Senate Committee on Homeland Security and Governmental Affairs on the 3rd of October, 2018, and then it says it was passed the Senate by -- passed the Senate with an amendment by unanimous consent also on 10/3/2018.

Do you see where it says that?

A Yes.

Q So it also passed the Republican Senate by unanimous consent. Is that right?

A Right.

Q Then there was a conference to resolve differences. It, again, passed the House and the Senate without objection.

Do you see where it says that?

A Yes.

Q Again, House and Senate were both Republican held at the time?

A Right.

Q And then it was presented to the President on 11/14/2018 and signed into law on the 16th of November?

A Yes.

Q Who was the President on November 16, 2018?

A To the best of my knowledge, it was Donald J. Trump.

Q Okay. Thank you.

So CISA was created through this bill that passed unanimous consent in the House, unanimous consent in the Republican Senate, and was signed into law by President Trump. Is that correct?

A Yes.

Q Okay. I want to turn to a CISA web page on election security. This will be introduced as number ten, exhibit 10.

[Stamos Exhibit No. 10
Was marked for identification.]

BY [redacted]:

Q And before we actually get into the meat -- you can take a moment to review, and then I'm going to ask you your understanding of what CISA's role is with respect to election security.

A Okay.

Q You were asked earlier about the definition of election infrastructure and who identified it.

Do you see on page 2 the second full paragraph that says: "In January 2017, the Department of Homeland Security officially designated election infrastructure as a subset of the government facilities sector, making clear that election infrastructure qualifies as critical infrastructure."

Do you see where it says that?

A I do.

Q Okay. So that would have been January 2017, so right at the turnover of administrations. Correct?

A Yes.

Q Okay. And as far as we know, throughout the Trump administration, there were no steps taken to roll that back?

A No, I don't believe there were.

Q Okay. And then we spoke in, I think, my first hour about what election infrastructure is.

A Uh-huh.

Q And they have a list here. So I just want to go through and ask you kind of your understanding of what each one of these things are.

So it says: "Election infrastructure is an assembly of systems and networks that include, but is not limited to:

"Voter registration databases and associated IT systems."

Are those the -- those are the technical systems that hold voter registration data. Correct?

A That's right. I think they also probably mean the web interfaces and the other ways by which voters can change their information and interact with the databases.

Q Okay. And then it says: "IT infrastructure and systems used to manage elections."

A Yes.

Q So, again, that's all -- that's IT systems. Right?

A Yes.

Q Okay. "Voting systems and associated infrastructure," are those actually the voting machines? Is that your understanding of that?

A I expect that means the voting machines and probably things like the counting systems. Where, like, a counting system falls between IT infrastructure and voting systems is an interesting question, but yes.

Q Okay. "Storage facilities for election and voting system infrastructure." Are these, like, warehouses, I guess, where the voting machines might be held?

A Yes, I believe so. And I don't think this is a mistake because there have been a number of issues where in the years between elections devices have been lost or stolen or they can't have chain of custody. So I expect that that's a focus on where do you keep all of the polling information and voting information in those off years.

Q Okay. And then "Polling places (to include early voting locations)," so that would be probably both the actual physical places where people can go to cast their vote and potentially drop boxes as well?

A That's what it sounds like, yes.

Q Okay. So these are the actual technical systems, the means by which people vote. Correct?

A Yes.

Q Has nothing to do with the politics around voting; it's really the operation of the vote. Is that fair to say?

A Yes.

Q Okay. And then on the next page it says: "CISA's Role." And it says: "CISA is committed to working collaboratively with those on the front lines of elections -- state and local governments, election officials, federal partners, and private sector partners -- to manage risks to the Nation's election infrastructure."

Do you see where it says that?

A Yes.

Q Okay. And, again, the infrastructure is what we just read through?

A Yes.

Q All the technical -- the nuts and bolts of how voting operates. Right?

A Right.

Q So CISA is actually tasked with working with the State and local governments? Right? That's part of their role?

A That's my understanding, that they are the agency that has been given the primary responsibility for coordinating the security of the election.

Q And EI-ISAC that we talked a fair amount about, they're kind of -- is it fair to describe them as something of a trade organization for local election directors or State and locals?

A I mean, EI-ISAC is its own thing. I consider it a collaborative -- a defense collaboration.

Q Okay.

A But, yes. The closer to a trade association I think would probably be NASS and NAZB.

Q Okay. So EI-ISAC is -- so the member organizations are -- or the member entities are State and local election officials and entities. Right?

A That's my understanding, yes.

Q Okay. So EI-ISAC is effectively a conglomeration of those entities, and then it interacts with CISA, which is actually what CISA is supposed to do is interact with State and local entities. Right?

A Yes.

Q Okay. We can move on probably.

A Did I pass the civics test?

Q You did.

A Okay.

Q I want to turn to the Jira tickets that we talked a fair amount about in the prior session.

And you said earlier you were the one who selected the Jira software. Right?

A Yes.

Q And you said it's a pretty commercially widely available software?

A Yes. I believe it is the most widely used ticketing software in software development certainly.

Q And is that -- so is it used -- obviously, you use it in your work with research regarding the spread of information online. But is it also used in other social research contexts, to your knowledge?

A I'm sure it is, but I can't -- I can't think of any specific examples right now.

Q Okay. So we talked through the columns, and I want to turn back -- actually I don't know which exhibit number this was.

[redacted]. Eight.

BY [redacted]:

Q Eight. We talked through the columns in exhibit number 8, and we talked through a couple of different examples.

There's a lot of -- and I'm not sure if it's actually in this example or not. What was exported and produced in the Excel spreadsheet, there's a lot of columns for comments. Right?

A Yes.

Q Why are there so many columns for comments?

A My understanding is when you export a spreadsheet from Jira is it needs a way to represent all of the comments, and some tickets might have zero comments, and some could have 50. So if you're going to represent that in a spreadsheet, you need a column for every single -- the number of columns needs to be equal to the maximum number of columns -- of comments on the max -- of the ticket with the maximum number in the database.

Q And I guess what I'm getting at is we talked through in the prior hour the comments that reflected interactions with social media companies.

A Right.

Q There was actually a lot of internal comments back and forth between students and supervisors and, I guess, potentially between researchers and each other. Right?

A Yes.

Q And was that actually the primary purpose of Jira was to help do that analysis of this material internally?

A Yeah. The two primary purposes was, one, as the data repository that we could use for our analysis and, second, as the way that our people could interact with each other and to track their tasks. So just like a -- ticketing systems are often used in situations where people work shifts so that you don't -- instead of e-mailing Bob, if Bob is done at 8:00 p.m., then you don't want that sitting in Bob's inbox. You want there to be a ticket that then the next person who comes on the shift it's their responsibility to finish the work.

Q Okay. So it was kind of an internal communication method?

A Internal communication, and it's our primary research database. So, like, for all of the data that went into our publications, the primary database where that was stored was Jira.

Q And a significant amount of the information that was produced to us were tickets that were generated by EI-ISAC. Right?

A Of the stuff that was produced --

Q Right.

A -- that includes all of the tickets that were generated by EI-ISAC, yeah.

Q But that's not actually representative of the total number of tickets that are in the database. Right?

A That's right. So in our report we document the number of tickets, which I believe was -- so in our final summary, we had 639 in-scope tickets. So the actual number in the database is closer to a thousand. This is from later us taking out things that -- test tickets, test data, situations in which two tickets turn out to be about the same thing.

Q Okay.

A So all of those things were condensed before we did our analysis so we didn't have duplicates. And I believe there's something like 100 and some tickets involving EI-ISAC, so it's less than a sixth.

Q Okay. So less than a sixth. Thank you for doing the math for me because I could not have done that in my head.

A Sure. How about, like, I'll do the math, and then you can explain how Congress passes laws in a moment.

Q So EI-ISAC, which is operated by CIS -- and I'm sorry. CIS is the Center for Internet Security. Right?

A Yes.

Q Okay. The State and local election officials would send them reports, and then EI-ISAC would effectively just pass them along to you. Right?

A They made a determination. I'm not sure how of whether to pass it along.

Q Right.

A But, yes, they would take, as we can see in here, emails they would get in, and then they could put that into a ticket for us.

Q And I guess my point isn't that they were passed along. It's that the original incoming information came from State and local officials. Right?

A That's right. If you look through the EI-ISAC tickets, I think for almost all of them you should have an original email that we can see where it came from.

Q Okay. And so we just talked through CISA and CISA's role. CISA's role is actually to interact with State and local election officials. Right?

A Yes.

Q Okay. So to the extent that CISA's name shows up in these, it's kind of part of their task, right, under the law that was passed by the Republicans in 2018?

A As I told [redacted], I can't speak to exactly what CISA's role was in some of these tickets where they were not communicating directly with us because they could not get directly into this.

Q Okay.

A So I don't really feel comfortable answering that.

Q Okay. Understood.

Do you have an understanding of why State and local election officials would be concerned about the information that they were flagging?

A Yes.

Q And what's your understanding of that?

A So I think it matters in the situation. In the situation where they found that somebody was misleading voters about how to vote, when to vote, that that is -- you know, part of their job is to enfranchise their voters, and that would be obviously quite upsetting if you did all of this work to educate people and then it was being undone by some influencer on Instagram. And so that's part of their job to make sure people are properly educated.

In some of these cases, they're probably worried about people who are trying to drive violence. So I believe we have a number of tickets where individuals are making claims about individual voting workers. This is one of the trends in 2020 that I think was an unfortunate new thing that might be with us for a while is trying to intimidate individual people who are working, the little old ladies that work in the polling places, as well as the employees who were like -- could make more money doing anything but working for their county, but then they're having their information posted and such. So in those situations protecting your employees would be a big deal.

So, yeah, I mean, I think there's a variety of reasons why they would be really worried about disinformation in their area.

Q And I think you touched on this earlier, but I'm not sure I heard the response.

Could it have been possible for you -- for EIP, I mean, to have set up a system where every State and local election official in the country could have just e-mailed you directly with items of concern?

A I think that would have been impossible with the amount of time we had. My understanding is, you know, one of the things CISA had to do here is just get the email addresses and the phone numbers of election officials, and that by itself was a massive project because there's thousands and thousands of people. And as you can see if you look through the tickets, there's, like, Yahoo accounts, Gmail accounts, AOL accounts. So it's not like they're all coming from.state.oh -- or something -- u.s.

And so having like an authenticated list of people that we could interact with would have been impossible.

Q Okay. And I'm sorry. You said one of the things that CISA had to do. Does that mean that CISA had to do to set up?

A I think to set the switchboard, so I'm not sure if that work was done by CISA employees themselves or if that was done by EI-ISAC. But in creating the switchboard, just having the contact information for all of those people, was a huge project.

Q Yeah. Okay. But, again, CISA was not flagging any material or sending any material to you. All they did was set up this switchboard that then enabled State and local election officials to pass things on to you efficiently?

A That's right. I'm not aware of any situation in which any of the content that was referred to us came from CISA itself.

Q Okay. I want to look at -- actually, I want to talk through, before we get back to this exhibit, the process of what happened after EI-ISAC created a Jira ticket.

So EI-ISAC creates a Jira ticket. And is there an alert for an EIP researcher? What happens next?

A It would go into a queue. I'm not sure whether generating an alert. But it would have been somebody's job to handle the incoming queue.

Q Okay.

A So they would have then gone and said, I'm taking this over. There's a button you can push to say this ticket is assigned to me. So a ticket at any moment has to be assigned to somebody, and they assign, okay, I'm taking and then they -- I'm taking responsibility for this, and then they would run the checklist of things that we had given our students of go archive it, go fill out -- we had our little form with all the little form fields. You can see how much is it spreading, how's it going viral, are there news stories or fact checks related to a factual concern, what category is it in. Part of that would be if it was not in one of those categories that we were paying attention, then they would mark it as out of scope and close the ticket; prioritization and such, and then they would fill out a little bit of a narrative in the comments of this is what I found.

Q And you said earlier -- you said just a second ago that one thing they would track would be how far it's going and how fast it's going. I think the spreadsheet uses the terms "reach" and "velocity." Is that --

A That's right, yes.

Q Okay. And so why were you interested in assessing reach and velocity?

A So a big part of this project was trying to understand how do viral rumors go viral. And so we were trying to study in real-time how do things go big. We actually have some interesting conclusions in here, I think, that were unique in that -- in some of our published papers, that we have a unique model of -- at least in this election, one of our findings was that virality for most of these narratives was not driven by kind of authentic engagement by individuals but by a relatively small number of influencers, who the moment one of those influencers said -- retweeted something or shared something or said, "I can't believe this is happening," usually a little comment, that would be the start of what we called the hockey stick.

So that you would have some claim about Sharpies or something that would -- you know, a couple of people are looking, a couple of people. And then one of the influencers -- you know, we have the top 25 list -- so Don Trump, Jr. retweets it, and then you'll have all the influencers retweet it, and then it goes exponential.

So one of the things we were studying was how quickly are things growing. Is it growing in a way that it's people organically looking at it, or is it growing because one incredibly powerful person gave it a kick?

Q Okay. And so, again, that was part of your research, the research function of EIP. Right?

A That was part of our research, and that directly went into our analysis and the papers we wrote.

Q Were you surprised by that finding?

A I was. I mean, we always knew that influencers were important, but something that we came out of this understanding is that very few things actually went viral on their own without a relatively small number of people deciding to make them a big deal.

Q Okay. So in certain instances after the -- so it sounds like there was an extensive analysis done of whatever the material was that had been identified. Right?

A Yeah. So we have that calendar in here where we spent months in the big -- in the first quarter of 2021 doing the data analysis so that we could write this paper. And then there's work that happened after that, after this report, for our peer-reviewed journal articles.

Q I'm actually talking about the period during the election.

A Oh, I'm sorry.

Q So when the ticket came in and there would be certain information entered between -- by the students -- and the researchers are mostly students. Right?

A Yes, the majority. 42 of our 50 people were students.

Q So there would be certain information entered by these student researchers, and there would probably be some discussion amongst them or between them and a supervisor. Right?

A That's right, yes.

Q And then at some point -- in certain instances, EIP did make the call to bring certain content to the attention of social media companies. Right?

A That's right.

Q Okay. How did EIP determine what content was appropriate to bring to the attention of social media companies?

A So we had a couple of criteria. If something was dangerous, that was something that we would do immediately. So if we thought there was either a threat to somebody's life or things like the bomb threat situation, then those are the kinds of things that would kind of jump to that, even if it wasn't of high spread. Right? So threatening somebody's life or posting the personal details, even if it only had ten retweets, that would be a big deal for us.

If people were doing an impersonation -- again, they didn't have to be widespread, but if somebody was pretending to be an election official, that's something we would report really quickly. And then if something violated their policies and it had good reach and velocity and it clearly violated platform policies, then we could refer it to them.

Q Okay. So just to repeat back what you said, threats to life or safety or health?

A Yes.

Q Impersonations?

A Yes.

Q And then the third category would be something that potentially violates platform policies?

A Right, and that has a reasonable amount of spread. We -- you know, if somebody just said something and four people saw it, even if it was, like, very violative policies, if there wasn't a real risk to people, then we probably wouldn't have said anything. If it got 50, 100, 2,000 retweets and we saw that the velocity was extremely high, then that would be much more likely that we'd point it out to them.

Q Okay. And once you pointed something out to a social media company -- I think we talked through this earlier, but just, again, for the record, once you pointed it out to the social media company, it was up to those companies to determine whether a post actually violated their internal content policies. Correct?

A That's right.

Q And it was up to them to determine whether to take any further action?

A That's right. It was totally up to them.

Q And they never came back to you and said, you know, what do you -- what's your opinion of this action?

A I don't -- I don't know of any situation in which they asked for our opinion on their action. Generally their response is, if you look at the tickets, are ack, which is acknowledge, thank you, and maybe sometimes they would tell us what they did. To do -- we actually have empirical evidence of what they did. To put the empirical evidence together, we actually had to test it ourselves because generally we would not be told by the companies what actions they took.

Q Okay. So I want to turn to this exhibit 8 now, and I want to talk through the interactions of social media companies. But before I do that, I want to actually look at the underlying content that's referenced.

So the first one, it's Case No. -- I'm sorry. It's issue EIP-482.

A Uh-huh.

Q And it's -- we talked through earlier. It says: "CIS Misinformation

Reporting."

A Yeah.

Q If you turn to the next page where it says "Description" at the top, it says: "I'm reporting this" -- it looks like it's an email, appears that the email sender said: "I'm reporting this disinformation about elections. Please take steps to stop it, and correct it publicly. Thanks."

A Yes.

Q Okay. And then on the next page, under "Archive URLs," it says -- there's a web address. It's web.archive.org/save/https://twitter.com/realDonaldTrump/status -- then there's a long string of numbers.

Do you see where it says that?

A Yes.

Q Okay. I want to introduce what that is into the record.

So this is exhibit number 11.

[Stamos Exhibit No. 11
Was marked for identification.]

BY [redacted]:

Q So this is a tweet from @realDonaldTrump. It says: "Strongly trending (Google) since immediately after the second debate is CAN I CHANGE MY VOTE? This refers to changing it to me. The answer in most states is YES. Go do it. Most important Election of your life!"

And it's 6:53 a.m., October 27, 2020?

So this is a tweet that then President Trump put out. In your assessment, does the question about changing your vote, is that accurate, do you believe?

A My understanding is no. I think because this is in pre-voting so that you would be talking about, for example, absentee ballots is that you cannot change your vote. And, in fact, if you went and tried to send another absentee ballot in, you would be violating the law.

Q Okay. So this is -- and it looks like there's a fact check -- I don't actually have the fact check. But on its face, there's certainly questions about whether or not this is true?

A Right. And if you look in this, here are multiple stories about it. So if they were in here, this means that the student looked at those and that they had a factual refutation of the claim that was being made here.

Q Okay. And a little further down on the page it says the reach was viral, 1,001 plus engagements.

A Yes.

Q Is 1,001 plus engagements, is that like a category? Does that just, like, mean it's the most viral it can be?

A Yeah. So this is the reach -- I believe this was a drop-down box that you could choose from a level, and I believe this was viral was the top, over 1,000 engagements.

Q Okay. And then it says -- on the next page -- sorry -- the column that says "Velocity," it says: "Growing: reach is growing linearly."

A Yes.

Q Do you see where it says that?

A Yes.

Q What does that mean?

A So we have a couple of different velocity options again in a drop-down box.

And so you can see two of them here. One would be linear, so it is growing, but not crazy. Viral would be the top level of growth, which means it's going exponential, like there's a curve like this [indicating].

Q Okay. And then I can't quite figure out from this spreadsheet if this was actually referred to Twitter or not, but I'm gathering that it was because of the response.

A Right. So there is a response here from Twitter: "Twitter received and is reviewing." You can also check --

Q I'm sorry. Which column is that?

A Comment 3.

Q Thank you.

A You can also tell it went to Twitter because if you look in platform column, which is near the end, it's labeled with Twitter. And so that meant that they had been added -- or I'm sorry -- not the platform column; the organizations column. So those organizations, those are the people who could see the tickets. So Twitter had been added specifically. Platform was just our own internal designation.

Q Okay.

A The organizations is the people who could see the ticket, so we have added @Twitter.

Q Okay.

A And this is clearly a message from Twitter saying Twitter received.

Q Okay. Twitter -- so this was sent to Twitter. Twitter did see this?

A Yes.

Q You did refer this effectively to Twitter?

A Yes.

Q And then I want to look at column 5, comment 5. And what it says is -- I think we read the first part of that sentence but not the second part. So the full sentence is: "We heard back from Twitter through CISA with this response. Our team concluded that the tweet was not in violation of our Civic Integrity Policy."

Do you see where it says that?

A I do.

Q Okay. So it says: "We heard back from Twitter." So it sounds like Twitter didn't actually even tell EIP directly?

A That's right. They -- generally companies -- it was a crap shoot whether or not they would tell us what they were doing.

Q Okay.

A They usually would just acknowledge it.

Q Okay. But at the end of the day, Twitter concluded that this tweet was not in violation of its content moderation policies. Right?

A That's right.

Q So they didn't take it down, at least not at that time?

A At this time they didn't take it down, no.

Q So this is an example of a situation in which the EIP flagged content for social media. The social media company, in this case Twitter, I guess assessed it against its own policies, or did something with it -- we don't know -- and came back and said, no, this doesn't violate our policies. Right?

A That's right.

Q Okay. So you had no control over that. You just sent it off, and they did what they did and sent it back and said no?

A That's right. And we, in fact, have hard empirical evidence on this, in that we went -- for the 4,000-some URLs that were sent to any platform that we went and checked them after the election of what had happened to them, and we found that in only 35 percent of the time had they made any decision, which is what you would expect if they were making their own determination per their policies of what they should do.

Q Sorry. So in only 35 percent of the time had they make any decision, meaning that --

A I'm sorry. Did they take any actions on anything we referred to them.

Q So in -- sorry. So in 65 percent -- am I doing the math right? In 65 percent of the time, they just didn't do anything with it at all?

A That is yes. That is what we saw. And the most common action -- and so I'm now looking at pages 39 and 40 of the report.

So of the 35 percent, the way that breaks down is 21 percent of all the URLs that were reported were labeled. 13 percent were moved, and one was called soft blocked, which means it wasn't removed, but it was hard to get to.

Q Okay.

A So the vast majority of time -- first, the majority of time they did not take any action on our report. And when they did, the majority of the time almost two-thirds of the time, their action was to label it. And generally the labels here were pretty generic. It was something like: Elections are complicated. Here's a link to our platforms, information, or our voting center, or something like that.

Q Okay. And you didn't have any insight into why they took particular actions with respect to any particular tweet?

A No. If they got back to us, sometimes they would say: We determine this is not violative of policy. And that's I think the most we would generally ever here. We had to make this table by going -- we built software that went and checked every single URL to see how it was being treated at that time.

Q And I want to look at the next example that was presented. It's EIP-257.

A Uh-huh.

Q This is misinformation related to absentee ballots and fraud. And there's actually -- there's not an archived web -- an archived URL for this one. But I think it says -- if you look at the description on the bottom of the second page -- or I guess the back of the first page, it says --

A So -- I'm sorry. Yeah, I see.

Q So I want to -- so I actually want to look at comment number two, which is where the description is.

A Uh-huh.

Q So it says: "This user is claiming that his father who died in 2018 received an absentee ballot in the mail. According to" -- and then it has a link to the Connecticut Election Services website -- "from the state of Connecticut, ballots are not mailed to individuals until October 2nd, 2020. It's possible (following the calendar) that the mail was in fact a registration form." And then it has a link to what appears to be the post.

Do you see where it says that?

A I do, yes.

Q Okay. So, in this instance, it appears that this content involved a claim that could not have been true. Correct?

A Yes.

Q Okay. And it specifically concerned ballots sent through the mail?

A That's right.

Q And ballots, you would agree, are a key part of election infrastructure?

A Yes.

Q Okay. And so if there's claims spreading about -- inaccurate claims spreading about whether ballots are available, that could impact people's ability to -- whether people choose to vote in an election or it could impact whether they do vote in an election?

A Yes. In fact, I think what the evidence shows is that all of the discussion that's incorrect about vote-by-mail ended up disenfranchising a decent number of people who decided not to utilize voting by mail during COVID and perhaps didn't vote at all.

Q Okay. And so in my first hour of questioning, we talked about time, place, and manner. This is kind of core time, place, and manner. Right?

A Yes.

Q And then turning to the description that we -- it's the second page, the description. It appears that the original flag came in from an individual named Gabe Rosenberg. If you look, he is the communications director for the Connecticut Secretary of State at the time. Right?

A That's what this says, yes.

Q So the individual who actually identified the concerning information worked for the Secretary of State of Connecticut?

A That's correct.

Q And presumably the Secretary of State of Connecticut would know for a fact the rules around time, place, and manner for voting in that State. Right?

A You would hope so, yes.

Q Okay. And I want to walk through one more example. We actually -- so we didn't print off the spreadsheet quite like this because in the examples I'm going to show you there were a lot of columns that were unused. So to make it a little more usable, we just took it out and put it into a single page. So it's not how it appears in the actual spreadsheet.

So this is exhibit number 12?

[Stamos Exhibit No. 12
Was marked for identification.]

BY [redacted]:

Q And I'll give you a minute to review it.

A Okay.

Q So this is EIP-396.

A Uh-huh.

Q The short summary is described as "Potential for voter fraud in Oregon and Washington."

And I want to actually introduce the -- we don't have it on the sheet that I just handed to you, but the archive URL, the actual underlying Facebook post at issue.

We'll mark this as exhibit number 13.

[Stamos Exhibit No. 13
Was marked for identification.]

BY [redacted]:

Q And it says, the comment 1 says: Hi Facebook, Reddit, and Twitter. This claim, based on a 4chan thread, that voter can be changed and mail-in ballots cancelled with only limited personal information is rapidly spreading online. There is an associated Gateway Pundit story that is a primary catalyst for the spread of the story off 4chan. The Gateway Pundit headline does nothing to dispute the claims even though a number of them are debunked in the story itself. Other claims within the story are left unfact checked with the publication simply stating 'We have not yet been able to confirm or debunk this claim.'

As the headline '4chan Users Claim to Have Found Way to Easily Change People's

Voter registration and Cancel Ballots Online in Oregon and Washington' leaves open false claims (debunked within the article itself) that delegitimize voting we recommend it be removed from your platforms?"

Do you see where it says that?

A Yes, I do.

Q Okay. So in this instance there was actually -- this is a claim about changing votes, changing ballots. Right?

A Yes.

Q Again, that's kind of core time, place, or manner. Right?

A Right. I mean, I believe they're making the claim that you could cancel ballots and that people had that ability, which is I believe not true.

Q Okay. And understanding that, what I want to look at actually is comment number six, because it appears that this was actually sent to Facebook. Right?

A It was sent to Facebook, Reddit, and Twitter.

Q Facebook, Reddit, and Twitter. And I'm sorry, is -- comment number one is that an internal comment? Is your read on that that that was a comment from student researcher sending this to Facebook and Twitter and Reddit or --

A This would probably be the tier 1 or tier 2 student --

Q Okay.

A -- writing this out, and then it would be a public comment that was seen by them.

Q Okay. And I think in the spreadsheet we don't know what Facebook -- what Twitter and Reddit did with it.

A Right.

Q But I want to look at comment number six. It says: "[REDACTED]," which

I believe is the name of the student here?

A Yes.

Q "Just following up here. Thanks for flagging this content. After a thorough review of the content, we can confirm that it doesn't violate our community standard as it relates to Voter Suppression." Correct?

A Yes.

Q Okay. And so Facebook didn't take this down. Correct?

A Most likely did not.

Q And I want to look at what we've introduced as exhibit 13, which is the actual Facebook post.

There's no label on this. Right?

A I'm sorry. What do you mean by "label"?

Q So there's not -- it's not labeled as inaccurate on the face of the tweet -- or on the face of the post?

A Yes. Facebook has not applied the label to this, no.

Q Okay. And if you look up in the upper left-hand corner, do you see where it says "6/22/23 7:33 p.m."?

A Yes.

Q That was yesterday. Right?

A Yes.

Q Okay. So we actually printed this off yesterday. This is still up on the web today?

A Right.

Q So there's been no action taken on this post?

A That's right. This would be in the 65 percent of the URLs in which no action was taken.

Q Okay. So just because a student analyst recommended that something be removed didn't mean that social media companies actually removed the content. Correct?

A That's correct.

Q Okay. Was content moderation the primary goal of the EIP?

A No.

Q Okay. And, in fact, an example like this where the ticket was not where -- sorry -- where the information was flagged for a social media company but it was not actually taken down by the social media company, would this still be of use to EIP for your research purposes?

A Yes. So we were able to archive this and then include it in our analysis of the different narratives that were being spread.

Q Okay. And it's because EIP was, by and large, a research project. Right?

A Yes. The fact that 65 percent of the time steps were not taken does not mean the project was a failure. In fact, I think it was a success because of the research we did.

Q And the 65 percent of the time, that's only of the things that were actually raised to the attention of social media companies. Right?

A That's two things. One, it's only things that were raised to their attention. Two, that is a conservative estimate. Because when we looked later, content could have been taken down by individuals or the entire accounts taken down by one of these platforms for their violations without us having any part to do with it. So 35 percent is the absolutely high watermark of actions that could have been taken based upon our referrals.

Q Okay. So it's potentially an overestimation actually?

A It's almost certainly an overestimation. It's the best we could do for our research.

Q Okay. So just to make this real clear, there were around 600 tickets total. Correct?

A That's correct, yes.

Q And of that, some small subset was flagged for social media companies because of either threats to life and safety, fraud, or concerns about violating the company's platforms or policies?

A Yeah. So if you look on page 37: "Of the 639 tickets," it says, "363 of them tagged an external partner to either report the content, provide situational awareness, or suggest a possible need for fact checking or a counter-narrative."

So if you look at the next page you can see which one of them were actually tagged to a platform. So this would not count when we said -- say, sent something to EI-ISAC around, hey, you might want to tell Maryland to go do a blog post, or here's an FYI for Kentucky. So the upper bound would be 363, but then you could see on this table on 38 the details of that.

Q So it was actually less than 3 -- it was actually probably --

A Yeah. We would have to go slice the numbers in a different way, but yes.

Q Right. But it's actually less than 363 tickets total?

A That's right. That's the absolute high watermark, yeah.

Q And of the 363, even assuming that was the universe, which is probably -- that's probably more, in 65 percent of the cases, the social media companies did nothing?

A That's right.

Q Okay. All right. Moving away from the Jira tickets.

A I'm sure we'll come back.

[2:33 p.m.]

BY [redacted]:

Q Are you familiar with allegations or criticisms suggesting that EIP engaged in censorship?

A Yes.

Q What's your response to those criticisms?

A We did not engage in censorship. EIP had no power to take down content or even have it labeled. And that was neither our goal nor the outcome from us doing our work.

Q Some activists have claimed that SIO cajoled or pressured social media companies to take certain actions. Are you familiar with those allegations?

A Yes, I have seen those allegations.

Q And are those allegations accurate?

A No.

Q Okay. And can you explain that?

A We would send URLs to platforms we thought they clearly violated the policies. If you look into the tickets themselves, there was not a "take this down or else" or a demand. I'm not sure how we would demand. We're an academic research project. We have no coercive power in any way. All we could do is refer these to them and then document the outcomes of what was going on in the election.

Q And, just by way of example, how many people total were involved in the EIP?

A A little over 100, I believe.

Q How many employees does Facebook have, if you know?

A Over I think 60,000.

Q Okay. So EIP is kind of a small fish? Right?

A All of EIP is smaller than just the team I supervised at Facebook, yes.

Q Thank you for that context.

Did EIP have a blacklist of accounts that it had -- that it kept track of?

A No, absolutely not.

Q Do you at SIO keep a blacklist of accounts?

A No.

Q Mr. Shellenberger, who we talked about in the first hour, he stated that SIO published a report urging news media to abandon the Pentagon Papers ethic and instead focus on the perpetrators of the hack and leak rather than its contents. Is that accurate?

A That's not.

Q Okay. Do you have any idea where that allegation came from?

A So two different people at Stanford, Andy Grotto and Janine Zacharia, wrote a white paper about how to handle hacker leaks. They are not part of SIO. They had no role in EIP. Stanford has something like 17,000 or 18,000 staff members. And so I am neither the former Secretary of State nor an Olympic swimmer obviously. And so I think he was just -- automatically assumed that anybody from Stanford that he could ascribe that their writings to us, that would be incorrect. And those people have nothing to with EIP in any way.

Q And I actually should have asked this much earlier, how many people are employed by SIO?

A Currently? So, if you count the post docs who are technically employees but are kind of pseudo students, I think we have seven or eight full-time employees.

Q Okay. And Stanford has about how many employees total?

A I think around 17,000 to 19,000.

Q So there's probably a lot of work being done at Stanford that SIO is not involved in. Is that fair to say?

A There's a couple of things happening on campus that they don't ask me about, yes.

Q Okay. There have been allegations that EIPs were targeting Conservative political speech. Are you familiar with those allegations?

A I am.

Q Are those allegations accurate?

A No.

Q Could you explain?

A Our goal going into the election was to have an apolitical set of standards around rumors, disinformation and misinformation about the functioning of the election. That could have come from either side. The outcome was asymmetrical, but that is clearly because one side lost and one candidate pushed his followers to believe that it had been stolen. And so I think that's a natural conclusion. But our conclusion, if you look at our statistics around Conservative versus Progressive, which I think people get this idea or the list of the top super spreaders, all of that is part of our academic research, our analysis after the fact. Going in, we tried to be as careful as possible. And, in fact, in 2022, we were pretty prepared for the possibility that lots of this content would be coming from both sides because there were candidates in the election who had a history of election denial --

Q Okay?

A -- from the Democratic side as well.

Q And I want to get back to what your research found in just a sound. But, before we do that, when EIP was founded in July 2020, did you reach out to potential partners in both the right leaning and left leaning spheres?

A We did.

[redacted]. I want to introduce as exhibit 14 an email dated July 21, 2020.

[Stamos Exhibit No. 14
Was marked for identification.]

BY [redacted]:

Q This was actually produced by the University of Washington in their production.

A Okay.

Q And it's part of a chain that began at the calendar invite dated July 30th, 202, but we're only going to look at the top email. I introduced the whole chain for clarity.

This email was sent by [redacted]?

A Yes.

Q And that's a Stanford student. Right?

A That's right.

Q It's dated July 31st, 2020, time-stamped 14:30:39. It says: Hello all. Thank you for joining us in yesterday's meeting. Please find this week's Next Steps below. Also copied into our Minutes Document at the top of today's notes section and our Slack #general.

And then it says: 7/30 EIP Workflows Sync Next Steps. We'll look at number one.

It says: Number one, meetings on the calendar for next week: 8/3 -- so August 3 -- NASS/NASED -- that's the National Association of State Election Directors?

A Yeah. National Association of Secretaries of State and the National Association of State Election Directors.

Q And that's what we talked about earlier; it is kind of a trade association for election --

A Right. That's the collection of all the people who run elections at the State level.

Q Okay. Common Cause, Twitter. On 8/4, which August 4. ASD, which is -- what's ASD?

A I believe this ASD -- I'm not sure actually. I'd have to look this up one.

Q Okay. CIS, DNC -- that's the Democratic National Committee. Right?

A That's correct.

Q And then it says RNC. That's the Republican National Committee? Right?

A Yes.

Q So is it fair to say that EIP met with the RNC almost as soon as the project was underway?

A We reached out to them. I'm not sure who it was -- who actually took the meeting with them. I don't think I was part of that meeting. But we did offer to them the ability for them to send in anything that they saw.

Q And did the RNC take you up on that offer?

A I don't believe they ended up sending us anything.

Q Okay. Did they not agree to join the -- to join your effort, or is it they didn't send you anything?

A So, for these kinds of partners, they didn't really have to join anything. We just offered them: Here's an email address, that if you see anything, you can send it in.

Q Okay. But you certainly made them aware of what you were doing?

A Yes.

Q And, as far as you know, this meeting actually did take place?

A I don't recall. I remember very distinctly sending the initial introduction email to the general counsel's office.

Q At the Republican National Committee?

A At the RNC, yes.

Q Okay. Do you know approximately when you sent that email?

A No, but we can look into that.

Q So you said a couple seconds ago that you were very careful with how you approached this project in part because you were mindful of the concerns about bias. Do you recall saying that?

A Yes. I think that's a paraphrase, but yes.

Q It's definitely a paraphrase. We can't ask the court reporter to read back in this setting, but --

A Because that slows everything down incredibly.

Q But you agree that, when you undertook this project, you had in mind the fact that research needs to be clean. Right? As clean as possible. It has to be -- you have to address concerns about bias?

A Right. I mean, the output here would not be acceptable to us or pass peer review if the work we did was biased politically.

Q Are there particular steps that can be taken to account for the risk of bias during the research process?

A So we had guidelines of -- for the students, as well as we did training to make sure that they were fairly applying what our standards were for scope. So I think that's where the most likely bias would creep in, would be in a situation where on that initial decision of "oh, I see something," is it actually in scope or not, if they had some feeling of "oh, a complaint from a Democrat is legit, but a complaint from a Republican is not." So we tried to make sure that, in those initial steps, they were accurately recording the things that they saw.

Q Okay. And when you were -- after December 2020, when you were going through and looking at the data that you had collected, did you take any particular steps as you were analyzing that data to account for the potential bias?

A Well, so we had standard -- you know, a big thing you do in this kind of post hoc data analysis is labeling, where this horrible, horrible job of just going through and for all the pieces of data applying fair labels. And so we had standards for that. In fact, we then did what's called intercoder reliability. So we had multiple people code all of this data. So this is a standard part of social science research, so it's H251. So we published the reliability scores where we tracked from multiple different people doing this work how much differentiation there were in their results.

Q Okay. So there's particular actual research steps that you took, and I'm sorry; what is it called multi --

A Intercoder reliability.

Q Intercoder reliability. There's particular research steps that you take to try and make sure the data is as accurate as possible. Is that fair to say?

A That's fair to say, yes.

Q Okay. And, actually, during the actual process of gathering the data, so July to December 2020, you actually did identify and report on misleading claims spreading through left-wing -- left-leaning audiences as well as right-leaning audiences. Correct?

A That's correct, yes.

Q So, for example, you reported on misinformation concerning Postmaster

General Louis DeJoy. Do you remember that?

A That's right. I believe we did a blog post on that.

Q And what was that misinformation, if you recall?

A There was a lot of concerns by Democrats that changes to how the post office was handling vote by mail were specifically meant to disenfranchise Democrats.

Q And were those claims accurate?

A I don't believe they were. And I believe we wrote it up as demonstrated there was no evidence behind those claims.

Q Okay. And then, skipping ahead into the 2022 election, EIP actually analyzed six networks of fake accounts attempting to influence midterm elections and determined that they were acting ways that were generally pushed toward Progressive causes. Right?

A That's correct. Those were networks that were run by Iranian and Chinese groups that were one very Progressive, kind of Democratic Socialist, Bernie-type content, Medicare for All and such. And then were particularly attacking Republicans. In one example, there was an entire Floridians against Rubio group where all the Floridians were actually Chinese -- not of Chinese descent living in Florida, sorry; people working for the People's Republic of China.

Q So, in the 2022 election you actually assessed that there was a -- foreign actors were acting on behalf of Progressive causes. Is that fair to say?

A Yeah, in both 2020 and 2022. So, in 2020, the most important foreign influence campaign was an attempt by the Iranians to convince Americans that the Proud Boys were stealing the election from President Trump. This actually came to us via a tip from the NAACP. I believe it's the only thing they sent to us, was they -- members of the NAACP, kind of prominent Black leaders, were getting death threats in email, and so they -- saying, "We are from the Proud Boys" -- and then sent it to us. And I believe the folks in the NAACP really thought it was the Proud Boys. So we asked them to send us the technical details, and then those linked to a video. And the video showed a desktop of somebody as they purportedly broke into the election systems of Alaska, downloaded data, and then used a somewhat obscure mail-in ballot generation system that's meant for overseas servicemembers that they scripted up creating hundreds of thousands of fake votes in Alaska to try to swing the election, all of them for Trump. And then specifically I think they had a Proud Boys background. And the whole thing was set I remember to Metallica's "Enter Sandman." So the first indication is that no, like, actual White supremacist group would use anything off of the Metallica "Black" album as the sellout album of Metallica as their theme. Second, there were technical indicators so we actually could tell from both the emails. And then we paused the video, and there was a moment where they forgot to redact part of it. And, instead of attacking systems in Alaska, it was actually a virtual private server in Moldova where they had set up a fake website for the Alaska State Secretary of State's Office. So, looking at the Moldova stuff and such, we could tell this is almost certainly a foreign actor, and there are death threats involved. So this is a situation where, you know, we did our normal EI-ISAC process, but we also directly sent it to the FBI all of our results. And then, 2 days later, I'm not going to take any credit for this -- I'm sure lots of people in the government were working -- but I believe the Director of the FBI and other core leaders went on the dais in the White House and said: We have detected foreign interference from Iranians trying to blame President Trump.

So, yes, the most interesting foreign campaign in 2020 was actually directed at trying to make it look like the Proud Boys were throwing the election to President Trump.

Q Is that documented in your report?

A Yes. And we wrote a whole blog post about it.

Q So, notwithstanding that, at the end of the day, you said a couple of minutes ago that you did identify the most super spreaders, I guess, or the most -- the most -- actually withdraw that.

Is it fair to say that, in 2020, EIP did ultimately identify more misinformation or information spreading among right-leaning audiences than among left-leaning audiences?

A Right. When we did our analysis, while there was disinformation among left-wing analysis, the more right-wing content and the right-wing accounts were much more effective and had a larger spread in virality of their content.

Q And did your research explain why it was that more disinformation was spreading through the more right-leaning accounts?

A I mean, I think the obvious example is that President Trump lost. And, therefore, he was the one who denied the election. You're not going to have -- well, let me take that back. There is a small but very dedicated set of Democrats who believe that the 2020 election -- that President Biden won legitimately but that the Republicans winning House seats was fake. That they really believe that there's some kind of bizarre conspiracy where they forgot to rig it for Donald Trump, but they did rig it for local House races. And so there are people like that, but it's a much less widespread belief. And I think the base thing is that President Trump lost, and he's the one who told his followers "it was stolen from me." So, therefore, most of the excitement is going to be there. If the other side won, then there's no reason to think that, you know, that --that it was thrown.

Q Do you think, if outcome had been reversed, that Donald Trump had won and Joe Biden had lost, do you think you might have seen trends in the other direction?

A I think you would have seen trends in the other direction. I don't think there's any indication that a losing President -- Vice President Biden would have been as aggressive. But certainly I think it's a possibility. If you look -- the specific example I think about from the Democratic side is Representative Stacey Abrams, who was very aggressive in 2018 of saying it was stolen. In fact, that's something we were looking out for in 2022 when she ran again. In the end, there wasn't a lot of content, probably because she lost by a big margin so it just looked silly. But certainly I think -- and this is actually my biggest fear as an American is that we'll get into a place that whoever loses always thinks it was stolen from them.

Q Thank you. We can go off the record.

[Recess.]

BY [redacted]:

Q Mr. Stamos, I wanted to touch back on topic we discussed in maybe in both hours, but certainly the first one. With respect to your tenure at Facebook, when you had the meeting you described with Mr. Zuckerberg, Ms. Bickert, and a few others high up in the company --

A Uh-huh.

Q -- was it one meeting or a series of meetings, if you recall?

A There was one big meeting where I presented our results. And then there was a series of meetings to figure out what to do about it, using I think generally a small -- so I think there's only two meetings with Mark Zuckerberg in that initial set and then a smaller group broke off to try to figure out what we were going to do and to structure the investigation of what we were going to.

Q And, during your tenure with Facebook, how frequently would you meet with Mr. Zuckerberg?

A Not very. I'd probably be in a meeting with him two to three times a month. We almost never met one on one during my time there.

Q And you said it was kind of well understood within the company that people are upset with Facebook on the 2016 election?

A Yes.

Q And did it seem it was more heavily weighted by one side of the political aisle than others -- than the other?

A I mean, it was pretty clear that Democrats were more angry at the company, yeah.

Q And can you just say a bit more, what is it that, to your understanding, the Democrats believed Facebook did wrong?

A So, you know, things changed, but initially, after the election, a lot of blame was put on fake news of just any kind of content that was fake being on the platform. And then, later, especially after we made our announcements, the assumption was that a significant amount of the anti-Clinton content was Russian.

Q Okay. And you left Facebook -- do you remember which month in 2018?

A I believe August.

Q So just a few months before the U.S. 2022 -- U.S. 2018 midterms?

A That's correct.

Q And, in the lead up to those midterms, do you recall there being concern within the company regarding whether a similar dynamic could play out as it had in 2016?

A We were certainly concerned about there being some kind of manipulation of the election, and it happened in a platform, which was why at that point we had built a team to deal with it and we were taking those meetings, as I discussed, with both other companies, as well as with the relevant government players.

Q Okay. With respect to the steps the government was taking, if I understood your answer correctly with the criticism, it seems two parties at least. Right?

Mr. Bellinger. Can I just say we are now at over 5 hours. What he did at Facebook a number of years ago is not relevant to your investigation. You had said we would really try to get out after 4 hours. So I would really like to try to keep this focused on the parts that are relevant to the committee's inquiry.

[redacted]. We are happy to turn right back to the questioning. We will complete it, and there will be other topics as well.

BY [redacted]:

Q It sounded like there were two parts to your answer: the fake news concern, which sounded content-based, that whatever is being posted is not true, and then the fact that some of it allegedly came from Russia so that would be actor based. Is that a fair understanding?

A That's right. And then, on the latter, on the Russia, that would also be behavior based since I think the assumption was they were not saying they were Russians.

Q And, again, to your recollection, the pressure, the concerns, the awareness of the political backlash that the company was facing, that was still present when you the left the company in 2018. Is that right?

A Yes.

Q With the understanding that you weren't at the company, but you said you remained in contact with colleagues and maybe friends at Facebook, do you know if that was still present in 2020 -- that feeling?

Mr. Bellinger. Again, this is really not relevant to --

[redacted]. The witness has the opportunity to answer.

Mr. Bellinger. He can answer if he thinks it's relevant.

Mr. Stamos. So, yeah, I mean, this has nothing to do with EIP, but certainly, by 2020, we were still in what we people called the tech lash, which is kind of an attack, you know, political actors attacking the platforms for a variety of different things, but including concern of foreign interference in elections and fake news and disinformation overall.

BY [redacted]:

Q And, to the extent you have a knowledge or understanding of this, is it your understanding that Twitter and Facebook both took action to moderate the Hunter Biden laptop story the day it was issued?

A So my understanding -- and all of this comes from public reporting and what I observed. So I have no special insight here. But yes, my understanding is, in both those platforms, put some kind of limit on the story. I believe Twitter banned The New York Post URL so you couldn't post the story at all. Facebook, it's my understanding, did some kind of limitation on spread so that you could post it, but they were not recommending it or it wasn't being highly ranked and that both those companies then removed those within a day or 2.

Q And, in your opinion, if absent this tech lash, to use the term you were using, do you think the companies would have taken the same content moderation steps that they chose to?

A Specifically around Hunter Biden?

Q Yes?

A I don't know. I think -- so my position is I -- I don't -- I think they made mistakes in doing that. There were two parts to the Russian interference in 2016, as we talked about. There was the hacking leak campaign by the GRU, and there was the activity that was right on the platforms. And the companies responded to both of those things. But the truth is on the hacking leak campaign, there's not much you can do as a platform because the real target there is trying to get the media to cover stories based upon hacked data, which was very effective by the GRU in 2016. And so I am not sure -- it's impossible to imagine what was going on different, but I do believe they made a mistake in that having policies that make them act in a situation where the content is not being posted first under the platform really means that they are so disconnected that there's no way they can make a reasonable determination of whether something was hacked.

Q And why do you think the companies adopted the content moderation policies they did with respect to hack and leak?

A Because it was a real big part of the Russian campaign in 2016. From my perspective, it probably was the more effective part of the Russian campaign. You know, they very effectively changed the tenor of the conversation in the last couple of months of the campaign to be about Hillary Clinton's email server and stuff like that. So I think they were reacting to that. And the feeling that they were being held responsible, I'm sure that's part of it. But, from my perspective, the appropriate thing for them to be responsible for is the content that is posted directly on their platform where they have some kind of knowledge. So it's different to me; if The New York Post posts something, it's up for The New York Post to authenticate whether they got the data from a Russian actor or something. If somebody creates an account and posts on Facebook, it's Facebook's responsibility to make sure that person isn't lying about who they are.

Q We had talked in the first hour about malinformation and the difficulties with that term?

A Yeah.

Q Again, to your understanding, do you recall any Federal Government agencies that would use the term "malinformation"?

A I -- there's an acronym around MDM for mis-, dis-, and malinformation. And so I believe DHS has used the MDM, and maybe some other government agencies have picked up on that.

Q And then CISA, which you identified as falling within DHS, do you recall if CISA has ever used the MDM --

A I --

Q -- term?

A I believe that was the name of the subcommittee in CSAC, the Cybersecurity Advisory Council, that was looking at this issue, is they called it the MDM Subcommittee.

Q To your understanding, what did the MDM Subcommittee look at?

A They were talking about CISA's role in issues involving mis- and disinformation.

Q And what does the second M stand for in MDM?

A Malinformation.

Q Again, understanding that you don't prefer the term, what is your understanding of what CISA meant by malinformation?

A My general standing is that malinformation is supposed to involve any information that could be used to weaponize, to cause harm.

Q And, to the extent you have an understanding, what is encapsulated under CISA's understanding about malinformation that is not already encapsulated by this information?

A I honestly don't know. The term is used by different people. I've never seen like a good definition. So I'd rather not speculate as to whoever at CISA used the term of what they meant by that, you know.

Q When you -- you mentioned that you do work with Dr. Kate Starbird. When you engage with one another, does your work ever concern malinformation?

A So, I mean, if you use malinformation as kind of an umbrella term, then yes, all of our work on EIP and the like you could count it as malinformation. Again, I would not use that, but if you had to use it, then yes, our conversations would be -- include techniques that include malinformation.

Q But would you use the term malinformation, or is that disfavored by the academics you're familiar with?

A Some people use it. I'm just saying I don't like it because I don't think there's a good definition in the way we have definitions for mis- and dis-.

[redacted]. Exhibit 15.

[Stamos Exhibit No. 15
Was marked for identification.]

BY [redacted]:

Q If I could have you flip to the last two pages, Bates No. 159 and 160, there appears to be an email sent from @2020partnership.atlassian.net, and there is reference to an EIP ticket number. To you understanding, is this consistent with an email notification that would be generated by the Jira ticketing system?

A Yes.

Q And then, if I could have you read the email at the top of Bates No. 159. There's an email -- you are not copied on this email chain, but there's an email that says -- the second sentence says: Evidently Director Krebs personally reached out to Stamos asking what happened around this event, around the time the content was taken down, which is only an hour after this ticket was created.

Do you recall if Chris Krebs reached out to you regarding various EIP events?

A I don't recall this situation, of him reaching out in this situation.

Q How would Chris Krebs know that an event was being monitored by EIP?

A So, in this case, it looks like the EIP ticket was forwarded to [redacted] here who probably showed it to him. Although Krebs is not on this exchange so somebody probably showed it to him, or there is another thread.

Q So, to your understanding, was Chris Krebs potentially receiving email notifications from the EIP?

A He should not have been receiving direct notifications, but somebody could have forwarded it to him. It looks like [redacted] might have forwarded this to people within CISA.

Q Do you know how frequently that occurred?

A I don't.

Q The email address has got an atlassian.net email domain. So, if [redacted] is forwarding it, is she forwarding it from the Jira system?

A Yes, she could have put -- she could have put him in there to get straight from Jira. That's what this looks like or -- yes.

Q And by "him," are you referring to [redacted]?

A [redacted], yes.

Q So could individuals be added to the Jira system how does [redacted] receive an email notification that [redacted] is in the Jira system?

A He would had to have been added to the ticket.

Q And he has a -- if you look an email above his email address is cisa.dhs.gov. It's your understanding that's the email domain address for CISA?

A Yes.

Q Now, when an individual is added to Jira, do you put in the email address, or is it -- do they have to accept a notification in advance before they can be forwarded the --

A I'm not sure exactly what the initial notification would be, whether you just get the ticket or whether you'd have to accept it.

Q Do you know who might know that information?

A Sir, you're talking about, like, specific generic configurations that don't exist anymore because we haven't used this system in 3 years.

Q So your answer is no one would have this information?

A I'm not sure we'd have the ability to recreate exactly what the configuration was at that time.

Q Do you recall forwarding Jira tickets to anybody during your operation of EIP in 2020?

A It's possible. I don't remember forwarding anything, but it's possible.

Q Independent of EIP, in the fall of 2020, how frequently were you in communication with Director Krebs?

A We probably texted every couple of weeks.

Q And did you have other professional interactions, other than EIP during the fall of 2020?

A With anybody or with him?

Q I'm sorry. With Director Krebs?

A I don't recall all the ways in which we interacted in the fall of 2020.

Q Are there any that you recall?

A So there were events, election security events, that we probably ran into each other.

Q Was there any --

A It's possible he came to calls in which we were briefing people. I'm not sure.

Q When you say "we were briefing people," are you referring to EIP?

A Yes.

Q And are you referring to, for example, briefs you provided to external stakeholders?

A So we did regular briefings on the things that were trending or that we saw happening. And so most of those were public, but, occasionally, I think we did private ones for folks like EI-ISAC and such.

Q Do you recall how many private briefings you had with EI-ISAC?

A No.

Q When you say it was with EI-ISAC, the individuals who were representing the EI-ISAC, are they employees of CIS?

A It should have been. It's possible that we sent things for them to forward to their membership. I don't recall our entire schedule of what we did that fall.

Q What form would these briefings typically take? Would it be in person, over Zoom?

A Probably Zoom. It was COVID; nobody was meeting in person.

Q In advance of a briefing, would there be an agenda circulated?

A I don't think so. There's probably just a calendar invite.

Q After a meeting, were meeting minutes ever circulated?

A Not that I know of, no.

Q Do you have any recollection of Director Krebs asking to attend one of these briefings?

A I don't recall what interactions we had in the fall of 2020. So he might have asked, he might not. If we put out something to the EI-ISAC, he might have gotten something forwarded to him. He might have attended; he might not have. I'm not sure.

Q [redacted] email references that Director Krebs reached out around the time the content was taken down, which was only an hour after this ticket was created: If the system is to work, we will need the turnaround time to be much faster for sending these tickets out to States.

What is your understanding of what the, quote/unquote, turnaround time for a typical ticket?

A So I think in this he's talking to the folks at CIS. So it says: If the system is to work, we'll need the turnaround time to be much faster for sending these tickets out to States. So I think what he's saying is that the delay between us seeing this content and labeling in this EI-ISAC and then the speed at which then that went to California in this case was too slow.

Q Okay. So the system here is the EI-ISAC he is referring to, not EIP?

A Yes, because, one, we are not on this thread. It is Aaron Wilson and Mike Garcia from CIS are the people he's emailing. So I think he is talking about EI-ISAC's. If we say: Hey, send this to California, that it should be faster for that to go straight to California.

Q Would EI-ISAC send that to California only after EIP had conducted its analysis?

A So we'd have to go look at this ticket to see exactly how it started, but since this is not how -- it does not look like this is a ticket that came from CIS. This would have been us finding something and then tagging in EI-ISAC, saying something along the lines of: You should probably notify Sonoma County.

Q We can take these back.

[redacted]. Exhibit 16.

[Stamos Exhibit No. 16
Was marked for identification.]

BY [redacted]:

Q Is this email consistent with the Jira notification we saw on the previous email chain, different EIP ticket but --

A This looks like the kind of notification that we would get from Jira.

Q Okay. And is it [redacted], is that -- am I reading -- saying her name correctly?

A Yes.

Q On the front line?

A Yes.

Q And she's with Stanford and with EIP. Is that right?

A That's right.

Q Okay. I will have you take a look at below where it says: View request and turn off this request's notifications.

It says: This is shared with TikTok, Facebook, EI-ISAC, Twitter, CIS misinformation reporting and CISA CFITF. Identified earlier in the spreadsheet, it's your understanding that CIS misinformation reporting versus EI-ISAC. Is that right?

A I believe so, yes.

Q What is your understanding of what CISA CFITF refers to?

A I don't know. I believe FITF is Foreign Influence Task Force. I'm not sure what the C stands for.

Q Okay. Was the Foreign Influence Task Force housed within CISA?

A I am not sure. I believe -- I thought the Foreign Influence Task Force was between different departments.

Q To your understanding, what entity was represented by CISA CFITF in the Jira system?

A I have no knowledge of what that is outside of what you just handed to me.

Q Is there a way to determine who was represented by CISA CFITF through the archived data or other means?

A We'd have to look to see whether there is an entry in the ticket that refers to them that makes it clear. I'm not sure the -- again, this is almost 3 years ago. So we don't have the kind of metadata configuration of the database anymore.

Q To your understanding, if a ticket was shared with an entity that's listed here, that would be an entity that could see public comments on a ticket. Is that right?

A That was the intention of the public versus private, yeah.

Q Okay. So, whichever entity is CISA CFITF, if consistent with the understanding, is likely able to see comments on this ticket. Is that correct?

A They should be able to see the public comments our people put in there.

Q And would they be able to see public comments by other entities that are tagged there, such as Facebook and Twitter?

A As we discussed, I'm not totally sure. We'd have to look to see -- yeah, I'm not sure. We'd have to try to figure out from looking at the tickets if there's any interaction between them.

Q Is there anyone else at Stanford that would have this information?

A We can go ask folks. I can ask around and see if anybody understands, if they remember exactly what was available in different public comments -- or of which kind of public comments were available to outside entities.

Q At a high level, are you familiar with what was redacted in the spreadsheet that was produced to the committee?

A Yes, I believe student names and -- was a key thing and the private comments that were only internal to EIP.

Q And I think we discussed this earlier, but, based off the spreadsheet, there's no readily identifiable way to determine if a comment is private or public based off the column heading?

A No, we had to figure it out based upon context.

Q And by "we," do you mean Stanford?

A I worked with our attorneys to try to figure that out.

Q And what was the rationale behind redacting the private comments?

A Because those are internal work product for an academic research project for which we have a pretty well established First Amendment right to do that research and to share publicly. We did not believe that was relevant to the legitimate investigative position of this committee, which is to look into the actions of the executive branch. And so we shared the things that could have been seen by outsiders, including platforms or EI-ISAC or whomever EI-ISAC forwarded things on to.

Q But, in determining whether a comment was viewed, was able to be viewed by an external stakeholder, there was no readily identifiable way in the archived data. You had to review the comment and make a determination? Is that right?

A Yes. And it's generally pretty clear because it almost always starts with the name of the organization, because the way you would tag an organization in is you would do like an @ symbol and put their name. So that would be the normal way in which you might want to make a comment available to somebody. You say @ -- when you see in there, it says, like, Twitter, Facebook, Reddit, I think it's most likely it is them saying @Twitter, @Facebook, which would automatically add them to the ticket and then have it sent on to them, which would then -- those are the organizations you see in the organization column.

Q Are there any -- to your recollection, were there any comments that you determined to be public that did not begin with the organization names?

A So certainly things that look like responses would be public. They would have to be public because they would come from those orgs so those were included.

Q Do you recall if there were any comments that you were unsure about, whether private or public comment?

A I sat with the attorney and worked through the ones that were ambiguous, and we did the best we could to try to determine that.

Q Does this document refresh your recollection at all regarding whether the entity that is CISA CFITF have the ability to submit tickets?

A I don't know of any situation in which they were able to submit tickets if -- not -- unless it was through EI-ISAC.

Q Do you have a sense, just a ball park figure of how many different individuals or entities a Jira ticket was shared with?

A So we don't have to ball park that; we have data on that.

Q Well, let me ask you this: So there is data in the report. To use the previous exhibit, where it looked like the Atlassian email address was [redacted] forwarding a ticket to [redacted], an individual.

A Right.

Q Is that captured by the report as in terms of the number of individuals who may have received any EIP ticket?

A I don't believe so, no.

Q Do you have a sense of how many people that might be?

A No, I do not.

Q The internal or private comments as you've referred to them, does that include only student comments, or is that -- was that comments that include, for instance, the managers as well but do not include external stakeholders that?

A That would include the managers. So, if a student asked a manager for "what do you think we should do here" or "what do you think of X," then the response to them would be a private comment in the ticket.

Q And, to your understanding, is there anything in the spreadsheet or the archive data that you have that produces some sort of record of when a Jira ticket is forwarded?

A So, if an organization is added, then they end up in that organization column. If it was forwarded to an individual, I have not seen anything in there that would indicate that. So it would have to be in the individual's inbox. They would probably have an email notification; it would be the only record we'd have.

Q Do you have any sort of access to that Atlassian email domain? That would seem like an automatic generator system, the one that's -- when an EIP ticket is forwarded to someone outside the system like I saw in the previous exhibit, to your knowledge, does Stanford have any access to that email address?

A So the email address is supposed to represent things that come in and out of the database. So anything sent in should end up with a ticket in the database. And things that go out are representative of the configs you put -- of what you put in into Jira. So, beyond what has been turned over, I don't think so, no.

Q You mentioned texting with Director Krebs. When communicating with him as part of your role at Stanford, what other forms of communication would you use?

A So I know we had some emails and probably text iMessage or Signal.

Q Was anyone else from Stanford in touch with Director Krebs with respect to EIP?

A It's possible. I don't know.

Q In setting up EIP, did you have conversations ever with Atlassian, the company that runs the Jira service ticket?

A Yes, we sent them emails because they had an academic discount rate. And so we asked to get the kind of academic package so we didn't have to pay like we were a big company.

Q And were you in touch with them at all when you decided to end the project after the 2020 election?

A I don't recall. I think generally at that point what we did is we archived the data, and then we started reconfiguring it for a Virality Project. I don't think we had to talk to them about that, but it's possible that somebody at Stanford had some interactions with them.

Q And was there a 2022 version of EIP?

A Yes.

Q And what were some of the differences between the 2022 version and the 2020?

A So it was much smaller. It was a smaller group with fewer shifts. It was midterms. We thought it would probably be less active, and that was accurate. There was no equivalent to the EI-ISAC relationship so we did not have tips coming from that the local and State governments. And we made no referrals to platforms. So it was -- it was more of just gathering what we found. We posted blog posts, and we're finishing up the final report.

Q Did you use the Jira ticketing system again?

A Yes.

Q And, when you use the system and you're jumping into it in 2022 as the election is leading up, is it the same system you used in 2020, or is it a new one?

A So these are new databases every time that we start from scratch.

Q And then, with respect to retention of those records, did you follow a similar approach with 2022 as you did in 2020?

A I would have to ask the team. I expect we've exported them, and we do all the work in Excel.

Q To your understanding, could you go back to the original database with the tickets?

A No.

Q Why not?

A Once we exported it and then we replace the database with the new ones so we can do the VP work.

Q So did you overwrite it or --

A I believe -- so we have licenses that we are given as part of the contract, and there are a number of seats that we have, and there's only a certain number of databases you're allowed to run. So I believe we downloaded it, deleted it, and created a new one to do our next work.

Q Was CISA involved with the Virality Project to your recollection?

A It's possible that they were one of the recipients of our output, but they were not kind of the core recipients because -- you know, vaccine issues aren't core to the mandate.

Q Who were the core recipients?

A So I believe there's Office of the Surgeon General, Health and Human Services, and State and local health officials who signed up for our notifications.

Q Who from the Surgeon General's Office did you work most closely with?

A I -- I don't recall who that was. I -- I was not part of most of those conversations.

Q Who at Stanford was most involved with the Virality Project?

A So [redacted] did a lot of work there, but the key person was an undergraduate student, [redacted] was -- and a couple other people -- of students who worked on doing a lot of the interaction because we had had a pretty smooth -- had gone to a pretty good smooth operational place by the end of EIP. EVP was more student run that is EIP was.

Q With VP, was there a similar manager role that existed with EIP?

A It was a much more simplified structure because the volume was much smaller so I don't -- I don't recall the exact structure there. And, again, well -- I was helping provide feedback to VP; I was not the one who was running it on a day-to-day basis. I was less involved than I was with EIP.

Q Were social media companies still receiving Jira tickets as a part of the Virality Project?

A Yes. So they could subscribe to different narrative types. So the goal of the Virality Project was quite different in that we knew with these vaccines being brandnew that what was true and what was false was going to be a much harder thing to determine than some of these election situations, which were very, very easy to know. Right? It's easy to know that you can't vote twice and then undo your vote. Right?

That was the example it was before. And so one of the differences with Virality Project is that the narratives that were found would be put into categories of different kinds of things that then the companies could subscribe to. And so they would get updates based upon this is what is going viral in these areas, not tied to whether or not it was about their platform or their policies of just like this is what people are discussing in this area. And, in some cases, that was pro-vaccine, and sometimes it was antivaccine. It was effectively like a clipping service for what was the most viral things being discussed on social media related to the vaccines.

Q Would you or would the Virality Project when sending a Jira ticket to a company send for instance to Twitter a series of tweets on topic?

A So we'd have to look at the specific tickets. But generally I think it was, like: Here's a description of what's being said.

And it would include: Here are tweets. Here are Facebook posts. Here is Reddit posts. Here's a YouTube video.

Q And obviously the relationship with social media companies dates back to the predecessor EIP. Is that right?

A And, for some of these companies, as I said, we had a preexisting relationship before that in our collaboration on foreign influence. But yes, for -- most of these companies were part of the EIP. And so they -- yeah, they already had that relationship, although it was sometimes it was different people at the companies because election security and health misinformation are sometimes different people at these companies.

Q Was there an understanding that the social media companies might consider taking down some of the specific pieces of content that were being flagged by the Jira tickets?

A So that was up to them. And most of the time, just as with elections, the response the companies had was to tag people and to push people into their own vaccine information centers.

Q So, again, with the understanding that EIP and Virality Project don't have the power to directly label or remove a piece of content, was the understanding that sending these Jira tickets may result in that?

A The understanding is we were telling them what was the thing that people were talking about. In a situation in which there was a narrative that was clearly false or clearly overblown or not based upon any fact, then it's possible that they might have taken actions under the new policies. In general, the platform policies on vaccine misinformation had a lighter touch than on the election, partially because of this issue that everybody was dealing with that nobody knew exactly what the truth was at the time. So what they did with the information we sent was completely up to them.

[3:35 p.m.]

BY [redacted]:

Q So, turning back to EIP, you know, we walked through the value and the benefit of your team's analysis and the report you issued later. What was the intention with adding in social media platforms as external stakeholders?

A For EIP?

Q For EIP.

A So, as we said, we wanted them to be aware if there was content that was violating their policies. And one of the things that we had the ability to do is, if a local official told us something, especially something that directly lied to individuals about how to vote or the mechanisms of voting or had a life-safety issue, then we felt it was our responsibility to help address that, not just document it.

Q Okay. And "by help address that," do you mean share it with the social media companies?

A When we shared it with them, then they could take the steps that they thought were appropriate based upon what we shared.

Q Okay. Would you send information to the social media companies if you didn't think action was needed?

A I believe there are tickets where they're added and it just says: You should know that this is something that is going big. You might want to watch.

So, you know, if you had -- if you had a narrative that looked like it might go viral or, "Hey, we don't know if this is true or not, but you should keep an eye on it," then perhaps it's the kind of thing we would have basically been cc'ing them for their knowledge, and I think there are a couple tickets that effectively say that.

For the most part though, we really should have -- you know, the goal was to only refer stuff to them if we knew it violative of their policies. So that means they might have labeled it. They might have taken it down.

Again, 65 percent of the time, they did nothing, and we knew that we had no power to make them do anything, and that, you know -- especially once we got the project going, that they would have to make their own determinations, and most of the time, they determined not to take any steps.

Q When you were briefing CISA in the summer of 2020 or maybe into the fall of 2020 and outlining what your intentions are with EIP, did you include, as part of your discussions with CISA, that you would be onboarding external stakeholders, including social media companies?

A We probably told them, yes, that we would have the social media companies, that we'd be able to refer things to them.

Q Okay. You said a couple times in different ways that EIP didn't have any power. Would EIP ever note that it -- either on Twitter or elsewhere -- that it had flagged a piece of content for a company?

A So, I mean, it's possible, like, in our blogposts where we're analyzing things, we might have said something along the lines of, we sent this to platforms. I'd have to go look to see exactly what we said.

Q And we touched upon earlier that, following the 2016 election, at least some of the major platforms were under criticism for not doing enough with respect to fake news and with respect to foreign influence?

A Yes. I mean, I would say Facebook got 95 percent of that, and 5 percent was distributed among the other platforms.

Q Okay. And, based off your earlier answers, it sounded like there was a particular sensitivity and awareness within Facebook -- and maybe these other companies but to a lesser degree -- of the pushback -- political pushback for not taking enough steps. Is that right?

A It was on TV every day. So it was definitely understood by people that we were being blamed, yeah.

Q And is it fair to say that the company wanted to avoid being blamed again in the future?

A So I think there were individuals who were really sensitive to that. I think the company overall did not want people to lose trust in the platform.

If you go on Facebook and you believe that all the people you're talking to are trolls, are fake accounts, are Macedonian teenagers, then that, in the long run, really lowers the value.

So -- and Facebook is a company that is very much driven by money and metrics. And so would individuals feel like "I don't like to be blamed for something"? Absolutely. But, in the end, most of these decisions are made based upon, like, hard, metric-driven discussions, and certainly metrics around the trust in the platform were going down during that period of time.

Q Do you recall who at Facebook in -- we'll say 2016 to 2018 -- was most sensitive to the political backlash that was occurring?

A So, I mean, the people who were dealing with it every day would be Elliot Schrage and Joel Kaplan in their roles of running the government affairs team. Probably of the senior leadership, the person who cared the most about this stuff was Sheryl Sandberg.

Q And, with respect to the blogpost, are there any -- did anyone from EIP ever communicate to the platforms that you were going to make these blogposts public?

A I mean, it's possible that we gave them a heads-up when we were posting about it.

Q And why would you do that?

A I think it's a polite thing to do so that they know that we're going public. We didn't want them to feel like we were blindsiding them.

Q And what do you mean by "blindsiding" them?

A We wanted them to know that there's going to be a possible discussion of what was going on in their platform, and they should know about it.

I think the -- you know, we were -- I am sympathetic to how hard it is to be in one of these companies and to try to balance all the different equities. And so, if somebody was writing something that could generate a communications moment during an election period, then that's something I would want to know for sure.

Q What do you mean by "communications moment"?

A So, if we wrote a blogpost that said, "This is something viral that's happening that's not true," you very well could find members of the media going out and then finding that content on five different platforms and then writing about it being up or not.

Q And, if it was still up, would some of those media publications be criticism of the platforms?

A It's possible.

Q And so, if EIP has the power to flag this content and produce a blogpost, does EIP have any sort of ability to incentivize the platforms to take down the content?

A No more than anybody else who has the ability to write a blog.

The companies were criticized constantly by both sides. They received letters from Members of Congress on both sides. They received -- according to what I've seen in the hearings -- emails from President Trump's office about content moderation.

So, compared to people who have actual coercive power such as Members of Congress or members of the executive branch, I think us saying "here's a narrative that's going viral" -- whether or not we mention the specific platforms where it's going viral -- is the exact same ability every American has, and especially -- and ours would be less than a celebrity or somebody with a massive following.

So, no, I don't think you would say we have any more coercive power than anybody else who has the ability to criticize platforms in our democracy.

Q You mentioned in contrasting your role in Stanford with the executive branch at Congress and the coercive role and coercive powers they have --

A Yeah.

Q What do you mean by the coercive powers that Congress and the White House have?

A In that Congress has the ability to punish companies through passing legislation, making their lives hard through subpoenas, which I know are always given out for true investigative purposes and not to punish people for their First Amendment speech. And certainly the White House has all kinds of levers in which they can try to make life hard for a company.

Q And, with respect to the coercive powers that Congress and the White House have, when you were talking earlier about the tech lash that Facebook was concerned about in 2016 and -- 2018, is part of that concern the coercive powers that Congress and the White House have, to use your terms, punish companies?

A Yeah. I mean, I think there was, in that period and for several years after I left Facebook, a real fear of significant regulation coming out of Congress. It turns out that fear was misplaced. Nothing substantive has happened since the 2016 election in this area or in any area of content moderation in the U.S. The E.U. is a different story.

But, yes, I am sure that they were worried, which is why each one of you has met probably 10 Facebook lobbyists over the last 6 months and that they have such an aggressive government affairs shop. Is that they do not want to get regulated.

Q Okay. And, when talking about this tech lash and the public criticism and the concern of significant regulation, in an earlier answer, you said it tended to be heavily from the Democratic side of the aisle. Is that correct?

A That was true at the time, and now it seems to have swapped, where a lot of this criticism is coming from Republicans about the same decisions but from the other side. Decisions that the Democrats thought were not sufficient are seen as overreaching or suppression of free speech by the Republican side.

So it is an interesting thing to observe, the tech lash going back and forth that -- effectively, the exact same arguments are being made by -- I saw a funny moment where Elizabeth Warren, I think, was retweeted by Ted Cruz. And that was kind of shocking of -- like, they're both making the same arguments of tech companies bad, but they both had a very different idea of why. And so it does seem to be moving back to the Republican side.

Q In 2018, when you were still at Facebook and Facebook is adding the CIB policy, at that point in time, the tech lash and all that was coming from the Democratic side, is your understanding. Is that right?

A Yeah. I mean, I think there was a lot more negativity towards Facebook from Democrats in the 2018 -- sorry. That would be 2017. In the 2017 timeframe.

Q Okay. And the concern -- when you say "significant regulation," to connect the two answers together, significant regulation coming from being pushed by the Democratic side of the aisle?

A I mean, at the time, I believe most of the regulation was being proposed by

Democrats, although there has been lots of regulation proposed by Republicans, too.

In the last couple years, now, a lot of that seems to have moved to the States. That all the really -- I'll say interesting, but I also mean unconstitutional -- things are being pushed by State legislatures.

Q And this kind of public criticism from the Democratic side of the aisle, to your understanding, that still persisted up until the 2020 election. Is that correct?

A I think it persists until today. I mean, I think there's -- there's criticism of the platforms for lots of things.

The feeling inside the companies is that, if you're a platform that has a couple hundred million Americans, you're going to end up reflecting all of the good and bad of America. But then people end up blaming the intermediary for carrying the speech that they both like and they dislike.

So, even today, Democrats are still submitting bills, as you guys know, to regulate the companies. On the Democratic side, it seems more about privacy and a lot of stuff around antitrust.

Q Okay. Is your understanding that the approaches to antitrust would be harmful to companies like Facebook?

A I mean, something aggressive like breaking the company up would certainly be -- they would consider that harmful, yeah.

Q Do you remember any discussions like that when you were still at Facebook?

A I wasn't involved in any of the antitrust stuff. That's outside of the realm of a CSO.

Q With the understanding it was outside of the realm, do you recall any discussions that arose in meetings or conversations with colleagues?

A I mean, I don't recall any discussions about, like, antitrust strategy or anything. They would never include me in that. Certainly -- yeah -- noises different administrations make around antitrust are being noticed by everybody at the company.

Q In an earlier answer, you were comparing Stanford and EIP and contrasting that with the coercive powers of the executive branch and Congress.

It is true, though, that certain members of the executive branch were at least engaging with EIP. Is that fair to say?

A So certainly we were engaging with members of the executive branch in a way that we thought was appropriate and that, my understanding, they had signed off on -- that they had gotten approval of by a Trump administration lawyer, by attorneys at the Department of Homeland Security.

But, yes, we were engaging with them. Of course, we were engaging with the parts of the government that have very little power. CISA actually has no regulatory capability. They don't have law enforcement capability. I believe they recently got administrative subpoena capability to do things like unmask IP addresses.

But that's actually, I think, one of the good things about CISA, is that for a long period of time, as a CSO, there was nobody in the government that you could work with defensively who couldn't also put you in jail.

And so it's like, you can't have a casual chat with an FBI agent when you're an executive at a company. It's not safe. You end up with a $3,000-an-hour row of people sitting next to you.

And so the invention of CISA, I think, was a positive thing because it is an organization that does not have regulatory or punitive law enforcement capability.

Q And what do you mean you can't have a casual conversation with the FBI? Why is that?

A I think defense attorneys would tell you that FBI agents are always looking out -- you might feel like you're having a friendly conversation with them, but you never know if you're actually the target.

And I think there has been a number of situations which companies have tried to engage the FBI because they were victims of, say, a cybercrime, and then they end up getting punished or their executives getting punished.

There is actually -- this was a big deal over the last couple of years where the CSO of Uber, who was my predecessor at Facebook, was prosecuted for doing some things that I don't agree with, but I understand how he got there. And it was kind of shocking because he was working directly with the FBI in situations where they had aligned law enforcement, and then DOJ turned around them like that.

And so, you know, dealing with a law enforcement agency that has coercive powers is just a risky thing to do if you're part of some big organization and some other -- there might be some investigation involving the organization that you don't even know about.

Q That perspective you just shared with respect to the FBI, do you think it was widely shared by the executives at Facebook when you were at the company?

A Certainly the policy of the company was that an executive could not talk to the FBI without attorneys present.

Q Okay. And, with respect to the Uber example you gave, did that -- was that example well known among industry partners?

A Sorry. That was just very recent. So that has been over the last, like, year and a half. That's from well after I left Facebook.

Q Okay. Do you recall any other similar examples like the Uber one?

A I'm sure I could look. But I think a number of people were concerned that you can end up going and having a conversation with the FBI and end up getting yourself into some trouble in a way that was not expected. So, generally, at companies, executives are required to take attorneys with them for those kinds of meetings.

Q Okay. And, to use the Uber example as one, even if the government represents that the interests are aligned, it could be the case that, later on, the government changes its mind. Is that right?

A Yes.

Q Okay. And this fact is well known by tech executives?

A Yes. And I think all executives of all public companies understand that there's lots of parts of the government that can punish you for activity that you thought was appropriate.

Q And that's regardless of what the government may have said. Is that right?

A Yeah. Yes. I mean, I think the determination of any individual U.S. attorney is disconnected from whatever the overall policy of the government happens to be.

Q Okay. In addition to the FBI, there are elements of DHS -- or I shouldn't say in addition to. FBI is in DOJ.

Are there elements of DHS separate from CISA that have coercive power?

A Over companies in particular?

Q Yes.

A I mean, clearly, if you're an immigrant, DHS is very important.

I mean, the only thing I could think of would be his, Homeland Security Investigations. A number of companies work closely with them because they have a long history of doing child safety investigations. They are actually probably the most important Federal law enforcement agency on child safety due to the history of -- if people are bringing child pornography into the U.S., it used to be you did that in magazines and photos in a suitcase. And so the investigations of smuggling raids across the physical border used to be the core of child safety investigations.

And so his is still, like, a big part of that, and that's probably the agency in which we work the most. I don't think anybody is really afraid of them. Like, you don't hear about them doing investigations of companies in the same way the FBI does.

Q Okay. Are you aware of any other similar types of partnerships that had multiple executive agencies working with them to monitor elections?

A Of partnerships --

Q So you represented EIP as a, you know, blogpost, which is accurate in a certain sense. You were producing blogposts. But you also partnered with multiple government agencies.

Are you familiar with any other types of blogposts or partnerships that had a similar set of relationships with the executive branch?

A So I don't think that's an accurate summation of what I represented EIP. EIP was an academic research program that documented and studied what happened in the 2020 election. We happened to then get tips from EI-ISAC and the GEC.

To call them partners -- you can use the word "partners," but in the end, they were sending us information, and we sent them information based upon our knowledge and our analysis of activities.

I am not aware of any other groups that were working with them like that, but it's -- I wouldn't be shocked, if you look at the NASSes or the NASEDs and the other kinds of organizations that do election security, that there's some kind of relationship with both CISA and the FBI.

Q Okay. Are you familiar with anywhere there is both large social media companies, such as Facebook and Twitter, on the same communication with Federal agencies such as CISA?

A Well, I think those companies interact with CISA probably all the time.

Q Are there any blogposts to help facilitate this?

A Are there any -- are there any academic research projects to help facilitate it? I don't know of any at this time, no.

[redacted]. Okay. All right.

Can we go off the record, please?

[Recess.]

[redacted]. It's 4:01. Let's go back on the record.

BY [redacted]:

Q There was a -- Mr. Stamos, there was a comment made in the last hour about SIO and EIP being a blog. Is that accurate?

A No.

Q Okay. They're research entities, right?

A The EIP is a research partnership. It's not actually a legal entity. It was a partnership between four institutions with a history of doing research into -- especially foreign interference into U.S. politics.

We had a blog, but we were much more than a blog. We were a group that created, I think, the most complete historical record of disinformation during the 2020 election, and I think the most interesting academic research that has been published both in our final report and in multiple peer-reviewed journals since then.

Q Okay. And you did -- you said you did have a blog, though?

A Yes.

Q And I think you were questioned about that a little bit.

Did you sometimes write the blogposts?

A I contributed. I don't think there's any blogpost that I wrote totally by myself, but I contributed to a number of them.

Q Is writing a blogpost an expression of your First Amendment rights?

A I believe so, yes.

Q Okay. And so there was an allegation made that, somehow, by the act of writing a blogpost, you are acting in a coercive manner. Do you remember that allegation?

A I do.

Q Is it fair to say that that's effectively suggesting you should be punished for exercising your First Amendment rights?

A That does sound like what he was saying, yes.

Q Okay. There was a lot of discussion about Facebook's internal reaction and concern about the political fallout -- let's call it -- after 2016?

A That's right.

Q Russia did, in fact, interfere in the Presidential election in 2016, correct?

A That's correct.

Q And it did so by manipulating the Facebook platform, correct?

A Among other things, yes.

Q Okay. Does Facebook have a vested interest in ensuring that nobody manipulates its platform, Russia or otherwise?

A Yes. Keeping the platform free of foreign interference, I think, is a key part of them keeping up the trustworthiness metrics that eventually lead to people wanting to use the platform and therefore them making money.

Q Okay. You were also asked in the earlier hour about the Hunter Biden laptop story. Do you recall those questions?

A I do.

Q Okay. Do you know -- and I know you didn't work on the specific -- this issue yourself, but just from public reports, how long was the Hunter Biden laptop story banned on Twitter?

A I think it was a matter of hours, but I don't remember exactly.

Q Okay. If I represent to you that it was 24 hours, would you agree with me?

A That sounds correct.

Q Okay. And what about Facebook, do you know how long it was -- how long Facebook --

A Probably about the same amount. It was never banned on Facebook, but I believe it was downranked for a day or less.

Q Okay. In the -- much earlier -- I think maybe it was the first hour of the day with the majority's questioning -- you were asked if the 2016 Russian election activity -- the Russian interference in 2016 had actually impacted the election, and you said you thought it was actually pretty hard to assess what impact it had. Do you recall that?

A I do.

Q Okay. Do you think it's possible to assess the impact of the 24-hour ban on the Hunter Biden laptop story on the 2020 election?

A On the actual outcome?

Q Uh-huh.

A I expect it was quite low because I think, in the end, the bans the companies put together created what we call the Streisand effect, that it ended up getting way more coverage than otherwise. I expect if you polled Americans, that a huge percentage of them know that Hunter Biden had a laptop with all kinds of nasty stuff on it.

So I expect it actually went the other way, that the blocks were probably beneficial to President Trump or at least not good for Joe Biden.

Q Okay. I want to turn back to exhibit 15, which is the email involving [redacted] [redacted]. It's EIP 243.

"Re: EIP 243. Claim the thousands of ballots found in dumpster in Sonoma."

A Sorry. I gave my copy back.

Mr. Bellinger. Here you go.

Mr. Stamos. Okay. I'll just use this one.

BY [redacted]:

Q Okay. And there was a question about whether the -- whether CISA had been added on to this ticket.

This is actually an email, right? It's not a ticket?

A This is an email that came from the ticketing system.

Q Right. So it was -- but it's not the ticket itself. It's just an email that perhaps attached the data from the ticket, but it didn't allow CISA access to the ticket itself, right?

A Right. So CISA did not have the ability to come and just look at tickets. But, if somebody -- like, in this case, it looks like she put in this person specifically to get it forwarded to him.

Q Are you familiar with the Sonoma County ballot dumpster story?

A I am.

Q And can you briefly describe what that is?

A This is something we wrote up in -- on our blog. There was a true report -- a photo of a dumpster in Sonoma County with all of these mail-in ballots. And the claim that was made was this was a demonstration of pro-Trump votes being thrown out.

It turns out they were real ballots, but they were ballots from the last election. And Sonoma County did something really stupid, which is -- instead of shredding those ballots, as they probably should have, and disposing of them securely, they just dumped them into a dumpster.

And so -- yeah. The claim was that these were being thrown away, and they were voting for Trump, but even if you looked at the photo -- if you zoomed in enough, you could see it was the California ballot design from the election before.

Q Okay. And so the claim that the ballots were current -- that they were ballots from 2020 that had been thrown out was just flat-out false, correct?

A That's right. And this was something we saw a lot of and we continue to see a lot of, is that you have a kernel of truth. Here are ballots in the dumpster. And it makes people feel -- oh, I see a photo. I'm doing my own research. I'm learning for myself. And then they accept the framing around it, which is these are this year's ballots, and these are Trump ballots being thrown out.

And so using that kernel of truth allows you to drive a story -- a narrative that's not true.

[redacted]. And I want to introduce as exhibit 17 the actual ticket from this.

[Stamos Exhibit No. 17
Was marked for identification.]

BY [redacted]:

Q This is from the Excel spreadsheet.

A Okay.

Q And this is -- I'll tell you, it's stapled on the wrong side, so you want to hold it like that. There you go.

And I'm hoping you can quickly turn -- sorry. Not quickly. Take as long as you need. The column labeled "reach." It is on the --

A I see it.

Q Yep. It says this is "viral, 1,001-plus engagements." Do you see where it says that?

A I see that, yes.

Q So this demonstrably false claim was among -- it was in the highest category of spread, correct?

A That was in the top category, yes.

Q Okay. And I'm going to ask you to turn to -- if I can find it -- the column that has the organizations listed.

So it's on -- it's labeled -- what's that -- the third-to-last page. Do you see where it says "organizations"?

A I do.

Q And the organizations listed there are EI-ISAC, Facebook, Reddit, and Twitter. Do you see where it says that?

A I do.

Q CISA is not listed there, correct?

A That's correct.

Q Okay. So CISA was not an organization that was brought in on this ticket?

A What he showed me before is it looks like an individual person had been added for it to be forwarded out of the platform.

Q Right.

A But CISA is not added because CISA themselves did not have direct access to the ticket.

Q Okay.

[redacted]. And now I want to turn to the other example they used, which is exhibit No. 16. It's the DeKalb County.

And I want to introduce the actual ticket for this one, which is going to be exhibit 18. And, again, this is stapled on the wrong side.

[Stamos Exhibit No. 18
Was marked for identification.]

BY [redacted]:

Q Okay. And I'm going to read quickly the description of what this was. It is in tiny, tiny font, so if you can't follow along, let me know, but --

A Most of my body is falling apart, but my eyes are actually okay. So I'm fine. Thank you.

Q So it says -- underneath description, it says: Can you help with this tweet? A person describing himself as an Emory professor says DeKalb County has rejected 40,000 absentee ballots. DeKalb has only rejected 240 ballots so far. Only slightly more than 1,400 have been rejected statewide. His tweet is totally false but is still getting pick-up -- and then there's links to the URLs -- any help you can provide? Ari Schaffer, director of communications, Georgia secretary of state.

Did I read that right?

A Yes.

Q Okay. So is it fair to say that this ticket involved a claim about the number of absentee ballots that had been rejected, and the secretary of state of Georgia -- somebody from that office said this is demonstrably false?

A Yes.

Q And the Secretary of State's office would be in a position to know if that was true or false, correct?

A Correct.

Q Okay. And I want you to turn to the "organizations" page for this one as well. I think it's probably near the end. Yeah. It's the last page.

And the organizations listed there are EI-ISAC, Facebook, TikTok, and Twitter. Do you see where it says that?

A That's correct.

Q Okay. And, again, CISA is not listed as one of those organizations, correct?

A That's correct.

Q Okay. So CISA, again, was not brought in on this ticket?

A Unless somebody forwarded it to them.

Q Right.

A They did not have direct access.

Q Right. And they wouldn't have been able to edit the ticket or contact social media companies through the ticket?

A They certainly could not have done those things, no.

Q Okay. Okay. There's a -- sorry. Real fast.

There was a comment made earlier about social media companies being onboarded to the platform. What's your understanding of what the term "onboarded" means?

A Onboarded would mean we would set up their accounts in Atlassian and then probably provide them some basic training of what was going to be happening, how they could access the tickets, what kind of notifications they would get, stuff like that.

Q Okay. So they were onboarded in that they had access to the platform, but that was really it, right?

A Yes. That meant they had a login that they could see the stuff that we put in front of them.

Q Okay. A couple questions about the Virality Project.

SIO created the Virality Project in 2021, correct?

A Yes.

Q Okay. And the purpose of the Virality Project -- actually, let's go ahead and introduce -- I want to introduce as exhibit 18 -- no. I think we're on 19, actually.

It's an SIO blogpost entitled "Launching the SIO Virality Project."

[Stamos Exhibit No. 19
Was marked for identification.]

BY [redacted]:

Q Are you familiar with this post?

A This looks like our initial post, yes.

Q So, on the second page of the post as printed, the first full paragraph on that page at the end --

A Okay. I'm sorry. So there are two things that we call the Virality Project, just to be clear. So our first launch was SIO only, which is what you're seeing here. This is from before the vaccines happened.

Q Okay.

A We were doing our own study of disinformation around the virus itself, right? So this is May. So things are getting hot.

Q Okay.

A So, for example, I actually brought a blogpost from it. We did a whole study of -- from this first version of the Virality Project, we did -- maybe I don't have it. We did a study of Chinese lies about the -- or, like, what Chinese social media was doing --

Q Okay.

A -- and what the Chinese Foreign Ministry was saying around the origin of the virus and Chinese responsibility for it.

Q Okay.

A Yeah. So this is the paper that came out from that. So that was the first version --

Q Okay.

A And then we effectively relaunched it. And we had the name, and we had the domain, so we reused it --

Q Okay.

A -- of relaunching it with the partners specifically around the vaccine.

Q Okay. So let's put this exhibit to the side.

A Yeah.

Q Because this is not actually what I want to talk about.

A Yeah.

Q The relaunched version. I think there was some muddle earlier in what the purpose of that relaunch version was. Could you just state again your understanding of what the purpose was with respect to the Virality Project, the second iteration of it?

A Right. So we -- just like with EIP, our primary purpose was to archive in real time the discussions that were happening around the vaccines. We knew this was going to be an incredibly important historical moment for the whole world and, as a result, would probably be the target of serious disinformation.

At this point, we had already, like I said, seen, for example, the Chinese doing lots of foreign influence work around the world, both trying to -- trying to push blame for the virus onto the U.S. and things like that.

The second was to then do an academic study of how -- how do people discuss these things in a rapidly moving scientific environment? So, as I said before, the difference between this and the election is that a lie about when the election is, is easily fact-checked. Saying a vaccine causes a side effect is something that is much harder to know whether that's true or not, or there might be a kernel of truth, but then somebody says: That's why you shouldn't take it, or everybody is going to get the side effect, right?

And so studying how that stuff worked online was a big goal.

And then the third was to provide health officials with a view of what was being said because we wanted them to be responsive to the actual concerns of citizens and not just do the normal doctor thing, which is to lecture at length, you know, in a very scientific way, like: This is what people are afraid of. This is what you should address.

Q Okay. There was discussion earlier about the Virality Project -- I'm going to call it VP for shorthand -- the VP's output.

A Yes.

Q What was the VP's output?

A So the primary output was the weekly reports. We did these weekly briefings that we sent to a mailing list, which included public health officials, companies, I think some kind of nonprofits -- NGOs who do public health work -- and then we posted those on the public website. We also then would send -- between those updates around the narratives we were tracking -- to platforms that subscribed to those specific narratives.

Q Okay. And that was just one-directional, right? Like, you would create the update, and you would hit "send," and it would go out into the world?

A That's right, yes.

Q Okay. So it wasn't like there was back-and-forth engagement with the platforms on those?

A Right. This was different than EIP in that we didn't have the back-and-forth engagement, nor did we have an EI-ISAC equivalent where you had somebody routing stuff to us from local and State officials.

Q Okay. So is it fair to say that you were summarizing the results of your research or whatever the research had been that week, writing it down, and sending it? Is that a fair summary?

A Yes.

Q Okay. That was also an exercise of your First Amendment rights, correct?

A I believe so, yes.

Q Okay. Did the Virality Project receive any Federal funding?

A No, it did not.

Q Okay. And that's true for both the 2020 iteration of the Virality Project and the 2021 iteration of the Virality Project?

A That's correct. We didn't get any of the NSF grant, which is our sole government funding, until after both of those projects were over.

Q Okay. Matt Taibbi has claimed that the VP had the capacity to take in 50 million tweets a day. Is that accurate?

A So what he's referring to -- I saw that tweet. He released a leaked email from inside of Twitter where Twitter had sent us an email saying: Hey, here's an API in which you can get COVID information. There's over 50 million tweets a day about COVID-19.

So that was an advertisement of Twitter saying: There's 50 million tweets a day. You can access it via APIs.

Q And what's an API?

A I'm sorry. Application programming interface, which in the end, we didn't have to use because we already had an integration with their general API that would allow us to look at the things we cared about, which was actually much tighter than all of COVID-19. So he had, like, a basic misunderstanding of what that email said.

Q And, just to be clear, an API is essentially a tool that Twitter created. Is that a good way to put it?

A An API is effectively a way you can talk to Twitter. So it's how Twitter on your phone talks to Twitter, is via an API.

Q Okay. It's a Twitter product?

A It's a Twitter product, yes.

Q Okay. Mr. Shellenberger has reported that the VP, quote, censored 66 different social media narratives. Is that accurate?

A No.

Q Do you know where that -- do you know why he would think that?

A So, first off, we censored nothing. We had no power to do any censorship. And I think he's going in that -- we identified in our final report -- we categorized what we found into different kinds of narratives, and I think we might have had 66 narrative archetypes.

To say we censored those things is absolutely incorrect because the whole point is that we saw those things on social media. We had -- those narratives are still going on. And our goal was to document: These are the things people were saying about vaccines. Some true; some false. Here are the 66 different categories that we put them into.

So we did no censorship at all. And the idea that we censored those things is just empirically wrong because you can look at social media today or you could look at it during that project and you would see plenty of discussion on all those areas.

Q And one last claim. Mr. Taibbi has claimed that the VP recommended that platforms take action against true vaccine side effects or posts that would fuel vaccine hesitancy. Is that true?

A No. So, in that case -- in that tweet where he makes that claim, he took a subset of an email, which students sent -- the student leaders of the project sent an email out to all of the platforms saying: Which of these narratives would you like to be updated on and get updates on?

They did not say you should then take them all down. And, clearly, they didn't because if you look at all of those platforms, all of those things we talked about happened a lot.

But we do do study of what kinds of tropes exist, what are the common narratives around vaccines, and that is something that we shared with the platforms, as I believe we have a constitutionally-protected right to do.

Q Okay. And you said that, to your knowledge, those are still actually available on social media today?

A I think if you opened it up right now, you would find plenty -- you could find an example of all 66 of those different kinds of narratives on social media, yes.

Q Okay. Okay. A handful of wrap-up questions.

Are you -- are you familiar with an individual named Renee DiResta?

A Yes.

Q Who is Renee DiResta?

A She's my colleague at Stanford. She's our research director.

Q How long have you known her?

A How long have I known Renee? That's a good question. I probably met her in the 2017 timeframe at a conference or something like that. Yeah. I don't remember exactly when I met her. I've worked side by side with her since 2019. So I've known her well since we hired her at SIO.

Q And you would say you know her well?

A Now, yes.

Q Okay. Are you familiar with an individual named Mike Benz?

A I very much am, yes.

Q Who is Mr. Benz?

A Mr. Benz is a gentleman who has been writing a lot of things about us that are not true. I believe he used to work at the State Department for a short period of time on cyber. And he likes to tweet about us and publish things and seems to be the person who is pushing a lot of these theories to the various committees and such.

Q Okay. I want to focus on one particular thing that he said about Ms. DiResta.

Mike Benz has publicly accused Ms. DiResta of being a CIA spy embedded at the SIO to help the government engage in censorship. And I know there's a lot to unpack there, so let's take it piece by piece.

Is Ms. DiResta a CIA spy, to the best of your knowledge?

A To the best of my knowledge, she is not a spy for the CIA.

Q To the best of your knowledge, did the CIA embed Ms. DiResta at the SIO?

A No. I offered her a job, and she accepted.

Q Okay. Does the SIO engage in censorship?

A No.

Q Okay. So it cannot be the case that -- so Ms. DiResta is, first of all, not a CIA spy?

A Right. So I think where this comes from is Renee was on her own in her family at a very young age and had to pay for college herself and ended up getting a National Security Fellowship that sent her to an internship at the CIA, which then paid for her to go through school.

I'm pretty sure she has not had any relationship with the CIA or been a spy for them or anything. And I think at the time, she was, you know, an undergrad, so she was probably just an analyst sitting at a desk somewhere in Langley. So I'm pretty sure she has had no official relationship with the CIA since then.

Q Are you familiar with the impact that this rumor has had on Ms. DiResta?

A Yes. Unfortunately, yes.

Q Are you able to speak to that at all?

A Renee has come under really extreme personal attacks over the last several months. I have too, but, unfortunately, as you often see online, this thing becomes gendered. So she probably gets five times as much hate mail as I do. I know she has gotten death threats and threats to her children.

Q And Mr. Benz has also tweeted about you. Is that right?

A I believe he has, yeah.

[redacted]. I want to introduce just one of these tweets.

[Stamos Exhibit No. 20
Was marked for identification.]

BY [redacted]:

Q It was actually from 4 a.m. this morning, so you might not have seen it.

A Oh, I probably did not.

Q And I'll give you a second to read it, and let me know when you're ready to continue.

A Okay.

Q Okay. I'll just read it quickly.

Mr. Benz, who tweets @MikeBenzCyber, tweeted: Interesting. December -- Dec -- 2019 was when Chris Krebs flew to Stanford for a meeting with Alex Stamos to discuss election censorship for 2020 election. Krebs' CISA then tapped Stamos' EIP to censor trending narratives. Wonder if Krebs was briefed by FBI on damning Hunter laptop first.

And I should say, this follows a comment from an individual named Sean Davis about the Hunter Biden laptop.

A Right.

Q And this was tweeted at 3:58 a.m., on June 23rd, 2023. I want to take this apart piece by piece.

Did Mr. Krebs fly to Stanford in December 2019?

A I don't recall. Chris visited and spoke to students and participated in a job fair to recruit students to the new CISA. I don't remember exactly when that was.

Q Okay. At any point in December 2019, to the best of your recollection, did you and Mr. Krebs discuss election censorship?

A No.

Q Did you discuss the Election Integrity Partnership?

A No. At that time, it did not exist.

Q Okay. And that was actually about 7 months before it would get underway, correct?

A That's right.

Q So that was well before it was really a thought?

A Yeah. It was not until early in 2020 that we started our internal discussions about what we were going to do about the election, and we didn't really pull the EIP together until June of 2020.

Q Okay. And then this continues: Krebs' CISA then tapped Stamos' EIP to censor trending narratives.

Did CISA tap or ask the EIP to censor anything?

A No.

Q With respect to the 2020 election or otherwise?

A No.

Q Okay. And we talked through the Hunter Biden laptop earlier. Just to restate, EIP had nothing to do with the Hunter Biden laptop story, correct?

A That's right. We published nothing on that. We had no tickets on it. It was completely out of scope because it was about a candidate's kid. About whether you would vote for a candidate had nothing to do with the actual mechanism of the election.

Q Okay. So is it fair to say that this particular tweet from Mr. Benz is entirely false?

A He spelled my name correctly. But, other than that, it's pretty much entirely false, yes.

Q Okay. Thank you.

A And it's unfortunate. I guess he's not a very good sleeper since he's tweeting about me at 4 a.m. That's unfortunate.

Q So Mr. Benz, Mr. Taibbi, and Mr. Shellenberger, and others have placed you in the public eye because of your work -- or not because of your work, but because of misrepresentations about what you do. Is that fair to say?

A I mean, they have certainly misrepresented what we do, yes.

Q Okay. And we talked through the consequences that this has had on

Ms. DiResta.

Have you also faced negative consequences because of what's been happening with the way you've been -- your work has been misrepresented?

A I think you could say that, yes.

Q What impact has this had on you?

A So there have been a number of threats against me and my family. The most disturbing was actually a very subtle one. I got a Twitter DM that the only thing in the DM was an extremely blown-up crop of my wife's face from a family photo, which I'm pretty sure the implication was not, "Boy, your wife is pretty. Why are you with somebody so beautiful?" That this was a threat against her life, the way it was portrayed.

It was pretty smart because it was both very scary and also exactly the kind of thing for which the context to try to represent to Twitter that this is really a threat against my family is quite hard.

So, yes, there has been lots of people lying about me. And, unfortunately, this is something that now, if you Google for my name, there's plenty of accusations that are totally incorrect. So I expect that this will have a long-term negative impact on my career.

Q And why a long-term negative impact on your career?

A Because we've tried very hard to do good academic work that is not politically-biased. And I've never wanted to be seen as a political actor. And, for some people, that's what they want. They want to be seen, and they want jobs where they're particularly partisan.

And, since I will most likely one day have to go back in industry, being seen as, like, a political player who is hated by half the country will be a real challenge for me. You know, if somebody googles me for my background and what they find is lies after lies after lies, it's going to make for -- much more difficult, especially if I was going for, like, a chief security officer role again.

Q Do you think the fact that you've been facing these kind of threats and the fact that you've been brought into this investigation for that matter -- might that have a chilling effect on your willingness to do this kind of research in the future?

A Absolutely.

Q In what way?

A Because it makes you really wonder whether it's worth it, right? In the end, my primary responsibility is to my wife and my three children, and it's very hard to justify for them -- even if it's unfair, for them to be put at any kind of physical risk because I want to do academic research into the election.

Q Do you think if other researchers or other academics are seeing what's happening to you, it might chill their willingness to do this type of research?

A Oh, I'm sure it is having that effect. Both this investigation and what is going on publicly, I expect that it is discouraging a number of universities from studying what happens in 2024.

[redacted]. All right. Oh, sorry. Before we end, I did want to enter your written statement -- the written version of your statement into the record. This will be exhibit 21. And it's just to have the complete record made.

[Stamos Exhibit No. 21
Was marked for identification.]

[redacted]. Thank you. We can go off the record.

[Recess.]

[redacted]. Back on the record, please.

Do you guys still have the exhibits? One was introduced by the minority in the previous hour. It was the spreadsheet of EIP 833. And then, in my previous round of questioning, there was an email with the same EIP 833 number.

Mr. Bellinger. Yep.

BY [redacted]:

Q Okay. If you were to flip to the second-to-last page of the re-creation of the spreadsheet row, there are two columns, one "organizations," one "platform."

A Yeah, I see that.

Q And there's reference to EI-ISAC, Facebook, TikTok, Twitter. And under "platform," it's Facebook, Instagram, TikTok, and Georgia Twitter. On the --

A If I may.

Q Yeah.

A The Georgia is in the State-targeted column.

Q Oh, okay.

A So it just looks like when it's printed here, but it's in the State column.

Q Thank you for clarifying.

So the "platform" reads Facebook, Instagram, TikTok, Twitter?

A That's right.

Q And then, in the exhibit that I introduced in the majority's previous hour of questioning, it says that the ticket had been shared with TikTok, Facebook, EI-ISAC, Twitter, CIS misinformation reporting, and CISA CFITF.

For the email, I'll represent that this was produced to the committee by one of the tech companies listed below. When the tech company receives this, they're able to see that both CIS Misinformation Reporting and CISA CFITF received a ticket. Is that right?

A If this is what you said, this went to the company -- if that's true, then yes.

Q Okay. Do you know why CIS Misinformation Reporting and CISA CFITF are not appearing in the archive data?

A So CIS Misinformation Reporting shows up as the creator. So I think what you're seeing here is that EI-ISAC is the organization that the humans are logged into, and CIS Misinformation Reporting is perhaps an automation system we are using to turn their emailed reports into an entity. So it is -- that part is listed here.

Q Okay. And what about CISA CFITF?

A Yeah. I don't know why that's listed here. It's perhaps that it was individually forwarded or they were cc'd, but that they were added specifically to this ticket. I'm not sure.

Q Okay. And, to your understanding, how could CISA be specifically added to this ticket?

A I'm not sure.

Q Could a government entity -- if it was not the creator and if it's not one of the social media platforms, is there a mechanism by which not just a government entity but other entities could be copied on or added to a ticket?

A I believe you could always put individual emails so that they get forwarded something.

Q Okay. So it might be the case that CISA CFITF is a personal email?

A It could be that that is the name of an email that has -- as it's represented in the Atlassian system, that if you put the email of an individual person the at CISA, it shows up as CISA CFITF. I'm not sure.

Q Okay. If you were the recipient of the -- I don't know which exhibit number this is, but the Bates No. is 1934, and the bottom of the email says, "This was shared with," and it lists a bunch of entities including CISA CFITF -- would you be under the impression that this information had been shared with CISA?

A It's possible, yes.

Q Okay. This is going back to just --

A And, to be clear, this was our work of information that we filled out and our analysis. So that's what they would have seen in the public component. But, in the email, that's what they would see, yes.

Q Okay. Would they see if this was submitted by EI-ISAC?

A So you can tell that from -- it says the CIS mis-. So what they would probably see when they looked in is it would say CIS Misinformation Reporting because that's what the reporter was set for the EI-ISAC tickets.

Q Okay. So the tech company would realize CIS created the ticket, and when it's being shared, it's being shared with major social media platforms and CISA. That's what this email represents. Is that right?

A That's what they could infer from this, yeah.

Q Okay. When -- I want to make sure I use the right term. Whether it's onboarding or engaging with the social media platforms, who was your primary point of contact at Meta in 2020?

A The person who supervised the most important team here would be Nathaniel Gleicher.

Q Do you recall any other names from Meta?

A I know a lot of people who work at Meta.

Q Sorry. In the context of engaging with EIP in 2020.

A Probably David Agranovich. He helped lead a bunch of investigations. Olga Belogolova. I'm not sure who else would have -- we would have engaged with directly or who were the people we onboarded on the platform.

In the end, I'm pretty sure the people who were doing this was not any of those three, but whoever was on-call in the trust and safety team that was handling the election at the time.

Q Do you recall if Neil Potts from Meta was involved with EIP in 2020?

A It's possible. I don't recall any actual conversations with him, but it's possible.

Q Did you have any regular points of contact with Facebook's or Meta's trust and safety team in 2020?

A So all of those people work on integrity. Of the team that is actually doing operations -- I should probably have said is probably what's called community operations, which is the team that would take a report from us and then make the decision of what to do with it. And I'm sure we onboarded one of those people, but I wasn't part of that process of onboarding them.

Q Who at EIP was part of the process of onboarding the social media platforms?

A I don't recall exactly who did that one, but I believe [redacted] and some of the other students did most of those onboardings and trainings.

Q Who from Alphabet did EIP engage with in 2020?

A So I think the key person was Clement Wolf, who I believe was kind of the point of contact for policy engagement.

Q Were there any other names you recall?

A That's the only one at this point.

Q In 2020, who was EIP's primary point of contact with Twitter?

A Probably Yoel Roth and Nick Pickles.

Q In 2020, who was EIP's primary point of contact with TikTok?

A The person who ran the team was Eric Hahn, who I believe recently left. I'm not sure who the actual person who might have been looking at the output, but Eric would be kind of the primary person that we interacted with.

[4:42 p.m.]

BY [redacted]:

Q Who was the EIP's primary point of contact at Reddit?

A I've forgotten her name. There was a woman in the policy team. We can come back to you.

Q Do you recall with respect to Alphabet if there was different points of contact for Google as opposed to YouTube or if it was the same point of contact?

A I believe it was the same. For these purposes, the central Google team was the one who was coordinating on their election policies.

Q In 2020, who was EIP's primary former contact with Discord?

A I don't recall with Discord.

Q What about with respect to Wikimedia?

A Yes. There's a -- I don't remember what the name is of the person at Wikimedia. I wasn't a part of those meetings.

Q Who would have been part of those meetings?

A Probably [redacted] or some of the students who were doing onboarding.

Q Who is EIP's primary point of contact with Pinterest?

A I don't recall.

Q Are there plans to -- you mentioned that EIP -- obviously, this is the 2020 iteration. In 2022, you said there were some differences. Are there any plans to have some continuation of the partnership for the 2024 election?

A That's an interesting question. I'm going to have to have a discussion with Stanford's leadership. Since this investigation has cost the university now approaching seven figures legal fees, it's been pretty successful I think in discouraging us from making it worthwhile for us to do a study in 2024.

[redacted]. Do you recall which exhibit we're on?

[redacted]. 21 -- 22.

[redacted]. 22. All right.

[Stamos Exhibit No. 22
Was marked for identification.]

BY [redacted]:

Q Do you know who Jessica Ashooh is? I don't know if I'm pronouncing her name right.

A Yeah. She was the woman I was thinking of, the head of policy for Reddit.

Q Great. And at her email at the top of the page, she says that "We" -- assuming referring to Reddit -- "are unable to participate in Jiras, but we are happy to receive info over email."

Do you recall that Reddit didn't respond in Jira directly?

A Right. They did not -- for whatever reason, did not want to have something they had to log into. They wanted things to be put in the email and sent directly to them.

Q Okay. And then there's an email below from you. You explain the situation. There are a couple of links. And then below you say: "It would be great if we could get somebody from Reddit on the Jira, just like Facebook, Google, Twitter, TikTok, Instagram, CISA, EI-ISAC."

Were you referring to CISA, the government agency?

A I was probably making a mistake there talking about CISA because EI-ISAC were the people who had access to the Jira.

Q But you list both EI-ISAC and CISA. Is that right?

A As I said, I believe I made a mistake in doing so.

Q In listing two entities when you meant one?

A I'm sure if you look through thousands of my emails, as you're doing, you'll be able to find me make some mistakes and typos, yes.

Q But there is a Jira ticket notification that has CISA as well. Is that right?

A I believe that that is a Jira ticket that an imudal system member had been added to. But CISA was not an organization that was onboarded that had the ability just to get the stuff. Any ticket, just like with this, could have been sent to somebody -- this is actually a great demonstration of this. Reddit, as is demonstrated in this email, is not onboarded, yet they received a notification, just as CISA does not have to be onboarded to receive a notification.

Q True. But you're representing to Reddit that CISA is on --

A As I said, in my thousands of emails, I'm sure I misrepresented -- made a mistake somewhere.

Q Okay. How do you think Reddit interpreted this email?

A She says right here, "Unfortunately as we mentioned at the beginning of this project we are unable to participate in external Jiras, but we are happy to receive info over email."

Q Sure. But do you think she read the email to interpret that CISA was on Jira?

A Possibly. And apparently it had no impact because her decision, as she made for herself, is that they did not want to participate in being onboarded onto Jira.

Q Do you think that they declined to participate in part because they were government partners?

A I don't know why they declined to participate. Reddit has always been a little bit of a different company in this. They have kind of a smaller trust and safety team and a different set of ways they enforce their policies because of the complicated relationship they have with their sub Reddits. So it is definitely possible they would approach doing any kind of policy around elections differently than other platforms.

[redacted]. This will be exhibit 23. I believe the majority introduced the same statement. As things go along, we will hand out new versions.

[Stamos Exhibit No. 23
Was marked for identification.]

[redacted]. And this is exhibit 7 earlier.

[redacted]. No problem.

BY [redacted]:

Q If I could have you -- first let me ask again, did you play a role in drafting this?

A Yes.

Q And who else from Stanford played a role in preparing it?

A My colleagues inside of SIO, and then we worked with Stanford lawyers and outside counsel.

Q If I could call your attention -- it will be the top of page 3. The question begins on page 2. The bolded question is: "Is it true that the EIP censored 22 million tweets and labeled them as 'misinformation'?"

And the answer continues -- it starts on the bottom of page 2 and continues on the top of page 3.

A Right.

Q The last full sentence -- there's a semicolon in there -- says: "The EIP informed Twitter and other social media platforms when certain social media posts violated each platforms's own policies; EIP did not make recommendations to the platforms about what actions they should take."

That last half of the sentence, "EIP did not make recommendations to the platforms about what actions they should take," do you understand that statement still to be true?

A So the policy of the EIP was that we were informing platforms when we thought content that we found violated their policies. It is possible that individual students would use language like "I recommend" or "we recommend." Those are the words of 18- to 24-year-olds who have no power, no coercive power, and had no ability to force the companies to do anything.

Q So when communicating with social media platforms via the Jira tickets, it was only students who would do that?

A No. There were also managers and tier 2 analysts, some of whom were professionals, who might add comments that would be seen.

Q Okay. In the previous exhibit we saw, it's the email is from you to Jessica. Is that right?

A That's right.

Q And even if you look down a little bit further, the notification where it's being forwarded to Jessica and there's that same 2020partnership.atlassian.net, the name that appears next to it is yours. Is that right?

A That's right.

Q Okay. So there were instances where there were not students sharing the Jira tickets with the social media platforms?

A That's right. There were professionals. We too, even employees, have First Amendment rights to have our own opinions about what's going on and to share those opinions with others.

Q And did the professionals who were sharing the Jira tickets with the social media platforms, did they ever make recommendations?

A It's possible. We'd have to go look. But, again, the EIP had no power to coerce the platforms to do anything. And, in fact, our hard empirical evidence shows that in 65 percent of the time they took no action because they determined that that was their decision under their own policies.

Q Same page, on page 3, the question is phrased as: "Did EIP receive direct requests from the Department of Homeland Security's" -- it says "CISA to eliminate or censor tweets?"

Did you phrase the question to avoid saying did EIP receive indirect requests from CISA?

A We phrased this question to try to be accurate. And the accusation that's have been made in front of a committee that, unfortunately, none of your members corrected repeatedly is that CISA was telling us to censor tweets. And that turns out to be false on multiple levels. We did no censorship, we had no power to have censorship, and we did not have CISA sending us those requests.

Q To your understanding, if the question had read: "Did EIP receive indirect requests from CISA," could you have provided the same response of a direct no?

A So I can't tell if CISA said something to somebody or if the EI-ISAC forwarded something that perhaps had CISA involved. Beyond the EI-ISAC reporting things to us, we're not sure where it's from. So this is an accurate statement and directly refutes the claims that -- the false claims that were made in front of your committee.

Q But if the question had said: "Did EIP receive indirect requests," could EIP represent the same answer of a direct no?

A If you asked me did EIP receive indirect requests from Donald Trump or from Chairman Jordan, I also couldn't answer it. That's why we try to say direct. We only have the knowledge of what went directly to us. If something was routed through somebody else, I have no idea. It's possible that President Trump asked somebody, who said something, who said something through EIP, and that would be impossible for us to determine. So we try to be as accurate as possible here.

Q Okay. But in the archived data you provided to the committee, there are social media platforms commenting on the Jira ticket system that they communicated through CISA by way of CISA. Is that right? We covered that I think in the second hour.

A Yes. Social media companies refer to them talking to CISA directly.

Q Okay. And you channel the requests through the EI-ISAC, which you represented is operated by CIS, which is funded by CISA. Is that right?

A Partially funded. I don't know where all of their funding comes from, but I do know they have grants from CISA.

Q Okay. And there are email notifications being generated by the Jira ticket system where it says the ticket is being shared with CISA. Is that right?

A There's at least one case that you showed me where somebody from CISA was cc's on the ticket.

Q Okay. And sitting here today -- this statement was drafted I think back in March. Is that right? I don't know if we have a date on here.

A That sounds right.

Q Sitting here today, based off your understanding of who is involved with the EIP, if the question was phrased "Did EIP receive indirect requests from CISA," what response would be accurate?

A Just as I said, I cannot provide any assurances that requests from CISA or any other political actor did not come through some other actor. So, as you can see, we got requests from government officials and such. And so if President Trump sent a request to a political ally of his in the Georgia Secretary of State's office -- maybe that's a bad example -- in the Florida Secretary of State's office and they sent something via EI-ISAC, that would be an indirect request from the government.

So this was accurate when we wrote it, and I still believe that we did not receive any direct requests from CISA.

Mr. Bellinger. So, [redacted], it is 5 minutes to 5:00. I think just to be respectful to the witness, we're going to leave at 5:00. We've taken an awful lot of time. We spent an awful lot of time in the beginning just doing a lot of background stuff, but -- so can we wrap up in 5 minutes?

[redacted]. We'll be done shortly.

Mr. Bellinger. Well, we're going to leave at 5:00.

[redacted]. Understood.

BY [redacted]:

Q With respect to your Florida Secretary of State example, the Florida Secretary of State is one of the offices that participates in the EI-ISAC. Is that right?

A I expect so. I'm not so sure, but I'm pretty sure they do, yes.

Q Okay. Is it your understanding that the role CIS plays is different than the roles that the offices of the various Secretary of State offices play?

A Yes. My understanding is that CIS operates the internal -- the overall organization that coordinates. They run the events. They run the switchboard. They run the mailing list and such.

Q And does --

A And then all of the Secretaries of State and local election directors are the members that generate the communications that then CIS routes.

Q And does CISA play a role with CIS's responsibilities with the EI-ISAC?

A I really can't speak as to the internal organization of the EI-ISAC.

Q Okay. Do you recall what the ticket was that was sent to the FBI?

A It was the -- I can try to find the ticket number. It was the ticket about the Iranians and the Proud Boys.

Q Yeah.

A We sent it to them because there was a direct death threat, and it seemed very possible to have a foreign component. So since that is a straight-up Federal crime, we sent it to the FBI.

Q Do you recall if any social media platforms were tagged on that ticket?

A So, to be clear, I believe the way I communicated to the FBI is I sent a direct email to them, and then we set up a call where we explained our findings to them. They -- I do not believe they got anything out of Jira. So that was me cutting and pasting our -- effectively a draft of the blog post that we eventually sent and sending them these are our conclusions and then talking them through it.

Q Yeah. And so you issued a blog post on this issue. Did that blog post predate the election?

A Yes.

Q And was it -- as part of the blog post, did you reveal that you had sent the information to the FBI?

A I don't recall, no.

Q Okay.

A The blog post is still available if you want to go to eipartnership.net.

[redacted]. Can we go off the record?

[Discussion off the record.]

[Whereupon, at 4:59 p.m., the interview was concluded.]

Certificate of Deponent/Interviewee

I have read the foregoing ____ pages, which contain the correct transcript of the answers made by me to the questions therein recorded.

____

Witness Name

____

Date

Transcribed Interview Suggested Errata Form

Interviewee	Alex Stamos
Date of Interview	06.23.23
Date of Review	07.13.23
Name of Reviewer	Caleb Thompson
Signature of Reviewer	

Page	Line	Suggested Correction
10	16	"tempting" → "attempting"
12	2	"so" → "to"
14	24	"kind" → "kinds"
15	23	"where as" → "whereas"
17	7	? → .
19	17	"Facebook" → "Facebook's"
20	21	"that" → "then"
22	8	"platform" → "platforms"
22	10	"states of" → "states'"
26	18	Insert "what" between "is" & "you"

Page	Line	Suggested Correction
28	23	"one to graduate" → "undergraduate"
31	8	"ops act" → "op sec"
38	1	Delete "sent"
48	8	? → .
80	5	"a" → "is"
82	13	"Trumpies" → "sharpies"
82	15	"anything. We reported the" → "anything we reported to the"
84	3	"tweeter" → "Twitter"
84	24	Delete "the"
91	16	"believe" → "belief"
92	14	"won their" → "wanted an"
93	5	Insert "the" between "was" & "key"
96	15	Delete "it"
96	16	Insert "of" between "number" and "companies"

Page	Line	Suggested Correction
98	11	Delete first "was"
98	12	Delete "he"
98	23	"our" → "other"
100	21	"UDOT" → "UW"
106	2	"at the" → "they"
106	11	"Coffield" → "Caulfield"
108	18	Delete first "that"
163	24	"hacking leak" → "hack and leak"
164	1	" "
176	14	"a" → "the"
178	8	"Elaina" → "Elena"
178	11	"EVP" → "VP"
182	2	Insert "was" between "it" & "violative"
190	21	"his" → "HSI"

Page	Line	Suggested Correction
191	3	" "
219	6	"imudal" → "individual"
[illegible]	[illegible]	[illegible]
222	14	Delete "have"
223	18	"ce's" → "ce'd"
178	11	"that is" → "than"