

**DATA SECURITY AT RISK: TESTIMONY  
FROM A TWITTER WHISTLEBLOWER**

---

---

**HEARING**  
BEFORE THE  
**COMMITTEE ON THE JUDICIARY**  
**UNITED STATES SENATE**  
ONE HUNDRED SEVENTEENTH CONGRESS  
SECOND SESSION

SEPTEMBER 13, 2022

**Serial No. J-117-75**

Printed for the use of the Committee on the Judiciary



*www.judiciary.senate.gov*  
*www.govinfo.gov*

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2025

COMMITTEE ON THE JUDICIARY

RICHARD J. DURBIN, Illinois, *Chair*

PATRICK J. LEAHY, Vermont	CHARLES E. GRASSLEY, Iowa, <i>Ranking Member</i>
DIANNE FEINSTEIN, California	LINDSEY O. GRAHAM, South Carolina
SHELDON WHITEHOUSE, Rhode Island	JOHN CORNYN, Texas
AMY KLOBUCHAR, Minnesota	MICHAEL S. LEE, Utah
CHRISTOPHER A. COONS, Delaware	TED CRUZ, Texas
RICHARD BLUMENTHAL, Connecticut	BEN SASSE, Nebraska
MAZIE K. HIRONO, Hawaii	JOSH HAWLEY, Missouri
CORY A. BOOKER, New Jersey	TOM COTTON, Arkansas
ALEX PADILLA, California	JOHN KENNEDY, Louisiana
JON OSSOFF, Georgia	THOM TILLIS, North Carolina
	MARSHA BLACKBURN, Tennessee

JOSEPH ZOGBY, *Chief Counsel and Staff Director*

KOLAN L. DAVIS, *Republican Chief Counsel and Staff Director*

# CONTENTS

---

## OPENING STATEMENTS

	Page
Durbin, Hon. Richard J. ....	1
Grassley, Hon. Charles E. ....	3

## WITNESSES

Zatko, Peiter .....	5
Prepared statement .....	42
Responses to written questions .....	45

## APPENDIX

Items submitted for the record .....	41
--------------------------------------	----



## **DATA SECURITY AT RISK: TESTIMONY FROM A TWITTER WHISTLEBLOWER**

**TUESDAY, SEPTEMBER 13, 2022**

UNITED STATES SENATE,  
COMMITTEE ON THE JUDICIARY,  
*Washington, DC.*

The Committee met, pursuant to notice at 10 a.m., in Room 216, Hart Senate Office Building, Hon. Richard J. Durbin, Chair of the Committee, presiding.

Present: Senators Durbin [presiding], Feinstein, Whitehouse, Klobuchar, Coons, Blumenthal, Hirono, Ossoff, Grassley, Graham, Cornyn, Lee, Hawley, Cotton, Kennedy, and Blackburn.

### **OPENING STATEMENT OF HON. RICHARD J. DURBIN, A U.S. SENATOR FROM THE STATE OF ILLINOIS**

Chair DURBIN. This meeting of the Senate Judiciary Committee will come to order. In 2006, the new social networking platform marked its debut when Jack Dorsey posted a message that he was, quote, “Just setting up my Twitter.” At the time, Dorsey’s startup, which allowed users to share short messages with their followers was a novelty. But in the coming years it would become increasingly source—an important source of news and social discourse, as it gathered millions of users around the world.

Twitter now plays an outsized role in politics, culture, and even in democracy itself. As Twitter has grown, so have the risks posed by bad actors looking to exploit its opportunities, and the data it holds. In July 2020, two teenagers hacked into the accounts of Twitter employees, gaining access to a number of high-profile accounts, including now President Biden and former President Obama. Those two teenagers then sent a series of tweets from the accounts and scammed Twitter users out of more than \$100,000 in Bitcoin.

In response, then CEO of Twitter, Dorsey, turned to a trusted name in the world of cybersecurity to lead an overhaul of Twitter’s security practices. And for more than a year, that’s what this individual tried to do, until he was terminated by Twitter and their new CEO this past January. Last month, this individual released a whistleblower disclosure, detailing a number of alarming allegations about Twitter’s security practices. Without objection, his disclosure will be entered into the record.

[The information appears as a submission for the record.]

That whistleblower’s name is Peiter Zatko, or as he’s more commonly known, Mudge. Mudge, thank you for joining us. You are here pursuant to a subpoena, not because you were opposed to ap-

pearing before the Committee, but so the public can hear the details of your disclosure. You've alleged a number of security flaws and weaknesses within Twitter, flaws that may pose a direct threat to the safety and privacy of Twitter's hundreds of millions of users, as well as America's national security.

The story actually began in 2011, when the FTC, the Federal Trade Commission, first concluded that Twitter was playing fast and loose with user data. They found that Twitter had, quote, "deceived customers and put their privacy at risk by failing to safeguard their personal information." The company was ordered by the FTC to, quote, "protect the security, privacy, confidentiality, and integrity of user data." But you've claimed those changes have never been made, and more broadly, you allege that compared to other technology companies, Twitter's security standards remain woefully deficient. You allege that thousands of employees within the company have extraordinary access to sensitive information of Twitter's users, and that there is little oversight over how that information is assessed.

Some Twitter users tuning in this morning may be asking, "Well, what's the big deal?" When you sign up for Twitter, you knowingly hand over your email, your phone number, other information. That's how it is with most social media companies. But you expect—do we not—that these companies will take precautions to protect the personal information that you give them. It's like depositing money at the bank. When you hand your money to the teller, they take it behind the counter and put it in a vault, but at Twitter, according to our witness today, the door of that vault is wide open. And that vault contains a lot more information about you than you can imagine.

Twitter doesn't just have access to your tweets and mail—email address, they also have access to all of the data necessary to directly access your device, and even pinpoint your exact location. Say you're an American citizen. You're exercising your First Amendment freedom at a political protest. Or maybe you're a woman seeking reproductive health care. If you're a Twitter user, it may not just be you at the protest or in that health care facility. Unbeknownst to you, someone else may be right there with you in your pocket, or purse.

Of course, many of us are comfortable with some of the programs on our phones having location data. It's helpful, but when that data isn't secure, we become vulnerable to bad actors, scam artists, stalkers, even foreign agents. To give an example, earlier this year, a Saudi national who worked for Twitter was convicted by a Federal jury for stealing the personal data of dissidents who criticized the Saudi regime and handed the data over to the Saudi government. This is a matter of life and death, as we know, for these dissidents, as the butchering of Jamal Khashoggi made clear.

There's also the matter of Twitter's reach. It was one of the largest megaphones that world leaders ever had at their disposal. We've already seen what can happen when small-time actors break into Twitter accounts, belonging to Government officials. But what if—what if next time it isn't two teenagers trying to pull a crypto scam? Imagine if it's a malicious hacker, or a hostile foreign government, breaking into President—the President's Twitter account,

or sending out false information, claiming there was a terrorist attack on one of our cities? We can see widespread panic. The bottom line is this: Twitter is an immensely powerful platform that cannot afford gaping security vulnerabilities. Today we have a chance to engage in a good-faith, bipartisan discussion to ask what needs to be done.

A final point, politicians on both sides of the aisle have criticized Twitter. I have, for one, believed that Twitter should be doing far more to combat the proliferation of hate speech and conspiracy theories. Republicans, on the other hand, claim that Twitter censors their conservative speakers. I urge my colleagues to set some of the partisan differences aside and try to find the common ground that we need to establish security standards that will be raised today by our whistleblower. With that, I turn to our Ranking Member, Senator Grassley.

**STATEMENT OF HON. CHARLES E. GRASSLEY,  
A U.S. SENATOR FROM THE STATE OF IOWA**

Senator GRASSLEY. Thank you, Chairman Durbin. A very important issue that you have brought before this Committee, and I thank you for doing it. I, for one, want people to know that I love using Twitter. But we also know that Big Tech companies, such as Twitter, collect vast amounts of data on Americans. In the hands of foreign adversaries, this data is a goldmine of information that could be used against America's interest.

Twitter has a responsibility to ensure that the data is protected and doesn't fall into the hands of foreign powers. Americans rightly expect that Twitter will protect that information. Thanks to a whistleblower that comes forward, we've learned that Twitter hasn't secured the data of tens of millions of Americans and countless other users. That whistleblower is here today. So, we welcome you, Mudge.

He comes before the Committee today, not only as an expert in the field of cybersecurity, but also as a whistleblower. I think all of my colleagues know that I have a great deal of admiration for whistleblowers. I've always said that whistleblowers are patriotic individuals, who often sacrifice their own career, as well as their livelihood, to root out waste, fraud, and abuse. Thank you very much for being here.

Because of Mudge's disclosures, we've learned that personal data from Twitter users was potentially exposed to foreign intelligence agencies. For example, his disclosure indicates that India was able to place at least two suspect foreign assets within Twitter. His disclosures also note that the FBI notified Twitter of at least one Chinese agency—agent in the company—company, I should say. Based on allegations, Twitter also suffers from a lack of data security. Due to that failure, thousands of Twitter employees can access user data, that data that they don't need access to in order to do their job. Yet they have access. And if foreign assets work for Twitter, that means these foreign assets can also access the data.

To put a finer point on the allegations, Twitter has allegedly used the data it collects and the tools it has to geolocate individuals who made threats against board members. In the hands of a foreign agent embedded at Twitter, a foreign adversary could use

the same technology to track down pro-democracy dissidents within their country, but also to spy on Americans. This has actually happened in the past.

In 2019, two Twitter employees were indicted by the FBI. They used their position at Twitter to access private user data, and then gave it to Saudi Arabia. These foreign agents were able to access and provide personal information on more than 6,000 individuals of interest to the Saudi government.

Simply put, the whistleblower disclosures paint a very disturbing picture of a company that's solely focused on profit at any expense, including at the expense of safety and security of its users. Additionally, it's been alleged that Twitter knowingly violated a consent decree that it entered into with the Federal Trade Commission, 2011. That consent decree required Twitter to address their access control failures. However, instead of complying with the consent decree, and fixing these very serious security matters, it alleged that Twitter executives, specifically CEO Parag Agrawal, intentionally misled Twitter's board of directors.

So, I'm concerned that for almost 10 years the Federal Trade Commission didn't know or didn't take strong enough action to ensure Twitter complied with the consent decree. This is a consent decree that was intended—intended to protect Twitter users' personal information. As Congress considers Federal data privacy legislation, I think it's very important that we draw on these revelations about how Twitter views its obligations with Federal regulators.

Congress should also be mindful of the FTC's ability, or lack thereof, to successfully oversee these important issues. Twitter also needs to answer questions about its content moderation. It was revealed to this Committee that Twitter outsources a great deal of content moderation to foreign countries. They have close to 2,000 employees in other countries, whose job is to screen tweets by Americans. They also lack the appropriate amount of translators to ensure that tweets in other languages are complying with Twitter's own rules.

Mudge had limited visibility to content moderation while at Twitter, so these are questions that need to be answered in full by Twitter, because we can't expect Mudge to respond to them. Unfortunately, this Committee will not be able to get answers about content moderation because Twitter's CEO has refused to appear today. He rejected this Committee's invitation to appear by claiming that it would jeopardize Twitter's ongoing litigations with Mr. Musk. Many of the allegations directly implicate Mr. Agrawal, and he should be here to address them.

So, let me be very clear. The business of this Committee and protecting Americans from foreign influence is more important than Twitter's civil litigation in Delaware. In conclusion, if these allegations are true, I don't see how Mr. Agrawal can maintain his position at Twitter. Going forward, Chairman Durbin and I will continue to conduct a thorough and in-depth investigation. Today's hearing is a part of that process. Thank you.

Chair DURBIN. Thank you, Senator Grassley. Mr. Zatko, you will have 6 minutes for an opening statement, and then each Member will be given 6 minutes questioning to follow up. We start with a

customary oath, and I ask you to please stand for that purpose. Please raise your right hand.

[Witness is sworn in.]

Let the record reflect that the witness has answered in the affirmative, and I appreciate your attendance here, and the floor is yours. I think your microphone may need—

**STATEMENT OF PEITER “MUDGE” ZATKO,  
INDEPENDENT SECURITY CONSULTANT,  
NEW YORK METROPOLITAN AREA**

Mr. ZATKO. Thank you very much, sir. Chairman Durbin, Ranking Member Grassley, Members of the Committee, I appear before you today to answer questions about information I submitted in written disclosures about cybersecurity concerns I observed while working at Twitter. My name is Peiter Zatkó, but I’m more often referred to by my online handle as Mudge. For 30 years, my mission has been to make the world better by making it more secure. From November 2020 to January 2022, I was a member of Twitter’s executive team. In my role, I was responsible for Information Security, Privacy Engineering, Physical Security, Information Technology, and Twitter Global Support.

I’m here today because Twitter’s leadership is misleading the public, lawmakers, regulators, and even its own board of directors. What I discovered when I joined Twitter was that this enormously influential company was over a decade behind industry security standards. The company’s cyber security failures make it vulnerable to exploitation, causing real harm to real people. And when an influential media platform can be compromised by teenagers, thieves, and spies, and the company repeatedly creates security problems on their own, this is a big deal for all of us.

When I brought concrete evidence of these fundamental problems to the executive team and repeatedly sounded the alarm of the real risks associated with them—and these were problems brought to me by the engineers and employees of the company themselves—the executive team chose, instead, to mislead its board, shareholders, lawmakers, and the public, instead of addressing them.

This leads to two obvious questions. Why did they do that, and what were the problems and vulnerabilities identified? And that’s what I’m here to talk about. So, first, why did they do that? To put it bluntly, Twitter leadership ignored—ignored its engineers, because key parts of leadership lacked the competency to understand the scope of the problem, but more importantly their executive incentives led them to prioritize profits over security. Upton Sinclair famously said, “It is difficult to get a man to understand something, when his salary depends on his not understanding it.” This mentality is exactly what I saw at the executive level at Twitter.

So, what are the problems I discovered? Two basic issues. First, they don’t know what data they have, where it lives, or where it came from, and so, unsurprisingly, they can’t protect it. And this leads to the second problem, which is, the employees then have to have too much access to too much data and to too many systems. You can think of it this way, which is, it doesn’t matter who has keys if you don’t have any locks on the doors. And this kind of vulnerability is not in the abstract. It’s not farfetched to say that an

employee inside the company could take over the accounts of all of the Senators in this room. Giving to the real harm—given the real harm to users and national security, I determined it was necessary to take on the personal and professional risk to myself and to my family of becoming a whistleblower.

I did not make my whistleblower disclosures out of spite or to harm Twitter, far from that. I continue to believe in the mission of the company and root for its success. But that success can only happen if the privacy and security of Twitter's users and the public are protected. In accepting an executive position at Twitter, I made a personal commitment to Mr. Dorsey, the board, the greater public, and myself, that I would drive the changes needed at Twitter to protect the users, the platform, and democracy. That's what I'm continuing to do here today. I stand by the statements I made in my lawful disclosures, and I am here to answer any questions you may have about them. Thank you.

[The prepared statement of Mr. Zatkan appears as a submission for the record.]

Chair DURBIN. Thank you, Mr. Zatkan. I'll start the questioning, and as I mentioned, each Member will have 6 minutes to ask you questions. Those of us who are not expert but rely on the internet everyday for personal and professional reasons, know that many times we are given disclosures, lengthy disclosures, that scroll across the screen, which are hardly ever read, in my estimation, and usually end up with a bottom box that said approve. And that is as far as we go warning about what we're getting into. Can we get into the real world now and talk about whether or not consumers across America have a right to be warned if they are opening or using a Twitter account, as to what's going to happen with their data?

For example, if I disclose my name and my address and my email address, I expect that that may be vulnerable. Somebody could use that in some future time. You hope not, but it could happen. But what I infer from your testimony and what we've read about your findings is that there's a lot more information being collected by Twitter, beyond that basic information that is going to be used by them for different purposes. Is that a fact?

Mr. ZATKO. Yes. I entirely concur. I mean, when we sign up for an account, I hope that the company is being responsible and not just saying that they are, you know, would like the data to be used correctly and safely, but that they're actually able to quantifiably, internally, you know, guarantee that that is the case. As far as the type of data, I believe Senator Grassley, you know, referred to an incident. We had a user on Twitter that was harassing some members of the executive team, and some members of the board.

And as an example, this person, the CTO, came to me and said, "Mudge, you know, is this a real viable threat? Do I need to be worried? You know, who is this person?" And it took me maybe 30 minutes to reach out to an employee and say, "What do we know about this person?" And it only took that person maybe 10 minutes to get back to me and said, "Okay, here's who they are. This is the address where they live. This is where they are physically at this moment. They're on their phone. We know their phone number. We also know all of the other accounts that they've tried to set up on

the system and hide. And we know who they are on the other social media platforms as well.”

Chair DURBIN. So, unbeknownst to a Twitter account user, there is access to information far beyond what you think you’ve disclosed that can be found. Should there be a warning? You say at one point, Twitter has about 20 percent of its vast trove of data registered and managed, meaning the company is incapable of securing the sensitive information it collects. Tell me—that is a pretty stark statement and suggests that a warning to users is that literally anything that you disclose or use the account for is traceable and could be used for bad purpose.

Mr. ZATKO. Yes. In this case, my concern was more that Twitter didn’t even know what it was collecting. And this was one of the problems, because I kept looking at why do they keep having so many security incidents? The same amount, you know, each year after year? Why are the same percentages, you know, from the same systemic problems? Why aren’t we closing on this? What is fundamentally under the hood broken? Where is the systemic failure? And then it turned out from an internal study that the engineers did on their own, because they weren’t given, you know, the cover and the time and the resources to do this as part of their job, that only about 20 percent of the information that they had—that they were collecting did they know why they got it, you know, why the person had given it to them, how it was supposed to be used. You know, when it was supposed to be deleted, you know, and the remaining—I think it was 80 percent—I refer you to the disclosures for the specific numbers—was, “Hey, we know that our systems are using some of this other data, but we don’t know what it is.” And then a lot of the data they just recognized, “We don’t even know what these are.” Petabytes, huge amounts of data. And they did a sampling that included personally identifying information, phone numbers, addresses. So, for me, the concern there is anybody with access inside Twitter, and half the company has access to the production environment that has this, could go rooting through and find this information and use it for their own purposes.

Chair DURBIN. So, if 80 percent of the data that is being collected is, in fact, not registered and managed, and the one with the Twitter account person is vulnerable in that regard, I wouldn’t exactly give a passing grade to Twitter when it comes to the security of information that they’ve gathered. Now, let me ask you, on the other side of the ledger, would you grade as well, the Government agencies that have some responsibility to make sure that the American consumer’s privacy and security is protected? For example, Federal Trade Commission, Security and Exchange Commission, and others.

Mr. ZATKO. So, that was something that I was—what came to mind as well is that we had a 2011 consent decree. This is over a decade. How have we been passing this, especially since there were at least two more times where there were violations for the same exact problem, the misuse of email data that was collected for security purposes, but then turned around and used for marketing. Which was a violation of the assumption of why you were providing them the data. How come we keep making these same mistakes?

You know, what is the FTC missing, or what is it that we are telling the FTC, as Twitter, that is incorrect? And I think—I think, honestly, I think the FTC is a little, you know, over their head. Compared to the size of the Big Tech companies and the challenge they have against them, they're left letting companies grade their own homework. And I think that's one of the big challenges.

Chair DURBIN. I'm running out of time, and I'll just say that I think that the area of great concern, as well, is the access of foreign governments and foreign agencies to the same data. Americans signing up for Twitter have no idea that they are at least vulnerable to that possibility, and we know that the conviction of individuals in Saudi Arabia, or for dealing with the Saudi government, is proof positive of that possibility. Thank you very much. Senator Grassley.

Senator GRASSLEY. I'm going to take off where the Chairman just left off. The Communist Chinese government bans Twitter, yet companies based in China advertise on the platform. When a user clicks on such an advertisement, they've presumably redirected to a website controlled by the Chinese government, which can collect vast amounts of data and track their location. With respect to pro-democracy Chinese citizens, is Twitter endangering their lives by allowing China to advertise on the platform?

Mr. ZATKO. I think that's a very valid concern, sir. And that was a concern that was raised to me by the employees inside Twitter, who were disturbed that in a country where the service was not allowed to be used and provide the—a voice to the public, but that money was being accepted from organizations that may or may not be associated with the Chinese government. And I believe that there was a Reuters article just a day or say ago, saying that they did identify that there were governments related to China advertising on the platform, possibly in violation of Twitter's own policies.

The executive in charge of sales, very shortly after I joined, said, "Mudge, this is a big internal conundrum. Because we're making too much money from these sales, we're not going to stop. We need something that will make the employees more comfortable with the fact that we're doing this." Figure out how we essentially thread this needle or frame it, which made me a bit uncomfortable. And they didn't know what people they were putting at risk, or what information they were even giving to the government, which made me concerned that they hadn't thought through the problem in the first place, that they were putting their users at risk for. And that was a very common problem, where I saw that Twitter was a company that was managed by risk and by crises, instead of one that manages risk and crises. It was reacting—it would react to problems too late.

Senator GRASSLEY. I think you just answered this question, but I want to ask it and see if you've said all you wanted to on the subject. While at Twitter, you raised concerns with their policy allowing Chinese advertisement. What was Twitter's response?

Mr. ZATKO. In a nutshell, it was, "We're already in bed. It would be problematic if we lost that revenue stream. So, figure out a way to make people comfortable with it."

Senator GRASSLEY. Okay. According to your disclosure, thousands of Twitter employees have access to Twitter user data and internal systems. That includes nearly 4,000 engineers, which is half of Twitter's workforce. However, you stated that they don't need that kind of widespread access to perform their job duties. Based on Twitter's reported lack of data security, what kind of access would foreign agents have and what kind of data would they be able to obtain? In your answer, please explain why this is a problem, and how it could impact U.S. national security.

Mr. ZATKO. Yes, sir. Let me break that down into two parts of an answer. So, Twitter has engineers and non-engineers. Twitter does not have—at least when I was there, which was up until January 2022—does not have a testing environment, or a developing or staging environment. This is—this is an oddity. This is an exception to the norm. Most companies will have a place where you test your software, where you build it, where you make sure it's working the way you want it to. Think about somebody building an airplane. And saying like, "I'm going to put it in a wind tunnel. I'm going to build it in an environment—I'm not going to put passengers on it, put it in the air, and then figure out how to build it or tweak the engines at that point."

Twitter just has the production environment, the running systems, the live data. When you become an engineer, which is half the company are engineers, you are by default given some access to this live production environment. You are doing your testing. You are doing your work on live systems and live data, irrespective of where you are in the world as an engineer. So, if you are a foreign agent and you are hired, and you are an engineer, you've got access to all of that data that we've talked about, the 80 percent that Twitter doesn't know what's in. Yet the engineers studied and realized this personally identifying information, other sensitive information, where there's a lack of access controls because they have too much data and they just didn't know where everything is, so they have to give everybody access. And the systems can access the information.

But also recall that foreign agents can have multiple goals. And sometimes it's not just the engineers or the technical access that they want, but it might be information about the plans of Twitter, what plans Twitter has to potentially censor information in the government or concede to a government's request, or what plans they have for expansion in a particular environment. And in those cases, that's where I saw, with high confidence, a foreign agent placed from India to understand the negotiations and how well they were going for or against India's party who was having difficulties with Twitter in India.

Senator GRASSLEY. In your disclosure you mentioned that the FBI notified Twitter that one of their employees was suspected of being a Chinese foreign asset. Were you and others at Twitter at all surprised by that?

Mr. ZATKO. This was made aware to me maybe a week before I was surprised and summarily dismissed. I had been told because the Corporate Security/Physical Security team had been contacted and told that there was at least one agent of the MSS, which is one of China's intelligence services, on the payroll inside Twitter.

While it was disturbing to hear, I and many others, recognizing the state of the environment at Twitter, were really thinking if you were not placing foreign agents inside Twitter—because it's very difficult to detect them—it is very valuable to a foreign agent to be inside there as a foreign intelligence company—you're most likely not doing your job.

Chair DURBIN. Thank you, Senator Grassley. Senator Feinstein.

Senator FEINSTEIN. Thanks, Mr. Chairman. On August 10, 2022, a Federal jury convicted a former Twitter employee of acting as an unregistered foreign agent for the Kingdom of Saudi Arabia. While employed by Twitter, the individual accepted payments in exchange for accessing and conveying the private information of Twitter users to Saudi officials. That individual is one of two former Twitter employees charged by the Department of Justice for their efforts to provide Saudi officials with the personal information of dissidents and activists critical of the Saudi regime, including sensitive data that could identify and locate these individual users.

Now, the question. As head of security, Mr. ZATKO, can you describe the types of efforts you've seen by foreign governments to infiltrate, control, exploit, or surveil Twitter and its users, and share what steps Twitter and regulators should have taken to protect against these attacks?

Mr. ZATKO. Yes, ma'am.

Senator FEINSTEIN. Thank you.

Mr. ZATKO. One of the disturbing things that I saw based upon being 10 years behind where I would expect a modern tech company to be, was a lack of an ability to internally look for and identify inappropriate access within their own systems. Other than the person who I believe, with high confidence, to be a foreign agent placed in a position from India. And from—it was only going to be from an outside agency or somebody alerting Twitter that somebody already existed, that they would find the person. What I did notice when we did know of a person inside, acting on behalf of a foreign interest as an unregistered agent, it was extremely difficult to track the people. There was a lack of logging and an ability to see what they were doing, what information was being accessed, or to contain their activities, let alone set steps for remediation and possible reconstitution of any damage. It simply lacked the fundamental abilities to hunt for foreign intelligence agencies and expel them on their own.

Senator FEINSTEIN. You said it was difficult to track. Explain exactly what you mean about that—what you mean, and second, what could be done to correct that.

Mr. ZATKO. One of the most senior engineers in the company came to me not long after I was there and said, "Mudge, you should know that this company doesn't really have centralized logging. We don't log the activities of the systems." I was surprised by this. Most tech companies—most companies I know of, even not in tech, you know, have logs about what's happening on their systems, and this tells you who tried to log in, who was doing what, where, when it happened.

Later on in my tenure, I learned that there were thousands of failed attempts to access internal systems that were happening per week, and nobody was noticing. And when we brought this up, peo-

ple said, “Well, who is it? What is it?” And I said, “That’s what we’re trying to find out. Why wasn’t—why weren’t we even being aware of this?” This fundamental lack of logging inside Twitter is, you know, a remnant of being so far behind on their infrastructure and the engineering, and the engineer is not being given the ability to put things in place, to modernize.

I can give an example. Let’s suppose you have five credit cards, and you’re receiving statements each month, but only two of those statements gives you detailed transactions. And you want to see if there’s fraud on your credit cards. Well, first off, three of those credit cards, you’re not going to be able to look at the transactions. You just know the total bill. And those remaining two, you don’t have time to go through the transactions and look for it. So, you kind of wing it and say, “I need all those credit cards to stay alive,” so you just keep paying off the bills. That’s kind of the analogy I have for the production environment and the logging situation at Twitter. So, you can understand that trying to understand what an adversary inside identified is doing can be pretty challenging, without logs.

Senator FEINSTEIN. Have you thought about how one would design legislation, which would maintain some basic, necessary rights, and yet cover this area?

Mr. ZATKO. Well, I’ve been thinking a lot about the regulators. Because, of course, I was very curious as to, you know, how was Twitter still operating like this since there was a 2011 consent decree that was aimed at addressing a fair amount of this? I noticed a few things. One, there were a lot of evaluations and examinations, which were interview questions. So, essentially, the organization was allowed to grade their own homework. Did you make things better? Yes, we did. Okay, check. There wasn’t a lot of ground—ground truth. There wasn’t a lot of quantified measurements. And a fair amount of the interviews came from companies’ auditors, that Twitter themselves were able to hire. So, I think that’s a little bit of—maybe a little bit of a conflict of interest.

I also noticed that of all the regulators, some of the foreign regulators were more feared than the FTC. For instance, the French CNIL, the CNIL—the French version of the FTC—terrified Twitter in comparison to the FTC. And when I looked at why, it was because there was more of the fear that it wouldn’t be a one-time fine. One-time fines are priced in. One-time fines didn’t bother Twitter at all. When I saw the recent amount of the fine that was much less than we had been concerned about—and each time it was a one-time fine, in my discussions with the chief privacy officer, with the privacy engineer head, that was a—and the executives, the thought was, “Okay, we’ll pay that and we can keep kicking the can down the road and hope, you know, maybe we’ll get another one-time fine.” Wall Street didn’t seem to care because it wasn’t a long-term problem that was ongoing. What did make these companies afraid, was if there was a risk of, “Hey, you’ve mishandled the same type of data repeatedly. Maybe we’re not going to let you monetize that type of data—

Senator FEINSTEIN. I’m sorry. Who mishandled the data?

Mr. ZATKO. Oh, so, if Twitter, for example, Twitter mishandled email addresses repeatedly, and a concern was, “If the FTC were

to come in and tell us that we're not allowed to monetize email addresses because of our continued inability to handle them correctly, well then we might not be on fair footings with our competitors." And that scared them and made them move. I believe something like that did happen to Facebook, which has been used as a sort of cautionary tale inside organizations. So, I think the regulators have tools that do work, but they're not able to see which tools in their toolbelt are the ones actually working and they're using the ones, the one-time fines, that the companies aren't really afraid of.

Chair DURBIN. Thank you, Senator Feinstein. Senator Lee.

Senator LEE. Thank you very much, Mr. Chairman. Mr. Zatzko, thanks for being here. In your disclosures, you include information that Twitter's head of privacy engineering and the chief privacy officer reported the following to the board of directors, toward the end of 2021. This is a quote. "Every new employee has access to data they do not need to have access to, for the purpose of their role." And also added that until Twitter could reach the point where it could implement a system to manage access to data, they were, quote, "at risk of inappropriate access or use of data." They also reported that, "Our inability to delete data compounds that risk, as we retain data that we should not have, and which is therefore accessible by people who do not need to have access to this data."

Tell me, Mr. Zatzko, what action was taken by Twitter's board of directors in response to this rather shocking information?

Mr. ZATKO. This is not the first time the board of directors had been made aware of that or told this. And there was no change or mandate or charge afforded by the board of directors.

Senator LEE. What do they mean when they refer to the inability to delete data? Why is that significant?

Mr. ZATKO. If you don't know where your data is—as we talked about, these large amounts of data—and somebody comes in and says, "I've left the system, you know," and maybe the FTC asks, "Well, you know, have you deleted all the user data?" You can't respond in the affirmative, because—

Senator LEE. Even if you deleted the account?

Mr. ZATKO. Correct, because you don't know where else this data lives in systems, because you don't know what data you have and where it is. That's correct.

Senator LEE. So, does this mean that Twitter is actually unable to delete data, or is it just unwilling?

Mr. ZATKO. It is unable because they do not know where it is, so they are unable to comply.

Senator LEE. Okay. But this has resulted from a deliberate decision at some point, to adopt protocols that don't allow them to do that, right?

Mr. ZATKO. To choose other priorities rather than to correctly register and track and understand where their data lives.

Senator LEE. Because it is physically possible. I mean, you can have a data base in which—

Mr. ZATKO. Yes, absolutely, if you knew where everything was in your data base, you could go delete it. If you chose to make that a priority, to make sure that the new data coming in was correctly registered, and to go back and figure out what data you have and

where it is. You could absolutely go delete it, but that hasn't been prioritized over other projects, such as increasing revenue or users.

Senator LEE. Now, I'm concerned, as I assume most or all Americans would be, those who become aware of these concerns, that Twitter has seemingly turned a blind eye, rather deliberately, to some pretty significant security risks. Potentially compromising their own personal data, including geolocation information, both to hackers and to foreign government agents, and to other people who for whatever reason, whether for corporate espionage purposes or other commercial purposes, or otherwise might want to gain access to this information.

Based on your disclosures, it seems to me that Twitter's CEO is more concerned with increasing influence and profits from foreign countries than with protecting user data from foreign spies or hackers. Now, you claim that Twitter has hired foreign government agents as cost—sort of the cost of doing business in countries like India, Nigeria, and China. And as you've related, Twitter has knowingly hired these government spies so as to not risk losing access to users and markets in those countries. Or in the case of China, to not lose access to advertising revenues. Do these engineers who are suspected of being foreign agents, do they have access to all user data, or just a certain subset of the user data?

Mr. ZATKO. To be very specific, the India incident was not an engineer, and as I mentioned to the other Senator, I think that was more put in place more to understand Twitter's intent in negotiations with the court and the ministry of India before Twitter—you know, to have an inside information to understand—

Senator LEE. He worked with other people who were themselves engineers?

Mr. ZATKO. Yes, sir.

Senator LEE. He had access to them.

Mr. ZATKO. Yes, sir. There were numerous engineers in the India office—I'm sorry—I focused on that, and I lost the other part of your question.

Senator LEE. So, let me ask you this. Is there anyway to track what data they access, or the data that they share?

Mr. ZATKO. We found that to be very difficult. We had to set up a specific small team, individually, to try and create a unique environment, just to allow us to track and monitor and log one individual. Because of the lack of general logging and access control, that we found would be unscalable and not reproducible, should there be any other people like that. It was a lack of basic, fundamental tools and access control.

Senator LEE. Okay, so I'm almost out of time, but I need to know this. Why would Twitter not create a tracking or a logging system to follow this sort of thing, to make sure that it was handled correctly? Particularly given that they know that many foreign governments like India and Nigeria and China specifically want to access and use that data to find and root out and punish dissidents. Why would they want to do that? Why would they want to subject their own users to this kind of harm, with the grave implications that it carries, especially in those countries?

Mr. ZATKO. I think they would like to, but they're simply unwilling to put the effort in at the cost of other efforts such as driving

revenue. I'm reminded of one conversation with an executive when I said, "I am confident that we have a foreign agent." And their response was, "Well, since we already have one, what does it matter if we have more? Let's keep growing the office."

Senator LEE. Right.

Chairman DURBIN. Thank you, Senator Lee. Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much, Chairman. Thank you, Mr. Zlatos. Following up on that point, I just returned from Ukraine, where Senator Portman and I saw first-hand the extent of the damage inflicted by the Russian invasion. I was troubled to learn that according to your written disclosures, Twitter's leadership recently considered agreeing to the Putin regime's request to censor and surveil Russian Twitter users. Twitter ultimately did not agree to Putin's request, as far as I understand. What can you tell us about requests made by foreign governments and the risk that those demands pose? And why would a company like Twitter consider agreeing to requests to censor and surveil users?

Mr. ZATKO. I was very surprised and shocked by that one-on-one conversation with which I had with Mr. Agrawal. This was prior to his assuming the CEO role. I understand—be it out of a frustration of the inability to perform—and this kind of goes into content moderation which we talked about before, and why all that wasn't my main bailiwick, and I've been informed I shouldn't go into details about conversations that I've had with Twitter counsel. There was a—we don't really have the ability and tools to do things correctly. This a lot of work. It's not, you know, driving our main executive incentive goals. Is there a way that we can simply punt? And since they have elections, doesn't that make them a democracy?

Senator KLOBUCHAR. Thank you. I am a big believer that these companies, and not just Twitter, have to invest more in protecting data and protecting the public, and I heard Senator Durbin talk to you about the agencies, right? And you, I think, agree with me that the agencies in the U.S. are underfunded when it comes to taking on these major cases. But I want to turn to ourselves and put the mirror back on ourselves here in Congress. Do you think it would be helpful if we passed some privacy legislation in Congress?

Mr. ZATKO. I think one thing that would be very helpful is that the FTC and other regulators don't have laws or rules that would create whistleblower protection programs for people while they were still in these organizations. And I think that's where—I mean, I learned a lot of information, a lot of people wanted to share the information. When I came on board, they were excited that there was an executive that was listening and that was willing to ruffle feathers, that was willing to fight for some of these things because they had tried to raise them—

Senator KLOBUCHAR. Yes. I understand.

Mr. ZATKO. Yes.

Senator KLOBUCHAR. Okay, are you aware that Senator Grassley and I actually passed a bill to change the merger fees that passed through this Committee unanimously, passed through the Senate—it's now sitting somewhere in purgatory over in the House—that would allow us to fund the FTC. So, maybe they would be as scary as France or some other country in that we have been unable to pass that. Or actually, despite this probably being our 50th hearing

between—and I'm looking at Senator Blackburn—between Commerce and Judiciary, we have not passed one bill out of the U.S. Senate when it comes to competition, when it comes to privacy, when it comes to better funding the agencies, when it comes to the protection of kids that Senator Blumenthal and Senator Blackburn have worked on. And so, at some point, when we talk about the agencies, I think we better be putting a mirror on ourselves, because I was listening to your quote from Sinclair Lewis. "It is difficult to get someone to understand something when his salary depends on him not understanding it." Could you talk about the lack of action in Congress and how that has actually created an environment where these companies feel like they can do everything from destroying our newspapers and our public good, to basically not taking correct actions when it comes to hacking?

Mr. ZATKO. So, that's your world, not mine. I appreciate the efforts and the work that you're doing. What I did see, is that any laws or bills passed, or actions in the past, if they are not able to be quantified and externally audited by an independent viewer, get gamed a lot by what I saw inside Big Tech, in their ability to sort of answer in an affirmative without actually doing what the intention was of the rule of law or regulation.

Senator KLOBUCHAR. One other bill I want to mention and teamed up here with Senator Coons and Portman on this Platform Accountability and Transparency Act, to require digital platforms to give researchers access to data. And the independent experts that you hired to audit Twitter's processes for addressing disinformation found serious problems, made recommendations. However, I think Twitter's leadership didn't listen. In your view, why do you think Twitter failed to act on the recommendations made related to the disinformation, and how could independent groups help?

Mr. ZATKO. Yes, I'm a big fan of independent groups having independent eyes and providing ground truth on that. I think this is—I should be clear, you know, first off, the engineers and the employees want this change. The culture, and I can speak primarily about Twitter, because that's what I'm here to talk about, the most recent Big Tech company I've been involved with. It's a culture where they don't prioritize. They're only able to focus on one crisis at a time. And that crisis isn't completed. It's simply replaced by another crisis.

Senator KLOBUCHAR. Correct.

Mr. ZATKO. So, I think they would like to wave a magic wand and have all of these things fixed, but they're unwilling to bite the bullet and look strategically and say, "Hey, we're going to have to devote some time and money to get these basic things in place." And to be honest with their investors, the public, their board, themselves, and do the legwork rather than just react to what's coming in that they hear from a hearing like this or from the news, just until the next crisis comes along.

Senator KLOBUCHAR. Exactly, as opposed to us putting some long-term rules in place. Last thing, you talked about in your disclosures that Twitter does not have enough resources focused on removing misinformation and hate speech. In particular, you noted that half of the content flagged for review in Twitter's Spaces fea-

tures, was in a language that employees didn't even speak. Obviously, you can't check whether a tweet violates Twitter's rules if you don't speak the language.

I have had my own experience directly conveying a misinformation that was put out on me, that resulted in an attack on a member of my family. I don't know if you knew that, because I told Jack Dorsey about it, and nothing ever changed, except when finally, regular media reported that it was a lie. But those are the kinds of things that happen to people in this building, because of the misinformation that is rampant on social media. Could you comment about what you think they should be doing about that?

Mr. ZATKO. I'm very sorry to hear about that. The lack of language was stunning to me. This was a situation where I brought in a world class leader for Twitter Global Support, who also identified this. And we started saying, "You can't react to a language situation." When something was happening in Myanmar, you can't wait until after it happens and then go, "Where are the Burmese speakers? Let's see who we can hire." Those translators are already hired elsewhere. You have to understand 80 percent—Twitter has to understand, 80 percent of their users are outside of the United States. You can't create, you know, a healthy environment. You can't serve the public conversation if all you can do is look at it and say, "I hope Google Translate is doing the right job for me."

Senator KLOBUCHAR. Thank you.

Chair DURBIN. Thank you, Senator Klobuchar. Senator Kennedy.

Senator KENNEDY. Thank you, Mr. Chairman. Mr. Zatkan, give me 30 seconds. Well, strike that. Senator Grassley is an active user on Twitter. I'll use him as an example. Give me 30 seconds on the type of information Twitter has on Senator Grassley, or someone like him.

Mr. ZATKO. If I was—if there was somebody just like what the CTO came to me and said, "Hey, we've got a problem with this user. Is this user—"

Senator KENNEDY. Just give me 30 seconds on the type of information—

Mr. ZATKO. Sure.

Senator KENNEDY [continuing]. That Twitter has on the average Twitter user.

Mr. ZATKO. Sure. What's the phone number? What's the latest IP address they've connected from? Are there other IP addresses that they've connected from? Is this the current email? How long have they been using that email with the account? What are the prior emails for it? From the IP address, where do we think they live? Where do we think they're connected to right now? Are they still connected, even if they're not actively using the information? What type of device are they connected with? What type of web browser are they using? Which brand is it possibly? Which computer? What language did they connect in it? Those are some of the front-end systems—

Senator KENNEDY. Thank you. Thank you for that. And I want to be sure I understand that you're telling this Committee that all of the engineers and half the employees of Twitter have access to Senator Grassley's account.

Mr. ZATKO. Half of the employees of Twitter are engineers. The engineers are, by default, given some access due to the production environment—

Senator KENNEDY. Do they have access?

Mr. ZATKO. From what I saw, if they wanted to root around in the data and find it, they could find it, and—

Senator KENNEDY. Okay, let me try this again. I want to be sure I understand, okay? I'm not trying to trick you. From your testimony, I understand that half of all of the engineers and half of the employees at Twitter have access to Senator Grassley's account. Is that correct?

Mr. ZATKO. Based upon what I saw, technically, yes.

Senator KENNEDY. Okay, and if they go into Senator Grassley's account, if an engineer does, for example, Twitter doesn't know that that engineer has done that. Is that correct?

Mr. ZATKO. It would be difficult to find the logs showing that is my understanding. Correct.

Senator KENNEDY. Okay, so you don't have a log in and log out system?

Mr. ZATKO. There was not an easy ability for me to find which engineers had logged into which systems, and what data that they had accessed.

Senator KENNEDY. Okay, so this engineer who can secretly go into Senator Grassley's account and get all this information—Twitter has no idea what the hell that engineer's going to do with that information, does it?

Mr. ZATKO. Under the hood, no.

Senator KENNEDY. Okay. So, that engineer at Twitter could sell it, for example, couldn't he?

Mr. ZATKO. I'm sorry. Could what?

Senator KENNEDY. Could sell it?

Mr. ZATKO. Could sell access? I've seen numerous accounts on underground forums offering to sell such access. Whether those are valid or not—but I have seen the offers to sell access to accounts, to delete accounts, to unban accounts.

Senator KENNEDY. Well, that engineer could just call one of their buddies and say, "Hey, you don't like Senator Grassley. Let me give you some information here and you may want to use it against him." Could that engineer do that?

Mr. ZATKO. With the access they have to—

Senator KENNEDY. Would Twitter know that the engineer had done that?

Mr. ZATKO. Not necessarily.

Senator KENNEDY. Okay. Now, did Mr. Dorsey know all this?

Mr. ZATKO. I did explain this to Mr. Dorsey. My understanding is he did not understand this prior to bringing me in, and that was one of the reasons that he wanted—

Senator KENNEDY. Does he understand it now?

Mr. ZATKO. I believe after seeing this hearing—

Senator KENNEDY. How about your CEO, does he understand this?

Mr. ZATKO. I believe since he has been there for 10 years and rose up through the ranks in engineering, and he has talked to the engineers, and they have told him—

Senator KENNEDY. Is that a yes?

Mr. ZATKO. I believe yes. I believe yes.

Senator KENNEDY. How about Mr. Bret Taylor, from Salesforce? He's the chairman of your board. Does he know all this?

Mr. ZATKO. He knows what I put in my reports. I do not know whether he understands it.

Senator KENNEDY. All right, you've got an executive from Mastercard, Mimi—I'm going to probably mispronounce the last name—Alemayehou, from Mastercard. Does this board member know that?

Mr. ZATKO. I do not know if she knows that.

Senator KENNEDY. Well, is this the kind of thing that a reasonable board member would inquire about?

Mr. ZATKO. I would think so, but I've also seen that what was presented to the board was not representative—

Senator KENNEDY. Did they—during your time there, did the board ever ask?

Mr. ZATKO. The board did not ask these directly, no.

Senator KENNEDY. Even after all these problems with foreign agents?

Mr. ZATKO. Not when I was there during the board meetings—

Senator KENNEDY. They just sat there?

Mr. ZATKO. They focused on other topics and other priorities.

Senator KENNEDY. Yes, right. Dr. Li, he's a professor at Stanford. Does he know all this?

Mr. ZATKO. Same response. I did not see any questions on this specific topic while I was there—

Senator KENNEDY. Patrick Pichette, who used to be with Google.

Mr. ZATKO. Same response, sir.

Senator KENNEDY. All right.

Mr. ZATKO. Oh, Patrick Pichette? Sorry—

Senator KENNEDY. Pichette.

Mr. ZATKO. Yes, Patrick Pichette was the one who when I brought up this instance, he hit the roof. He was very upset, said, "This is—"

Senator KENNEDY. Did he fix it?

Mr. ZATKO. No, he asked for follow-up information—

Senator KENNEDY. Any why hasn't Google—and why hasn't Twitter fixed this?

Mr. ZATKO. There were other priorities.

Senator KENNEDY. It's about the money, isn't it?

Mr. ZATKO. It's about whatever crisis and the other priorities, correct.

Senator KENNEDY. To fix this would cost them money, wouldn't it?

Mr. ZATKO. It would take away focus on other projects—

Senator KENNEDY. It would cost them money, wouldn't it?

Mr. ZATKO. Most likely, yes.

Senator KENNEDY. Yes. Okay, Twitter, for a while, was going to go into the porn business. Did they do that?

Mr. ZATKO. I don't know that they did that. I didn't know that they were going to go into the porn business.

Senator KENNEDY. Oh, okay. Well, they were. You don't know why they decided not to?

Mr. ZATKO. I do know that there were discussions about age related information, and the discussions internally that I heard were simply concerns about lack of tools to correctly regulate or constrain it.

Senator KENNEDY. So, it wasn't a moral issue. It was they didn't—why didn't they go in the porn business?

Mr. ZATKO. I do not know.

Senator KENNEDY. Okay, sounded like you knew a little bit about it. Last question, I'll ask it quickly, Mr. Chairman. Who sets the standards for censorship at Twitter?

Mr. ZATKO. I believe that comes out of counsel.

Senator KENNEDY. Your lawyers?

Mr. ZATKO. I believe so, sir.

Senator KENNEDY. And do they talk with the board about it?

Mr. ZATKO. I have been advised out of an abundance of caution that I shouldn't comment on any Twitter counsel conversations for A-C Priv that Twitter might assert.

Senator KENNEDY. Thank you, Mr. Chairman.

Chairman DURBIN. Thank you, Senator Kennedy. Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Mr. Chairman. Thank you and Senator Grassley for holding this hearing, and thank you, Mr. Zatko, for your being here. You are an extraordinarily insightful and significant testimony here today, at substantial professional and personal risk—which is the tradition of whistleblowers—and your cooperation with me and my staff off the record in providing details that are important to our understanding. And the more of it that's made public, I think, the better. Would you agree with me that Twitter has put its users' health and safety severely at risk?

Mr. ZATKO. Yes, sir.

Senator BLUMENTHAL. And it's put the national security severely at risk.

Mr. ZATKO. Yes, sir. That was part of my disclosure.

Senator BLUMENTHAL. Its management has misled its own board of directors.

Mr. ZATKO. Yes, sir.

Senator BLUMENTHAL. And in that event, the management ought to be certainly restructured, shifted, changed. Correct?

Mr. ZATKO. Yes, sir.

Senator BLUMENTHAL. That kind of structural reform is necessary to achieve changes within the company.

Mr. ZATKO. That is my belief.

Senator BLUMENTHAL. You've also said that this company has misrepresented facts to Government agencies, especially the FTC. That's correct, isn't it?

Mr. ZATKO. Yes, that is correct, sir.

Senator BLUMENTHAL. And I think you shared in your complaint that Twitter management was intending to mislead as well French and Irish regulators about compliance with the consent decree. Correct?

Mr. ZATKO. Yes, sir. That's correct.

Senator BLUMENTHAL. How high in the Twitter management would you say that intent to mislead, and, in effect, deceive Government agencies went?

Mr. ZATKO. To the CEO. I do not know to what level inside the board. They did not know because of misrepresentation or chose not to push.

Senator BLUMENTHAL. The misleading of Government agencies is one of the reasons why stronger action hasn't been taken?

Mr. ZATKO. That could very well be, sir.

Senator BLUMENTHAL. But is also, in effect, is the result of a lack of vigor in law enforcement, whether because of inadequate resources or a failure of will.

Mr. ZATKO. That could be as well, sir.

Senator BLUMENTHAL. In fact, the most recent settlement with Twitter, which was a payment of \$150 million earlier this year. The FTC and Department of Justice stated that Twitter violated the 2011 consent decree. That's no surprise. But the size of the penalty, a mere \$150 million amounts to the kind of burden on us average drivers when we pay the toll to go into Manhattan, given that its profit in the second quarter this year was about \$1.18 billion. Correct?

Mr. ZATKO. That is correct. While I was there, the concern only really was about a significantly higher amount, significantly higher, or if it would have been a more institutional restructuring risk. But that amount would have been of very little concern while I was there.

Senator BLUMENTHAL. To effectively address this problem, we need not only to insist on restructuring the company, but also, likely restructuring, reforming, and energizing our regulatory apparatus. Not only as to Twitter, but also as to other internet companies and platforms. Would you agree?

Mr. ZATKO. Yes, I would. The intent of the regulators, I think, is the right intent, but it is not being followed or correctly adhered to.

Senator BLUMENTHAL. All of what you're saying—everything in your complaint, and a lot of what we've heard in this Committee and in other committees leads me to think that we need a new agency. As reluctant as I am to suggest a new Government bureaucracy, I don't think it needs to be a Government bureaucracy with a lot of new people. But it needs to be a new means of enforcement here to bring cases to the Department of Justice, focusing on privacy, security, and protecting users, as well as our national security. Would you agree?

Mr. ZATKO. I had not considered that. I will have to think about that. It is a very interesting approach.

Senator BLUMENTHAL. I'm not reaching any conclusions, but clearly what we're doing right now is not working. You would agree with that?

Mr. ZATKO. Yes, what I have seen, the tools that are used out of the toolbox are not working. I do believe other tools in the toolbox do work, but the regulators aren't able to quantify and get measurements that would show them to switch to the other tools they have.

Senator BLUMENTHAL. What are the remedies that, for example, other countries have that enable them to better protect privacy?

Mr. ZATKO. Some are simply much more aggressive and do not accept answers at face value, put very strict time constraints on re-

quiring answers, require data to back up the answers, and threaten to preclude monetizing entire markets, such as maybe you won't be allowed to monetize in France or maybe you won't be allowed to use particular data source in France. You know, and you have a week to respond, sort of approach.

Senator BLUMENTHAL. And let me just finish on that note. To expand on the Upton Sinclair theory of the case here, essentially users and their information are Twitter's product. They are the means to monetize the eyeballs on the site; to collect, use, and monetize that information is the Twitter business. And so, their reckless disregard for their users' health and safety and for the national security is a product of that incentive. Would you agree?

Mr. ZATKO. Yes, sir, and that's why I understand the M in mDAU to be monetizable daily average users.

Chair DURBIN. Thank you, Senator Blumenthal. Senator Blackburn.

Senator BLACKBURN. Thank you, Mr. Chairman. Thank you for joining us today. I'm a mother, and a grandmother, and I want to talk with you about this process Twitter has gone through. They tried to start a new subscription based adult entertainment section. Are you familiar with that?

Mr. ZATKO. No, ma'am, I'm not.

Senator BLACKBURN. You're not, okay. Well, they had to scrap the plans because an internal team found that they had too much child and nonconsensual pornography that was on their site already. Are you aware of that?

Mr. ZATKO. No, ma'am. Unfortunately, it does not surprise me.

Senator BLACKBURN. Okay, well, there's a Federal court case right now against Twitter because the site repeatedly refused to take down tweets of children as young as 13 and 14 performing sex acts in photographs and in videos. And these were posted by sex-traffickers who were impersonating a teenage female. So, my question is why, what—for what reason would Twitter refuse to take down this sexually explicit content, if it knew that it was affecting underage children, why would they leave this up? And why would they refuse to take this down?

Mr. ZATKO. From what I saw on the area of adult content, because that was brought up, and our concern was certain advertisers didn't want adult content to appear next to ads they were putting. And that was a concern inside the company. The lack of—

Senator BLACKBURN. They had a monetary concern, but not a moral concern?

Mr. ZATKO. They had—there was a—I can't speak to the morals of the people internally, but there was a concern whether or not they could even correctly identify and get ahead of this, because they lacked the basic tools and the resources in those teams, and it would have to be in a reaction after things were posted and maybe brought to their attention—

Senator BLACKBURN. All right, so, what do they do to police this sexually explicit material, especially when it pertains to children?

Mr. ZATKO. Unfortunately, that was not under my area, so I don't have information to talk specifically to that.

Senator BLACKBURN. So, there's not a standard operating procedure to block this, to pull it down?

Mr. ZATKO. I believe they do have—or I was told that they have some voluntary self-tagging and self-reporting of whether you were an adult content account, but I'm not aware of any of the other processes or procedures in the company.

Senator BLACKBURN. Let me ask you about the FTC. Senator Blumenthal was just asking you about that. Did you ever participate in calls or meeting with the FTC, in which you heard specific misrepresentations made by Twitter?

Mr. ZATKO. No, ma'am. I was not in the calls. I got briefings—

Senator BLACKBURN. So, you had no direct knowledge?

Mr. ZATKO. Well, I got direct briefings from the people who were in the calls telling me what they did.

Senator BLACKBURN. All right. So, it was all second-hand.

Mr. ZATKO. Correct, from the people involved in the calls.

Senator BLACKBURN. Okay, did the FTC come to Twitter and identify specific conduct or representations that concerned them?

Mr. ZATKO. That would be a question that you would have to ask the chief privacy officer, who would have been the recipient of those outreach.

Senator BLACKBURN. Okay, let me ask you about the issue of click-through ads, because I know that many times that our adversaries will, through a company in China, specifically, the CCP will be part owner of a company. So, they use click-through ads to gain access to platform user data, including China, including other adversaries, and including places where Twitter is blocked. And they are finding ways to evade the tracking and to get into these networks. In your experience, is this a typical practice that happens at the global tech platforms?

Mr. ZATKO. Click-through ads do expose a risk that non-click-through ads do not. If you can get a user to click through, you get the information that I was describing before, the IP address, the browser. From the IP address you can determine the IP geolocation or if they're using a VPN or not, if that is allowed in your country. And then you can further interrogate that person's computer or get them to provide more information maybe that they don't know that they're providing directly to you, thinking that it's an ad on a service.

Senator BLACKBURN. Could this be remedied in anyway? And Senator Klobuchar talked to you about this, a national privacy standard. If we had a national privacy standard, would that help to secure an individual's information online and would it help in any way, in policing these click-through ads?

Mr. ZATKO. I think addressing, in general, the difference of the information, or making people aware, and then providing a context around when a user knows if they are providing information and what information they are providing no longer to the service they thought they were interacting with could definitely benefit a user.

Senator BLACKBURN. I want to ask you one thing about censorship. And during your time at Twitter, did you participate in any conversations or meetings where content moderation decisions were made based on a poster's political views?

Mr. ZATKO. I never investigated or heard of decisions on that particular topic. I was focused on the crisis and fires in the areas of my domain.

Chair DURBIN. Thank you, Senator Blackburn.

Senator BLACKBURN. Thank you.

Chair DURBIN. Senator Coons.

Senator COONS. Thank you, Chairman Durbin, Ranking Member Grassley, and thank you, Mr. Zatkan. Thank you, Mudge, for coming forward. This is yet another eye-opening moment for our public, for our Nation, and for this Committee. We know that social media and new communications technologies have empowered people across the world to connect and share information at an unprecedented scale. But we also know that concentrating all this information, all these resources, in just a few hands comes with great risks. So, your whistleblower complaint contains really striking allegations, which shed light on several key realities, and I wanted to focus on those. The first, as you've stated in a number exchanges with my colleagues, is that the public lacks any credible way to assess whether and how major platforms and technology companies are protecting or prioritizing user privacy. And I want to talk for a bit about a bill that I've got that Senator Klobuchar also mentioned would help strengthen some of that transparency. And then the second, which I'll get to later, is that these platforms are a target for foreign actors, something where a Subcommittee I chair is having a dedicated hearing tomorrow afternoon.

You commissioned an independent report regarding Twitter's platform integrity, and their ability to combat misinformation, disinformation, and that report found, and I'm quoting, "Twitter's consistently behind the curve in acting against disinformation and misinformation threads," and that, "Twitter doesn't have the ability to measure the impact of its work to protect site integrity." What I've concluded from your testimony today is that Twitter lacked the ability to measure the effects of interventions it implemented because of decisions by management, and because of the lack of a credible, regulatory oversight agency and penalties. Is that correct? Do I understand your testimony correctly?

Mr. ZATKO. Yes, sir. The inability internally came from 10 years of security and engineering that just kept accruing.

Senator COONS. And your complaint also details how Twitter's executive team was concerned that the report that you'd commissioned would be damaging if it got out, and that they worked to intentionally remove or modify information that might be especially embarrassing for Twitter. Is that correct?

Mr. ZATKO. Yes, sir. I found that very disturbing. The company that I hired, with the knowledge of the other executives and the head of site integrity, which did not report to me, but that this independent organization was going to analyze and do gap analysis. The company reached out to me and said, "Hey, Mudge, Twitter is jumping in and making us open a separate contract and telling us not to provide you the results to your own work—to your own work. This does not feel right to us. What's going on?"

Senator COONS. So, a lot of the information that both regulators and Congress relies on when considering how to regulate social media companies comes from the companies themselves. As I think

you put it before, they're essentially grading their own homework. So, the conclusion that we ought to reach is that the information that we receive isn't trustworthy, from some social media platforms.

Mr. ZATKO. Yes, sir. That's what I experienced.

Senator COONS. So, I've released a bill with Senator Portman, Senator Klobuchar, referenced earlier. We are looking for additional Republican cosponsors. It's called the Platform Accountability and Transparency Act. It would allow external researchers to look at exactly these kinds of problems, to better understand and analyze the algorithms that drive social media and some of their practices. Would empowering researchers and mandating better disclosure help hold companies more accountable and cause them to invest more resources in site integrity?

Mr. ZATKO. Yes, sir. In fact, I think one of the things we learned from that study, and what I am hopefully shedding light on in my lawful disclosures is just how much a gap there is between Twitter and some of Twitter's peers. And even learning that sort of discrepancy would help understand and raise the level of hygiene for these organizations and their ability to perform their tasks, and the ability for us to accept what they're saying, as to whether it could possibly be true or not.

Senator COONS. This also opens up enormous national security risks, as you testified earlier. There's roughly half of Twitter's employees that had unnecessary access to vast amounts of sensitive user data. Senator Kennedy was asking you earlier, just give us a quick sense of what information Twitter might have about Senator Grassley, or about any of us on this Committee. And it is deeper and broader, and I suspect if you'd gone further, it then unlocks a whole profile that can give really dramatic insight into members of law enforcement, members of military, Members of Congress, and their families, their travel, their preferences, their actions, their consumer activities. All of that has some real consequences. You wrote in your complaint, the India government forced Twitter to hire India government agents, who then had direct and unsupervised access to data. And a former Twitter employee was convicted last August of working as an agent of the Saudi Kingdom. How common do you think it is for foreign entities, for hostile agencies to successfully install sympathetic actors at Twitter and why might they do so?

Mr. ZATKO. Well, there's any number of reasons. You know, there were many of reasons why you would do so, in particular, to not just to identify people of interest, or track groups of interest, but also to look at whether or not Twitter has identified your agents, or your information operations. What other governments has Twitter possibly identified? And remember, you know, outside of the ability to access large amounts of data on the engineering side, you would want to know what Twitter's plan is, as far as whether they will cede to your demands for control of information within their environments or not, in order to change different types of political pressure, such as strong-arming. And as we saw, that country was even threatening to put Twitter employees in jail if Twitter didn't change particular activities on the platform.

Senator COONS. With 80 percent of Twitter users outside the United States and with Twitter having a deep access in resources to critical leaders in our country and other countries, I think this is genuinely concerning. Tomorrow afternoon, the Subcommittee I chair, Subcommittee on Privacy, Technology and the Law, Senator Sasse and I will be holding a hearing on how to further understand the depth to which hostile actors and adversaries are going to obtain American citizens' data, and that will expand on a lot of the topics we've pursued today. I hope Members of the Committee will attend. I want to thank you for your testimony and Mr. Chairman, for the chance to participate in today's hearing.

Chair DURBIN. Thank you, Senator Coons. We're going to take a 5-minute break after Senator Cotton asks his questions. Senator Cotton.

Senator COTTON. Thank you, Mr. Zatzko, for your very informative testimony this morning. I want to start with some questions about Twitter's censorship policies. I know you weren't at Twitter for most of 2020, but I want to start with an example from June 2020, specifically, me. As left-wing street militias were rioting and looting in our streets, I posted on the website that the National Guard and even the active-duty military have been used to stop such rioting in the past, most recently in 1992 in the LA riots. Within a couple of hours, a low-level employee at Twitter's national office contacted my staff and said that if I did not delete that tweet that my account would be permanently locked. My staff worked with this low-level employee, calling her on several occasions, because she seemed very reluctant to put anything in writing in an email.

They documented the accuracy of my comment and gave examples of how other elected officials have used similar language. The 30-minute window passed. My account was not locked. Ultimately, she said that Twitter would not take any action about my account. As I said, I know it was before you began at Twitter, but from your experience, would a low-level Twitter employee typically have the authority to permanently lock the account of an elected Member of Congress?

Mr. ZATKO. From my experience, they should not have the authorization to do it, although it would probably be a low-level employee that would be instructed to do it.

Senator COTTON. So, she was likely taking direction from more senior officials at the company.

Mr. ZATKO. Not knowing the situation, I can't comment on this specific one, but that is the sort of activity that I would see there. And I can concur that I did notice some reluctance to put a lot of things in writing on particular topics.

Senator COTTON. I noticed that in the emails that Mr. Agrawal sent to you, he seemed very reluctant to put things in writing, or made statements about what he was going to verbally express to the board, and yet he apparently did not express those things.

Sticking with the censorship, again like I said, I know you weren't there in the lead up to the 2020 election, but once you arrived, just a couple days after the election, you selected an outside company to do an evaluation of Twitter's censorship policies. The report that you commissioned found that Twitter's content controls

are “ad hoc” and “informal.” Those are two direct quotes. And the policy decisions behind it are made mostly by a small group of Twitter staff at San Francisco, quote, “frequently during a time of crisis.” Is that accurate?

Mr. ZATKO. I didn’t hire them to do a report on censorship, but that was the Platform Manipulation Organization, and yes, how you cite the report as what they found on that team is correct.

Senator COTTON. When it says frequently in time of crisis, what type of crisis was the report referring to?

Mr. ZATKO. I believe the report also said—and this is from what I experienced—if something was brought up in the media, if the Government brought it up, if somehow it became publicly aware, or if there was, you know, an ongoing outage to the system or some active disruption or crisis.

Senator COTTON. Thank you for that. Because the report does go on to say that according to Twitter employees interviewed, Twitter usually censors information, quote, “only if it is flagged by reporters or news headlines, partners—which it means to include—academic organizations and other social media companies or political officials,” end quote. So, does Twitter have special channels of communication with fellow social media companies like Facebook to discuss so-called misinformation?

Mr. ZATKO. If they do, I believe that they would be ad hoc. I am not aware of official ones. That would not have been within my organizations.

Senator COTTON. Okay, what about other so-called partners, like pharmaceutical companies or advocacy groups?

Mr. ZATKO. I am not aware of those. Again, that would be out of counsel or other organizations.

Senator COTTON. So, saying ad hoc, you think in these cases, say an executive at a pharmaceutical company that doesn’t like what’s being posted on the website or a left-wing activist at a Washington think tank would just use pre-existing relationships to contact someone at Twitter on an ad hoc basis?

Mr. ZATKO. I do not know.

Senator COTTON. Well, how can they— how can they coordinate if they don’t have some kind of channel of communication set up?

Mr. ZATKO. In the report that was an attachment from the organization, they talked about disinformation operations, which I do believe my understanding was that the site integrity team spoke with other organizations and with other social media companies about ongoing disinformation or platform manipulation. I do not know anything beyond what was in the report for that topic.

Senator COTTON. You said something earlier. I just want to come back to it. This isn’t an exact quote, but I want to give you a chance to elaborate a little bit. It was something along the lines of, “If you don’t have a foreign intelligence officer inside Twitter, you probably aren’t doing a very good job as an intelligence agency.” Is that close enough?

Mr. ZATKO. Yes, that’s close enough, sir. I worked for the Government. I held a high-level position. I worked running research and development and programs for the Department of Defense and Intelligence Communities. And from my interactions with these people in these organizations, Twitter would be a gold mine from my

understanding, from the people in the community who focus on foreign intelligence organizations and assets. If you placed somebody in Twitter, as I believe—as we know has happened, it would be very difficult for Twitter to find them. They would probably be able to stay there for a long period of time and gain a significant amount of information to provide back on either targeting people, or on information as to Twitter’s decisions and discussions and to the direction of the company.

Senator COTTON. Does that include in Twitter’s U.S. offices versus overseas or is that distinction immaterial given the way Twitter functions?

Mr. ZATKO. I believe that’s immaterial into both.

Senator COTTON. Thank you.

Mr. ZATKO. My pleasure, sir.

Chair DURBIN. Thank you, Senator Cotton. We’re going to take a 5-minute break and return to Senator Whitehouse.

[Whereupon the Committee was recessed and reconvened.]

Chair DURBIN. Resuming the hearing. Senator Whitehouse for questions.

Senator WHITEHOUSE. Thank you very much. Mr. Zatkan, I just wanted to follow up a little bit on the repeated suggestions that you’ve made in your testimony that the cybersecurity vulnerabilities will expose the United States to risks and to attacks and that Twitter security failures threaten the country’s national security. Good with that?

Mr. ZATKO. Yes, sir.

Senator WHITEHOUSE. Okay, so, I get hidden ad buyers. We saw the same thing with Facebook when they were taking ads with the payments denominated in rubles and not bothering to figure out that there might have been Russians behind those ads. And you’ve mentioned concerns about hidden Chinese ad buyers. But if we could talk a little bit more about the national security risk associated with, for instance, the unregistered Saudi foreign agent who worked at Twitter, or the pressure to hire Indian government agents. Walk us through a scenario of how an individual planted in Twitter like that could create a national security risk for the United States. And if you would, make particular reference to the fact that—at least when I use Twitter, I’m sending stuff out. It’s intended to be public. So how, in that environment, can a foreign agent create national security risk of any significant nature?

Mr. ZATKO. Yes, sir. There are several aspects to that. There’s the nonpublic information that we’ve spoken about earlier today, your location, your phone number, your email address, things that aren’t advertised to the world. In fact, I believe 200 million—if you want to say regular users, not necessarily from a national security standpoint—Twitter in 2020 internally assessed that they lost information on 200 million users for email addresses, phone numbers, other information like that. This is the information that you need in order to start taking over other people’s accounts. With your phone number and an email address, I can hijack your phone number. I can then change your Gmail, your Coinbase, your Ameritrade, your other accounts. I can cause financial harm that way. I can then assume your identity.

But more importantly, I probably want to be able to understand your whereabouts, your network, and understand—well, I'll give you an example in foreign governments, a concern, and then we can apply that to the United States. There were requests for information about members in the farmers'—at the farmers' protest. There might be organizations or groups in the United States where once I know your home address and your home phone number, I can approach you in real life. I can put pressure on you. I could possibly recruit you. You can be a witting or unwitting accomplice, and then I could influence you or target you for influence operations in the real world.

Senator WHITEHOUSE. Let me just offer the thought that my home address, phone number, and email address are pretty widely known, and indeed in the public domain. So, how does Twitter access to that information—is there more or what's the difference between being able to look me up in the phonebook and having Twitter access to that information?

Mr. ZATKO. Having been in the public sector myself, yes, a lot of my information became known. There's also a lot of people who are in particular roles where that information is not known. And the targeting of them, perhaps staffers, perhaps aides, perhaps people around you influencing to build that network, which we have seen within, not Twitter, but which the U.S. and the Intelligence Communities have seen as part of the great game in the Intelligence Communities and world.

Senator WHITEHOUSE. Okay, so just play that out for me a little bit more, given that so much of this information is available through other channels. What would the end game be for let's say a foreign government seeking to put that kind of pressure on somebody who could make presumably make a difference or a decision to the benefit of the foreign country?

Mr. ZATKO. Perhaps identifying a relative, a family member, a colleague, who is in financial issues or has other elements that can be leveraged against them to help them influence you in a particular fashion, without your awareness.

Senator WHITEHOUSE. So, somebody would be able to create a sort of a family or personal network around an individual Twitter user and extract information about folks in that network?

Mr. ZATKO. That is one particular aspect that Intelligence Communities are—

Senator WHITEHOUSE. How would that—how would that take place through the—if somebody's gotten into the Twitter system, how do they find that out?

Mr. ZATKO. Well, it might be used in combination with other data collection sources. For instance, one of the concerns of U.S. people traveling to other countries is was their information in the OPM data base and can that information be cross-indexed against the health care industry data bases that have been lost. Do we know that this person has a particular political bias on Twitter and start to tie all of these things together for people of influence or access within governments or within sensitive positions?

Senator WHITEHOUSE. Thanks very much. My time is up.

Chair DURBIN. Thank you, Senator Whitehouse. Senator Graham. I'm sorry. Senator Cornyn.

Senator CORNYN. Mr. Zatkan, I want to explore just in the next 6 minutes the kind of data that is available on American citizens that can be used for appropriate or inappropriate purposes. You're familiar with the concept of ubiquitous technical surveillance, aren't you?

Mr. ZATKO. I can understand those words together and get the general context I believe, sir. Yes.

Senator CORNYN. Basically, all of the cameras that are publicly posted, data on your smart phone, you've already talked about geolocation data, the type of transactions you engage in. Where your home is, how much you paid for it, even Google Earth may have taken a picture of your home or your place of business. So, there's already huge volumes of data available for whatever purposes. Even above and beyond what social media collects, correct?

Mr. ZATKO. Yes, sir. There is a lot of information about a lot of us in many different ways available through technology right now.

Senator CORNYN. And I dare say, I bet most Americans just can't fathom the volume of data, and that's without even getting to things like social media. For example, in 2015 I think it was, there was a hack of the Office of Personnel Management records. I think it was 22 million records of Government employees, including their applications for security clearances was hacked, reportedly by the People's Republic of China. And then if people decide that they want to figure out their family ancestry, and use one of the DNA testing companies, my understanding is many of the testing—much of the testing is outsourced to places like China, where obviously it's not secure from Chinese government access. And so, when we're talking about the privacy concerns of Americans, this is—this is not just limited to platforms like Twitter and social media. Correct?

Mr. ZATKO. That is correct, sir. I was informed that I was in that OPM data base and that my information and my security clearance information was collected as well.

Senator CORNYN. And turning to Twitter, you've already talked about the lack of what I would call protection from insider threats in the Intelligence Community. If you're working in the Intelligence Community, they have logging protocols that will determine who accesses what information, correct, so that it can be audited later on to determine whether there had been inappropriate access. That's the sort of protocols or mechanisms that were not available at places like Twitter when you worked there. Correct?

Mr. ZATKO. Yes, sir. Correct.

Senator CORNYN. And so, anyone who could get access to that information, could on top of all the information that I asked you about earlier, outside of social media, if you look at the cumulative data picture, is that the kind of information that foreign governments like the People's Republic of China are regularly accessing for their purposes?

Mr. ZATKO. I can't say whether they are regularly accessing. I don't have that direct information. I have been—I am aware that some people in organizations have gotten very good at cross-indexing across very large amounts of data collected on numerous people from various sources, OPM, medical, etc. Twitter would be a very decent contribution to that multi-source collection.

Senator CORNYN. And that's where things like artificial intelligence can come in to comb or mine vast sources of data for more targeted or narrow purpose. Is that right?

Mr. ZATKO. The ability to collect and mine, yes, has been augmented by modern AI techniques.

Senator CORNYN. So, there are what I would call defensive concerns about people or individuals or government's access to your personal data, but there are also offensive concerns as well, and that's where the issue of disinformation, or a term that became popular—popularized during the 2016 aftermath was active measures. These are efforts by foreign governments, perhaps foreign intelligence services to actively create a narrative or a message that is essentially propaganda by this foreign government that can be used to try to influence American public opinion. Is that accurate?

Mr. ZATKO. Yes, sir. Not just America, that has happened worldwide, such as Myanmar and in 2018, Facebook acknowledging that the disinformation campaigns on their platform contributed to genocide.

Senator CORNYN. And as you pointed out earlier, it is not—when you're looking at the data that is available on each one of us as American citizens for whatever purposes, for good or ill, there's also a lot of information about who we interact with, right? Something—in the Intelligence Community sometimes they talk about pattern of life. Maybe you'd want to talk about a network of friends and associates, family members and the like, from which inquiring minds could obtain additional data about us.

Mr. ZATKO. Yes, and to your point, information operations are of a concern. Twitter acknowledges that they do happen on their platform. They have disclosed numerous ones, and they are aware of others that are ongoing.

Senator CORNYN. I'm aware that TikTok, which is a Chinese company, I believe, and even Instagram, which is owned by Facebook, have 13-year-old age restrictions in terms of their terms of use. But there's no limitation on people's ability to pretend to be an adult, to pretend to be somebody that they're not and gain access to social media accounts, and to use it for whatever purpose that they wish.

Mr. ZATKO. I can't speak to TikTok or Facebook. I'm not familiar with their internal technology for age gating. I do know that that was a challenge at Twitter, and from what I was told, the majority of age gating was voluntary, self-reporting of what your age was.

Senator CORNYN. And finally, can you tell me—do you have recommendations based on your 30 years of experience in terms of data security and what sort of regulations or laws that Congress and the Federal Government should consider passing? We don't have time to talk about all those here today, but we'd certainly welcome any of your recommendations and insights. Do you think this needs to be an area where the Federal Government needs to be actively engaged?

Mr. ZATKO. Yes, sir, I do. I'd be happy to supplement my—my written report.

Senator CORNYN. Thank you.

Chair DURBIN. Thank you, Senator Cornyn. Senator Hirono.

Senator HIRONO. Thank you, Mr. Chairman. Thank you for coming to testify, Mr. Zatko. Your testimony and all of your responses to the various questions we have asked you says to me that this situation regarding data security and national security issues with regard to Twitter is massive and that Twitter is not doing very much to be helpful at all. In fact, there are major disincentives to Twitter doing anything to spend the time or the resources to address the concerns that you raise.

So, for example, the FTC, very out resourced with regard to try to keep Twitter under any kind of even a consent decree that was entered into back in 2011. And more recently, they're contemplating making Twitter pay \$150 million for some misuse of information. One hundred fifty million dollar fine for a multi-billion dollar company is nothing, to provide any kind of incentives for them to change what they're doing. And yes, there is information out there from so many different sources, including our appliances and cars and everything else. However, Twitter is a huge, single platform where one can access information. So, who is going to force Twitter really to do anything? If we were to adopt some of the legislation that's contemplated, if we don't have an agency that can implement and enforce that law, then we are back where we started from. So, what is it going to take to force Twitter to change its ways?

Mr. ZATKO. Well, this starts at the top of Twitter, and you need an executive team that is willing to go in and say—you know, the executive teams themselves acknowledged, and I heard them say, "We have 10 years of unpaid debt here, that at some point we really need to get ahead of." They need to prioritize that. And to my understanding, a board's primary role is to make sure the right executives—executives are in charge of the company, the CEO in particular, to make sure they are, you know, sending the company in the right direction. This needs to be a long-term incentive rather than short-term incentives for the companies, because the short-term incentives just mean that they're going to tactically run from fire to fire and not actually pay down debt for a long-lived valuable company.

Senator HIRONO. So, your description of Twitter though, is they're mainly focused on the short-term monetary incentives. Who's going to force them to look at the long-term? Do people need to go to prison? I mean, what do we need to do to get Twitter to—from what you're telling me, they cannot even identify foreign agents in their midst.

Mr. ZATKO. Yes, ma'am. And you know, to be blunt, some foreign agents would probably be pretty good and difficult to identify, but some were, in this case, not. And they're only, to my awareness, being identified when they are brought to them. They're not even attempting to—I think—I think holding people accountable is a good start. I think that is something that people are concerned of. But what—you can only hold people accountable if you can measure and quantify what their targets are and what changes need to happen. And if you say, such as what I saw, you know, Twitter needs to have a mature software security program, or security program. That's a very ambiguous and qualitative term. So, holding accountability and setting quantitative goals and standards that

can be measured and audited independently, I believe, is what's going to be required to change management structures and drive change in companies when it's needed, such as this.

Senator HIRONO. So, we don't even have the kind of standards to which we can hold Twitter accountable to. Is that right?

Mr. ZATKO. From what I saw, they were able to be answered in the affirmative without actually meaningfully making—the intent of the regulators was correct. But you could then say, “Yes, I've done this,” hold up an isolated example, and allow somebody to assume that that example was the whole environment, knowing that you're misleading—

Senator HIRONO. Excuse me. So, do French regulators have better standards to which to hold Twitter accountable to?

Mr. ZATKO. My understanding is that one of the reasons that the French CNIL is more feared is that they dig in technically and go toward more quantitative results that are less easy for organizations to sort of wordsmith around in their response and answers.

Senator HIRONO. Yes. I think that's something we can learn a lesson from. More specifically, are you sure that you discovered Twitter compromises its user data long after the users close their accounts? In fact, you stated that the accounts are simply deactivated while the data is not fully deleted. At the time of your departure from Twitter, was the company—was that the company's continuing general practice? They don't really eliminate the data?

Mr. ZATKO. Yes, I was told straight out by the chief privacy officer that the FTC had come and asked, “Does Twitter delete user information when they leave the platform?” And the reason this person told me this is he said, “I need you to know this, because other regulators are asking us, and this ruse is not going to hold up. So, instead of answering whether we delete user data, we intentionally have replied, “We deactivate users and try to side-step the program, because we know we do not delete user data and cannot comply with that if they demand us to.”

Senator HIRONO. You would think that that would be something that they could do technically, to be able to delete data, because for the users, to deactivate your account means that there should be nothing there of your account information, so, isn't there something technically that they could do?

Mr. ZATKO. This goes to one of the fundamental root problems I mentioned in my opening oral statement, which is they would need to know what data they have, where it is, and why they got it, and who it's attached to in order to do that. If they did that, which should be a fundamental expectation that I would have as a user, yes, at that point they could absolutely delete the information.

Senator HIRONO. Thank you.

Senator OSSOFF. [Presiding.] Senator Graham is recognized for 6 minutes.

Senator GRAHAM. Thank you very much for coming to the Committee and giving us your insight. Something good will come from this. Do you believe that?

Mr. ZATKO. I hope so. I'm basically risking my career, and reputation, and if something good comes from this 5, 10 years down the road, it will have been worth it as a sacrifice.

Senator GRAHAM. And you're willing to take that risk because it's that important to you?

Mr. ZATKO. Yes, I've been doing this for 30 years. People who know me in the industry know that, you know, I'm willing to put it all on the line, hoping that we can improve things.

Senator GRAHAM. Well, I'm going to work with my Democratic colleagues to make sure this is not in vain. Let me ask you a question. Do you still use Twitter?

Mr. ZATKO. I still have an account on Twitter. I still read it occasionally. I have not tweeted since I've left.

Senator GRAHAM. Given what you know, would you recommend that all of us continue to use Twitter, or should we take a time out?

Mr. ZATKO. I think Twitter is a hugely valuable service. It really shapes people's—

Senator GRAHAM. So, no matter what you've said today you're okay with the rest of us still tweeting?

Mr. ZATKO. I think people should look at the information they're getting off of it differently, and I think people should put pressure on Twitter and ask questions from the public and from the Government and regulators—

Senator GRAHAM. You're not asking to shut them down. You're asking them to get better.

Mr. ZATKO. Absolutely, sir.

Senator GRAHAM. Okay, would you buy Twitter, given what you know, if you had the money?

Mr. ZATKO. Well, I guess that depends on the price.

Senator GRAHAM. That's fair enough, but I guess the reason I asked that, you know, for the rest of us, we take what you say seriously. It's pretty unnerving. I'm going to go ahead and use Twitter, but I'll use it differently. And if nothing good comes out of this, shame on us all.

So, let me just tell you where I'm headed. There's no way to deal with this without bipartisanship, from my point of view. So, I'm working with Elizabeth Warren of all people. We have different perspectives on most everything. But Elizabeth and I have come to believe that it's now time to look at social media platforms anew. And we have this general understanding among ourselves that the regulatory system regarding social media is not working effectively. Do you agree with that?

Mr. ZATKO. Based upon what I saw, a lot of things are not working effectively. Yes, sir.

Senator GRAHAM. Okay. The Federal Trade Commission, that's the primary regulator for Twitter, as far as we know?

Mr. ZATKO. I do not believe that Twitter should be able to be viewed as in compliance—

Senator GRAHAM. Well, my point is, do you know when the Federal Trade Commission was founded?

Mr. ZATKO. No, sir, I do not.

Senator GRAHAM. 1914. A lot has happened since 1914, World War I, World War II, and an explosion of social media. Would you say, given what you know, it seems like the regulatory bodies are sort of outgunned here?

Mr. ZATKO. In Big Tech, I think they are absolutely outgunned.

Senator GRAHAM. Yes, they're like big time outgunned, and I want people to understand paying a \$150 million fine seems to be of little consequence. Is that your testimony?

Mr. ZATKO. In this case, absolutely.

Senator GRAHAM. Okay, so just imagine what I just said, Mr. Chairman. A company doesn't mind paying \$150 million and just getting back on to doing what they're doing. So, one of the things I'm trying to do with Senator Warren and others, is create a consequence for these organizations to give them an incentive to do better. Don't you think that's where we should be headed?

Mr. ZATKO. Yes, sir. I do.

Senator GRAHAM. One thing. Do you have a car?

Mr. ZATKO. Yes, sir. I do.

Senator GRAHAM. Do you have a driver's license?

Mr. ZATKO. Yes, sir.

Senator GRAHAM. Okay, if you drive a car, you need a license. If you sell real estate, you need a license. If you practice law, you need a license. If you're involved in the securities business, you need to get licensed. Is there any licensing requirement to run a social media company?

Mr. ZATKO. Not to the best of my knowledge, sir.

Senator GRAHAM. Okay, can you sue a social media company when they do you wrong?

Mr. ZATKO. I do not know.

Senator GRAHAM. Well, the answer is no. So, they're not licensed. You can't sue them. And to be shocked that we have a problem is kind of naive on our part. So, here is what I promise to you. That we're going to take your testimony, that we're going to learn from it, we're going to create a system more like Europe, a regulatory environment with teeth, an agency that came about after 1914, with the power to deal with privacy issues, content moderation. If you're going to be in this space, you have to harden your sights against foreign interference. You have to protect your sites against criminality. And if somebody takes your content down, you'll have an appeal process outside the group who did it. Does that sound kind of like where we need to be going?

Mr. ZATKO. Those all sound good to me, and I would hope measurable and transparent, and thank you, sir.

Senator GRAHAM. Well, we're headed that way with my good friend, Senator Hawley, who is going to join the Graham/Warren team. We're going to come up with a regulatory system to make sure that people in this space pay better attention, they have consequences if they don't change their behavior. It's long past due.

Would you say that the companies that we're talking about are some of the most powerful in the history of the world?

Mr. ZATKO. I don't know, sir.

Senator GRAHAM. Well, I'll say that. I will say that these companies make massive amounts of money. They're virtually unregulated. They're regulatory body was founded in 1914. They're completely outgunned. And under our law, you can't sue them when you're wronged. Having said all that, there's much value to these companies, Facebook, Twitter, Google. They add value to life. But there's a dark side. And we're going to address the dark side.

So, I will just close with this. Your testimony today has legitimized what most of us feel is a process out of control. That the regulatory environment is insufficient to the task. It's time to up our game in this country. I'm not about putting these people out of business. I'm about making them do business in a normal way and take their job more seriously. And if Elizabeth Warren and Lindsey Graham can come together around that concept, I think we're off to the races as a body. Thank you very much. What you did today will not be in vain.

Mr. ZATKO. Thank you very much, sir. If what I've done can contribute to positive change, it will be worth it. Thank you.

Senator OSSOFF. Thank you, Senator Graham. Mr. Zatkan, thank you for joining us. Mudge, thank you for joining us. I'd like to ask you about what you encountered in terms of the corporate incentives at the top of the company. Something like pushing patches in security updates to employee devices. Cyber hygiene is not easy, but that's a relatively low-cost way to mitigate a lot of risks. And there is significant risk here, reputational risk, financial risk, so, why based upon your experience working within Twitter's corporate leadership, would the company not have elected to take that step, to mitigate risk in that relatively low-cost way, or other steps like that?

Mr. ZATKO. I didn't see any financial incentives at the top levels that would then give prioritization to such efforts. In fact, I saw incentives counter to that, and combined with a culture where the company needs a crisis to operate and is driven by crises. Those didn't afford time or focus from what I saw, to do the basic security hygiene.

Senator OSSOFF. What are the basic incentives against something like patching?

Mr. ZATKO. So, it was just—so, I'll give you an example. One of the things that I was surprised while I was there, we did a media day from the executives for the street. It was the first one that Twitter had done in a very long time. It set very ambitious goals for revenue growth, goals that I was concerned that the company would not be able to hit. Not too many months after that, there was an internal value creation award presented to me, offering \$10 million if we tripled these growth goals. And I raised concerns saying, I don't know how we can do that unless we entirely cut corners everywhere. I do not like this incentive structure. How are we going to be able to devote resources to the basics, such as fixing security patching, getting the systems up to date, building a development and testing environment for all of the different functions—

Senator OSSOFF. Okay, but how is the growth incentive hostile to something like pushing software updates to employee devices? And given that that is a, as I understand it, a fundamental security practice, a basic cyber hygiene practice, why were you unable to implement a change like that. That sort of baseline hygiene practice where you'd want all employee devices to be updated to the latest version?

Mr. ZATKO. Yes, I brought that up numerous times. I was repeatedly told that, you know, 92 percent of the systems had security software. And I kept asking what is the security software report-

ing? It took me a month plus to get the truth that 30 percent of the systems were not—they had turned off software updates. There was a culture of not reporting bad results up, only reporting good results up, because that was the internal incentive structure. You were rewarded based upon relationships and how you performed in an emergency, not for identifying existing errors and doing the groundwork for keeping the lights on and running the business. My inability to find such basic information was disturbing.

Senator OSSOFF. So, you couldn't get the authorization, for example, to implement an MBM system, or some system to push patches out to user devices, or you just couldn't work the bureaucracy to make it happen?

Mr. ZATKO. I had the authorization. I couldn't get the real information, because people were misrepresenting to the executive team and the executive team was then further misrepresenting only good news and incorrect news to the board. So, it took me several months to start going and getting ground truth, and to find out that this had been a culture of only present good and positive reports up. And that's how you move forward in the company.

Senator OSSOFF. Okay, let's talk about the data, much of it, no doubt sensitive, within Twitter's possession, and some of the most alarming aspects of your disclosure and testimony is that the extent to which Twitter may not know what it has. What would—and, of course, you don't know what you don't know, but what would be an example of the kinds of data sets that Twitter might possess, but not fully understand it possesses, and what would be the mechanisms, other than monitoring user activity, by which it would have accumulated such data?

Mr. ZATKO. Sure. One example, I was surprised to see that in an internal incident review in 2020, 50 million Twitter employees' information had been exposed. And that number confused me because Twitter doesn't have 50 million employees. Twitter has all of the information of all past employees, contractors, and other users, because they haven't deleted that data. They've kept that data in that system, and those systems when they are exposed, expose that information. That was surprising to me. I'm sorry, what was the second part of your question, sir?

Senator OSSOFF. No, that's helpful, and I'm running low on time, so I want to get to this next point. And I know some of my colleagues have covered it, but the risks associated with targeted advertising, whether for the purpose of inducing targeted users to click on links that could then harvest data about their devices or their web use or their location. Or possibly inject malware or for targeted influence campaigns. Can you please talk about what you observed and what you view to be the risks associated with the advertising model and the capability of enterprise clients of Twitter's to target ads and links to specific users?

Mr. ZATKO. Yes, so that area wasn't specifically my domain. That was under the executive of sales engineering. The parts that I believe are relevant were not only the additional report that we talked about earlier with the information operations, but I did see that data sets internally to the organization when I first joined, thousands of users had access to the advertisers' information, including their bank accounts and routing numbers. And when I first

joined, people could change that information, and you could understand why changing the banking account information of a company such as Apple or Nike might be problematic.

Senator OSSOFF. Final question, and then I'll yield to Senator Hawley, and I'm going to follow up with you on this one for the record as well, to get as much detail as possible. But what records, documents, or technical information, with as much specificity as you can muster right now, would you suggest that the Congress should seek from Twitter, to understand the extent of the alleged lack of security practices, but also what data may have been exfiltrated when and by whom, what the level of national security risk might be? What should we be seeking from this company so that we can assess the level of risk and the threat and make policy accordingly?

Mr. ZATKO. Yes, sir. I submitted, I believe, 100 plus pages in my disclosure, with data, talking about the sources of that data and providing a road map for investigators. I will do it a disservice trying to summarize the large numbers of sources and locations of that data. But hopefully, my lawful disclosures provide that road map, and I am happy to follow up—

Senator OSSOFF. Okay, we'll review it, in full, and send you any follow-ups.

[The information appears as a submission for the record.]

Mr. ZATKO. Yes, sir.

Senator OSSOFF. Thanks for your testimony. Senator Hawley, for 6 minutes.

Senator HAWLEY. Thank you very much, Mr. Chairman. Mr. Zatkan, thank you for being here. Thanks for your testimony.

Mr. ZATKO. Thank you.

Senator HAWLEY. I want to just make sure I get this straight. You stated today, and in your report, that about 4,000 Twitter employees are classified as engineers. Is that right?

Mr. ZATKO. Yes, sir. At the time, half of the employees—I believe there was 7,000 plus full-time employees.

Senator HAWLEY. Got it, and that means that these 4,000-ish employees would have had access to live user data all over Twitter. They could access users' personal information, including their live data. Have I got that right?

Mr. ZATKO. Yes, sir. So, they would have access to the production environment. If they spent the time to meander around and look around, they would find that they could access these large troves of data.

Senator HAWLEY. Including geolocation data? Did you testify to that earlier today?

Mr. ZATKO. I know that Twitter has IP locations, and that they do use geolocation services based upon IP addresses.

Senator HAWLEY. Wow, 4,000 employees with access to that data. That's extraordinary. So, those employees would be in a position then, if they wanted to, to get this information and dox Twitter users. Is that fair to say?

Mr. ZATKO. That is a concern of mine. Yes.

Senator HAWLEY. Wow. That's a significant concern. 4,000 people with the ability to dox individual users who pick up the phone and use Twitter. That's extraordinary. Have you ever seen it happen?

Mr. ZATKO. I have seen numerous situations where Twitter engineers had to patch a problem and I said, "What was the problem?" And they said, "Oh, engineers could tweet as anybody." The data was exposed in this part, and it was always reactionary—and finding these wounds left and right and putting band aids on them because the systemic underlying problems were not addressed, the broad access to too much information and too many systems.

Senator HAWLEY. When you say Twitter engineers could tweet as anybody, tell me what that means.

Mr. ZATKO. That meant a Twitter engineer, understanding how the running systems and the data flows were operating, could then access and inject, or put forward information as—as I mentioned in my oral statement—any of the Senators sitting here today.

Senator HAWLEY. And have you ever seen that happen?

Mr. ZATKO. Not with the—no, not directly.

Senator HAWLEY. Not directly. Are you concerned it has happened? Do you have some reason to believe it may have happened?

Mr. ZATKO. The number of cases that were reported to me by individual engineers saying, "Hey, we found this. I'm going to try and have somebody fix it," where that was the exact problem, and we wouldn't know if it had happened in this past? Yes, I am concerned.

Senator HAWLEY. Wow. I think that's pretty significant testimony. Let me—let me make sure that I understand also just this point. A Facebook whistleblower came forward a couple of years ago now, came to me, to my office, and told us that at Facebook they at least had some policies on the books that restricted backend developers from using—from accessing user data. Now, whether or not those policies were ever followed, who really knows? But is it your testimony to me that Twitter had no similar policies in place that would have restricted these 4,000 engineers from accessing user data in this way?

Mr. ZATKO. Not technical enforced—not technical policies that were enforced. I did see basic policies, such as "Hey, you're not supposed to access inappropriate systems." But I also saw policies saying that, "Your work laptops should only run in the following setups," and I was aware that I don't believe any of the laptops were in compliance with those policies.

Senator HAWLEY. None of the laptops?

Mr. ZATKO. Based upon the policy that I read, I do not believe that any of the laptops were in compliance with that security policy.

Senator HAWLEY. Zero. Zero in compliance with their policy. That's extraordinary. Let me ask you about this. That same Facebook whistleblower told us a couple of years ago now, that Twitter's content moderation staff routinely collaborated with content moderators at Facebook and Google. Is that true to your knowledge? Do you have any information about that?

Mr. ZATKO. That would be in a team under counsel, and I wouldn't have first-hand knowledge of that.

Senator HAWLEY. Are you aware of any Twitter policies that would have prohibited coordination on content moderation between Facebook, Google, and Twitter?

Mr. ZATKO. Not to the best of my knowledge. I am not aware.

Senator HAWLEY. Okay, so it's immanently possible is what you're saying?

Mr. ZATKO. Yes, sir.

Senator HAWLEY. Let me ask you about this. Are you aware of any communications regarding content moderation with Twitter staff and the U.S. Government in your time at the company?

Mr. ZATKO. I am familiar with the conversations that happened through Department of Homeland Security, the Traffic Light Protocol, where there are messages sent out to organizations about threats that maybe the FBI or other organizations had insight into.

Senator HAWLEY. So, earlier this year, documents that we obtained from a different whistleblower at the Department of Homeland Security exposed that the Disinformation Board that the Department of Homeland Security set up, that first on the Disinformation Board's list of companies to meet with was Twitter. And they had an extensive memo, which by the way is public information now. We've released it. You can go and look at it. But they had a memo prepared with notes for this meeting with Twitter, talking about cooperation and content moderation and frankly in monitoring Americans' speech. And now we know thousands of Twitter employees have access to that. This was all in these documents. I guess my question to you is—and I know that you weren't in those meetings—but why do you suppose that the Disinformation Board had Twitter first on the list of entities to come to, to talk about coordinating and monitoring Americans' speech?

Mr. ZATKO. I can't opine on that, but I can say that Twitter is a tremendously influential platform, and we do know that there are information operations being run on Twitter.

Senator HAWLEY. Do you think it's maybe because Twitter has proved so pliant to government pressure, to censorship and monitor people? I'm thinking of, you know, first of all the Hunter Biden story. We now know that Twitter killed the Hunter Biden reporting. We know Mark Zuckerberg has said that the FBI pushed Facebook to do so. Facebook throttled it down. Twitter killed it completely, you know, locked up accounts that were trying to report what we now know was a true story. Or how about in your own report, you claimed that the Twitter CEO proposed caving to the Russian government's demands to censor content on Twitter and spy on its users. And you noted that this occurred even as you were directing employees to prepare for the Russian invasion of Ukraine. That sounds like an executive team that's pretty darn pliant to the demands of governments to weaponize, effectively, their platform to control information, to spy on its users. What's your view?

Mr. ZATKO. I wasn't there when the Hunter Biden issue happened, and I don't have any information on that. I wasn't briefed into it or involved in any of the investigations. The CEO was the CTO at the time, when he proposed to me that, "Hey, what do you think about, you know, why don't we just let Russia perform their own moderation? They're a democracy. So, why shouldn't we let them do it?" I didn't know what to think at the time. I'm sure I was a little flabbergasted.

Senator HAWLEY. Well, I think I know what to think, which is that Twitter has been all too eager to take private information from its users without telling them, to sell it and monetize it without their permission, to expose them to the worst kind of security threats, to censor them, to spy on them. I mean, you have painted a picture of a company that is not only out of control, but is truly, in many ways a malign actor. And I thank you for being willing to be here and testify. Thank you, Mr. Chairman.

Senator OSSOFF. Thank you, Senator Hawley. Thank you for appearing before the Committee today. The hearing record will remain open for 1 week for submission of materials for the record, and with that, this hearing is adjourned.

[Whereupon, at 12:25 p.m., the hearing was adjourned.]

[Additional material submitted for the record follows.]

## APPENDIX

### Miscellaneous submissions:

Whistleblower Aid ..... 60

#### Alpha Combined Files

*<https://www.govinfo.gov/content/pkg/CHRG-117shrg60055/pdf/CHRG-117shrg60055-add1.pdf>*

#### Bravo Combined Files

*<https://www.govinfo.gov/content/pkg/CHRG-117shrg60055/pdf/CHRG-117shrg60055-add2.pdf>*

KATZ BANKS KUMIN

WHISTLEBLOWER  
AID

**Written Statement of Peiter (“Mudge”) Zatko  
United States Senate Judiciary Committee  
September 13, 2022**

Chairman Durbin, Ranking Member Grassley, and Members of the Committee. At your request, I appear before you today to answer questions about information I submitted in written disclosures about cybersecurity concerns I raised and observed while working at Twitter.

My name is Peiter Zatkan, but I am often still called by “Mudge,” my online handle. From November 2020 until January 2022, I was Twitter’s “Security Lead,” a senior executive role in which I was responsible for Information Security, Privacy Engineering, Physical Security, Information Technology, and Twitter Services, the company’s global support and enforcement division.

For 30 years, my mission has been to make the world better by making it more secure. As a cybersecurity expert with over a decade of senior leadership experience, I identify and balance cybersecurity vulnerabilities with business goals. The cybersecurity vulnerabilities I deal with expose individuals, organizations, and the United States to risk and attacks that cause physical, financial, and emotional harm.

I agreed to join Twitter because I believed it was a unique position in which my skills and experience could meaningfully improve the security of users, the United States, and the world. Twitter was and continues to be one of the world’s most influential communications platforms. What happens on Twitter has an outsized effect on public discourse and our culture. I believed that improving the platform’s security would benefit not only Twitter’s millions of users, but also the people, communities, and institutions affected by the information exchanges and debates taking place on the platform.

To understand how I got here today, however, I think it is important you know about my past.

Since the 1990s, I have been a pioneer in the computer and information security field, including helping to found the responsible disclosure movement, which some people refer to as “ethical hacking.” The responsible reporting of security problems aims to inform people and institutions about cybersecurity vulnerabilities and to show them how to strengthen security.

When a responsible practitioner finds a vulnerability that bad actors can exploit, the person first makes a quiet disclosure directly to the institution, giving the affected company or government the information and the opportunity needed to fix the vulnerability. If the vulnerable institution does not want to hear the truth or fix the problem, the person reporting the problem must determine if public disclosure of the unaddressed security vulnerability is necessary to protect the public. If the benefit of public disclosure outweighs the risk to the recalcitrant institution, then the responsible practitioner makes the public disclosure necessary to alert the public to the risk and to encourage the institution to address the vulnerability.

I continue to follow this ethical disclosure philosophy and am here today because I believe that Twitter's unsafe handling of the data of its users and its inability or unwillingness to truthfully represent issues to its board of directors and regulators have created real risk to tens of millions of Americans, the American democratic process, and America's national security. Further, I believe that Twitter's willingness to purposely mislead regulatory agencies violates Twitter's legal obligations and cannot be ethically condoned.

Given the potential harm to the public of Twitter's unwillingness to address problems I reported and Twitter's continued efforts to cover up those problems, I determined lawful disclosure was necessary despite the personal and professional risk to me and my family of becoming a whistleblower.

This is not the first time I have had to deal with critical cybersecurity vulnerabilities. I have advised a sitting president, administrations of both parties, Congress, and the intelligence community on these issues. In 2010, I accepted an appointed position in charge of running Cyber Programs for the Department of Defense and Intelligence Communities at DARPA; for my service, I became a decorated civilian after being awarded the medal for exceptional public service (the highest medal able to be bestowed upon a non-career civilian by the Office of the Secretary of Defense). I then returned to the private sector and worked in senior leadership positions for companies like Motorola, Google, and Stripe, where I continued to help those companies focus on protecting companies and users from security risks.

I joined Twitter after it was infamously hacked by a group of teenagers, who launched what was then the largest hack of a social media platform in history. They took over the accounts of high-profile Twitter users as part of a crypto-currency scam. Afterward, Twitter's then-Chief Executive Officer, Jack Dorsey, reached out to me because of my unique breadth of experience in security, asking if I would join the company to assess the state of its security and make fundamental changes.

Experience, however, has taught me that making big changes to improve security is hard. And hard changes draw intense opposition from people who profit from the status quo. It was clear to me, however, that Jack Dorsey was committed to change, so I accepted the challenge. In doing so, I made a personal commitment to Twitter, the greater public, and to myself that I would do my best to drive the changes that Twitter – and its users and our democracy – desperately needed.

I have lived by that commitment.

Upon joining Twitter, I discovered that the Company had 10 years of overdue critical security issues, and it was not making meaningful progress on them. This was a ticking bomb of security vulnerabilities. Staying true to my ethical disclosure philosophy, I repeatedly disclosed those security failures to the highest levels of the Company. It was only after my reports went unheeded that I submitted my disclosures to government agencies and regulators.

KATZ BANKS KUMIN

WHISTLEBLOWER  
AID 

In those disclosures, I detail how the Company leadership misled its Board of Directors, regulators, and the public. Twitter's security failures threaten national security, compromise the privacy and security of users, and at times threaten the very continued existence of the Company. I also detail that despite these grave threats, Twitter leadership has refused to make the tough but necessary changes to create a secure platform. Instead, Twitter leadership has repeatedly covered up its security failures by duping regulators and lying to users and investors.

I did not make my whistleblower disclosures out of spite or to harm Twitter. Far from that, I continue to believe in the mission of Twitter and root for its success. But that success can only happen if the privacy and security of Twitter's users and the public are protected. Many of the engineers and employees within Twitter have been repeatedly calling for this, but their calls are not being headed by the executive team.

It became clear by Twitter's actions that the only path to achieve that outcome was through lawful disclosure. My genuine hope is that my disclosures help Twitter finally address its security failures and encourage the Company to listen to its engineers and employees who have long reported the same issues I have disclosed.

I stand by the statements I made in my disclosures and am here to answer any questions you have about them.

Thank you.

**QFRS  
Senate Judiciary**

September 21, 2022

Peiter "Mudge" Zatko  
Independent Security Consultant  
New York Metropolitan Area

Dear Mr. Zatko:

Thank you for your testimony at the Senate Committee on the Judiciary hearing entitled "Data Security at Risk: Testimony from a Twitter Whistleblower" on Tuesday, September 13, 2022. Attached are written questions from Committee members for your review and response. We look forward to including your answers, along with your hearing testimony, in the formal Committee record.

To complete a timely and accurate hearing record, please submit an electronic version of your responses to [record@judiciary-dem.senate.gov](mailto:record@judiciary-dem.senate.gov) no later than 5:00 p.m. on Wednesday, October 5, 2022.

In the case that circumstances make it impossible to comply with the time period provided, witnesses may request an extension to the above email address. Any additional questions, comments, or concerns may also be directed to this email.

Sincerely,

Richard J. Durbin  
Chair  
---

Senator Chuck Grassley, Ranking Member  
Questions for the Record  
Mr. Peiter "Mudge" Zatko  
Independent Security Consultant

Following the Senate Committee on the Judiciary hearing entitled  
"Data Security at Risk: Testimony from a Twitter Whistleblower"

on

Tuesday September 13, 2022

**1. Senator Hawley asked whether you were aware of communications regarding content moderation between Twitter staff and the U.S. government. You replied, "I'm familiar of the conversations that happened through Department of Homeland Security, the traffic light protocol, where there are messages sent out to organizations about threats that, maybe, the FBI or other organizations had insight to."**

**a. Please explain the traffic light protocol, including its purpose, the frequency of use, who sends and receives the information, and how Twitter uses the information.**

**ANSWER:**

From what I saw while at Twitter there were several communications paths with the government but none of the conversations, at least that I was aware of, focused on content moderation.

**QFRS**  
**Senate Judiciary**

The methods of communications I was aware of were:

- Legal demands, court orders, subpoenas, etc. Handled by a system called 'Zipbird'
- Communications from the US Government to US companies containing early warning of upcoming risk and security events.
- Ad-hoc communications with Twitter employees through personal/professional relationships

Zipbird was the official system and process to handle in-bound communications involving legal demands, subpoenas, court orders, etc. The procedures for making these requests are described on Twitter's website<sup>1</sup>. I am unaware of what percentage of requests were legal demands regarding content moderation. The team managing the initial handling and vectoring of inbound requests lived in Counsel's organization. There had been discussions to transition the operations aspect of Zipbird to my organization but this had not happened prior to my unexpected departure from the company.

Early warnings of near term threats and risks came into Twitter from CISA (Cybersecurity and Infrastructure Security Agency) and/or DHS. These were emails from USG agencies sent directly to Twitter employees who signed up to receive the alerts. The alerts used the Traffic Light Protocol (TLP) to indicate how the information should be handled and whether it was allowed to be shared within the company or external to the company. Twitter did not, to my knowledge, maintain awareness of who in the company was receiving these government alerts or whether these employees were corresponding with the USG bi-directionally. The Traffic Light Protocol is described in a footnote here<sup>2</sup>. At a very high level RED means no sharing, AMBER means sharing is allowed only within the company, and GREEN would mean the information in the advisory can be shared within relevant industry businesses. There was no request for content moderation to the best of my recollection.

It was also apparent that there were ad-hoc relationships with government personnel in various agencies. These were believed to be personal or professional relationships between individuals. I had laid out plans to better understand, capture, and formalize these communications to ensure they were appropriate. However this effort was immediately scrapped upon my departure. Mr. Agrawal, with 10 years of engineering work at Twitter and elevated to the position of CEO in November 2021, wanted to kill this effort even though the executive team had approved it, the approved effort had been presented to the board, and the effort had been scoped and funded. Given the range and number of suspected relationships within Twitter there was concern about whether these relationships were appropriate and what information was being shared and in which direction (i.e. inbound to Twitter or outbound to the USG). I am unaware of whether these conversations included topics regarding content moderation. However I was made aware that members of Site Integrity, the organization in Counsel with overlapping responsibility for content moderation, maintained some of these ad-hoc relationships.

---

<sup>1</sup> <https://help.twitter.com/en/rules-and-policies/twitter-legal-faqs>

<sup>2</sup> Cybersecurity and Infrastructure Security Agency, Traffic Light Protocol (TLP) Definitions and Usage, available at: <https://www.cisa.gov/tlp>

**QFRS**  
**Senate Judiciary**

**2. You told Senator Kennedy that you have seen numerous examples on underground forums where individuals have offered to sell access to accounts, delete accounts, or unban accounts. Did Twitter investigate the incidents to determine whether the individuals offering these services were employees of the company? If so, what were the results? If not, should Twitter investigate as a matter of course?**

**ANSWER:**

There are several types of Twitter access and services one can find offered for sale in underground marketplaces (sometimes referred to as the "darkweb"). There are advertisements on the darkweb offering to buy "fake followers" (e.g. paying to have a lot of bots instructed to follow your account to artificially inflate the perception of an account being more influential than it is). There are also advertisements offering to sell fake Twitter accounts. These accounts may then be used for a number of purposes (e.g. spam, scams, harassment, etc.). Such fake accounts are advertised as having already fooled Twitter's simple checks to determine whether or not they are "bots".

While both of these are of concern, the most disturbing access being sold on underground marketplaces I was made aware of was "initial access". This meant accounts or credentials that would provide the purchaser with access into Twitter's company and computers.

I believe the Senator is asking about this last class: "initial access".

To the best of my recollection Twitter was not investigating underground offerings of initial access to determine whether the offerings were real or fraudulent.

It was my experience that Twitter would prioritize resourcing and investigating issues primarily only after they had become a publicly known issue and there was negative external press.

Fixing access control, system software and configuration hygiene, and compliance (e.g. data awareness and control), would fix much of this and also make it possible to more easily identify the root of the problem instead of just the symptoms.

Twitter was not mature enough with their internal engineering infrastructure and security monitoring, nor were they staffed appropriately, to try to investigate every underground market offering for initial access (many of which would be scams, though some would likely be valid).

**3. Regarding click-through ads, Twitter appears to be aware of the increased risk to user data as compared to non-click through ads.**

**a. Does Twitter make any effort to protect users or warn users of the potential harm of click-through ads?**

**ANSWER:**

**QFRS**  
**Senate Judiciary**

I was not aware of Twitter efforts to educate or protect users from potential increased risk that may be posed through click-through ads.

**b. Does Twitter set rules for advertisers on the types of information that advertisers are allowed to collect? If so, what mechanism has been put into place to enforce the rules? If none, please explain why not.**

**ANSWER:**

Twitter's stance was that Advertisers are responsible for their ads, not Twitter. Twitter has a written policy<sup>3</sup> capturing this stance and "asking" advertisers to largely act responsibly and self-police their ads and ad-content. To the best of my knowledge Twitter did not have restrictions or protections in place to enforce safety on click-through ads.

While there are technical challenges to this problem, what I saw within Twitter was that very few people knew what information was being collected or sent to third parties in the first place. Lacking this knowledge more broadly meant it was very challenging for the company to assess threat model risks in this area even if someone had the foresight to consider these risks and concerns about the users of the platform.

**c. Does Twitter determine what data a potential advertiser may take from a user before allowing the advertiser on the platform? If not, should Twitter do so?**

**ANSWER:**

Not to the best of my awareness. I heard no mention of this in executive meetings or through my interactions with sales engineers and managers during my time at Twitter. If this was a defined concern it was not a focus that was shared with the executive team. The closest I can recall is Twitter's Ad policies document telling the advertiser what types of content is inappropriate for the service (e.g. weapons, illicit drugs, political content). This document, and largely self-policing policy, does not touch upon technical information that advertisers should limit themselves to collecting from users by way of click-through ads.

**4. Your testimony made clear that Twitter is focused on user growth, revenue, and crisis response over data safety. In your opinion, what enforcement actions, whether through Congress or federal agencies, could best motivate Twitter to shift its focus to user protection and data security?**

**ANSWER:**

In my experience one-time fines from the FTC, or any other regulatory bodies, did not meaningfully shift Twitter's focus to user protection and data security. A dedicated privacy engineering team, comprised of privacy experts, was only created after I joined. One-time fines are not viewed as impacting future revenue and hence the executive team, the board, and investors, could treat individual fines as exceptions that would not impact future projections.

---

<sup>3</sup> <https://business.twitter.com/en/help/ads-policies.html>

**QFRS**  
**Senate Judiciary**

Rules and regulations that represented continuing impact to growth, revenue, or operational tempo, were much more successful at shifting Twitter's focus. Examples include:

- ongoing fines equal to a percentage of revenue
- blocking access to a market (e.g. France, California, etc.) until the problem is corrected
- restrictions on monetizing particular data collected from users (e.g. e-mail addresses, phone numbers, etc.) until the problem is corrected
- mandating new requirements or specifications regarding how internal engineering or business functions and processes must be run going forward
- making members, or a subset of members, of the executive team and upper management have some amount of personal liability (civil and/or criminal)
- Being required to pass audits performed by external companies not paid or contracted by Twitter
- Press about Twitter describing concerns and potential ongoing fines and restrictions that are on the table for continued failure to address problems

**5. To the best of your knowledge, are there other companies, besides Twitter, that also suffer from poor data privacy controls or a susceptibility to foreign influence? If so, which ones?**

**ANSWER:**

No. Not to this degree, to the best of my knowledge.

**6. During your testimony, you cited the need for increased whistleblower protections for individuals working in the tech industry. What type of whistleblower protections do you believe are needed the most?**

**ANSWER:**

I believe that whistleblower protections should be broad and comprehensive to protect whistleblowers across the private sector. Instead of piecemeal laws that provide coverage by industry or type of wrongdoing, we need a law that will encourage all potential whistleblowers to share information, whether they come from the public or private sector, whether they are employees or contractors, or whether their companies are privately held or publicly traded. Part and parcel to this is to ensure that those protections have teeth because without it, those teetering on whether to come forward or not may elect to stay silent.

Whistleblowers who raise potential securities violations about publicly traded companies have broad protections under the Sarbanes Oxley Act and, depending on the jurisdiction, whistleblowers in the private sector who report unlawful conduct may enjoy strong protections. The federal government should consider similarly broad protections for whistleblowers in the private sector. The FTC Whistleblower Act of 2021 proposed important whistleblower protections for whistleblowers who provide information about potential violations of laws, rules or regulations enforced by the FTC.<sup>4</sup> While this law only covers reports regarding legal violations under the FTC's purview, it includes significant legal components that have proven effective in protecting whistleblowers, so I will highlight a few of those components here that I believe are especially important to include in any general federal whistleblower protection law.

<sup>4</sup> <https://www.congress.gov/bill/117th-congress/house-bill/6093>

**QFRS**  
**Senate Judiciary**

First, the legislation includes a prohibition on retaliation by the employer against whistleblowers who make internal disclosures or disclosures to a government entity. While all whistleblowers are vulnerable to retaliation, tech workers are especially vulnerable because of the wealth and power in the tech industry.

Second, the legislation protects the identity of whistleblowers by ensuring that any identifying information about the whistleblower is not subject to public disclosure. At the same time, for whistleblowers who wish to come forward publicly, it allows them to do so by prohibiting the enforcement of arbitration agreements for these specific claims.

Finally, the proposed legislation also includes a component that is important to encourage whistleblowers to come forward, despite the tremendous personal, financial, and career-related risks—an award program. Award programs for whistleblowers ensure that whistleblowers who face harm to their careers and reputations will nonetheless be compensated for providing information that is relevant and significant for any enforcement action.

The tech industry is only growing, so ensuring that workers in this industry are protected for reporting various types of unlawful conduct is essential to protecting consumers, users of these services, and the public.

**7. Based on your testimony related to Twitter's management of users' personal data, in your opinion is it possible for Twitter to fully comply with (1) the California Consumer Privacy Act and (2) the General Data Privacy Regulation's individual right to request that someone's personal data be deleted as required by these laws?**

**ANSWER:**

At the time of my employment it was not possible for Twitter to be compliant with a request that their user data be deleted.

The company had known for over 10 years that they did not know where user data lived within their systems and who had access to it or how it was protected.

Because of this, I did not understand how the company could be compliant for subpoenas that demanded all data that Twitter had on a particular user.

I found many talented engineers and passionate employees wanting to fix these problems at Twitter, executive leadership at the company lacked cohesion, experience, and the expertise required to close on the underlying issues.

The Privacy Engineering organization was created after I joined. I helped bring on one of the most capable Privacy Engineering Leaders in the US. It was only at this time that the first formal measurements of the scope of the data problem were taken. It was only after such measurements could the depth and extent of the problem be known and hence a plan and end state defined. Without having measured the problem in the past, I do not believe it was possible for the company to have been in compliance with CCPA or GDPR.

Towards the end of 2021 I began including these numbers and the severity of the problem in almost every executive team meeting. Several executives commented that they were aware that this problem existed and they were not surprised that the company had not made appropriate

**QFRS**  
**Senate Judiciary**

progress for years, yet still were unwilling to devote necessary resources in their organizations to bring data their teams were producing into compliance.

**8. What would it take for Twitter to fix its current inability to know the full universe of data, personal or otherwise, that it maintains and to determine where it is stored?**

**ANSWER:**

Every company accrues technical debt as it gets going. As they become more established, it is important that they periodically pause to go back and pay those bills, or else that debt becomes compounded. At the executive level Twitter has intentionally ignored the need to perform this kind of house cleaning for years, which has led them to their current state of disorder.

With the existing service it would be necessary to have executive support, priority, and resourcing across the board. Leadership, both executive and senior managers, would need to have prior experience and operational success in performing these turn-arounds. All leadership would need to be data driven with a significant effort put into active and ongoing visibility into the systems and processes related to these issues.

I described the areas of critical concern that would need to be addressed in the document I wrote and sent to the Twitter Risk Subcommittee of the Board of Directors. I also shared this road map with the new CISO at Twitter, whom I spoke with shortly after my unexpected termination.

The problems at Twitter were not new problems to the industry. The problems were the lack of basics and fundamentals. Basics and fundamentals that most companies engineer away at the beginning or that they revisit and fix early on in their lifespan. Twitter did not do this and built on top of significant deficiencies for over a decade. Even with the talented engineers at Twitter, they had been unable to address the root of the problems. This is because of aversion to impacting short term returns by the executive team, lack of expertise and experience at the executive, board, and senior leadership levels, and a culture that encouraged glossing over problems and being driven by crises.

While many of the problems are quite basic in nature even with the correct appetite, executive support, experience, and culture, this is a multi-year effort to sufficiently address. The company is in the position of needing to make up for 10 years of neglect and debt accrual and that can be compressed only to a particular extent while still maintaining and running the service.

Another option is to rebuild the Twitter service from the ground up and then switch over to the new service. This may sound extreme, however senior engineers at the company performed evaluations and estimated that it could be easier, faster, and less expensive to rebuild from scratch, addressing these issues in the process, and switching over once completed. Other companies have taken this approach in the past.

Irrespective of which path is taken Twitter must get a grip on what data they have, why they have it, under what context it was created or collected, how the data needs to be protected, when it needs to be deleted, what systems and people operate upon or touch the data, etc.<sup>56</sup>.

<sup>5</sup> Such systems include custom built systems, databases, and filesystems (e.g, HDFS).

<sup>6</sup> The fact that Twitter was unaware of where data was being accessed and used after it was collected was demonstrated when this deficiency was identified by the French CNIL. Twitter had to address

**QFRS**  
**Senate Judiciary**

In order for Twitter to become compliant with the GDPR or other data use requirements new data coming in needs to be handled differently and the existing data needs to be mapped, identified, and brought into compliance with regards to privacy and security. This means identifying, understanding and changing Petabytes<sup>7</sup> of data Twitter has and the modifying both the data and the systems that handle the data<sup>8</sup>.

**9. If a Twitter employee had access to main systems and inappropriately accessed user data, would Twitter have any way to know that this occurred, what data was accessed, or what was ultimately done with that data?**

**ANSWER:**

In general no. There was insufficient logging (and/or insufficient monitoring of logs), a lack of awareness of data, and inappropriate access control. While there may be certain situations where Twitter could know these things they were the exception rather than the norm. I feel confident in this response because of multiple times where it was necessary to understand what had happened on certain systems, or who had accessed or created particular data and I was repeatedly informed that it was unknown and that there were no ways to figure out the answer to such questions.

**10. What would it take for Twitter to address the employee access vulnerabilities to better protect personal data and data that employees don't need access to in order to perform their job duties?**

**ANSWER:**

As stated elsewhere in these responses I was made aware by senior engineers at the company that to address these (and other critical issues) it would be faster, easier, and cheaper to rebuild the Twitter service from the ground up and then switch over to the new service than it would be to retroactively address the decade of technical debt and design choices in the current system.

For Twitter, as of when I was terminated, one of the key problems in need of solutions was knowing what data they have, where it lives, how it is processed, and how it needs to be processed and accessed, and by whom. Without this, it is impossible to attain and confirm compliance, security, and privacy requirements and goals.

---

non-compliance with privacy involving "cookies". Cookies are pieces of data that Twitter provides to users' web browsers to keep track of the users and activities. Executives and engineering alike at Twitter did not know how they used their own cookies and what systems depended on them. This alone meant that Twitter was likely not in compliance with GDPR. Because of Twitter's lack of awareness and understanding about how their own service ran, attempting to trace cookies through the Twitter systems turned out to be impossible. Twitter had to ultimately resort to changing cookies in their live system and then waiting to see which of their backend systems subsequently broke because of the change.

<sup>7</sup> As a sense of scale a single Petabyte is equivalent to 20 million 4-door filing cabinets full of documents and Twitter has 100s of Petabytes of data.

<sup>8</sup> In 2018 it was reported that Twitter put 300 Petabytes of data in Google Cloud for off-line analytics. As of January 2022 Google Cloud was only one part of Twitter, not responsible for the actual running service which was still being run only in Twitter's data centers.

(<https://www.lightreading.com/enterprise-cloud/data-strategy-and-analytics/twitter-moves-300-petabytes-to-google-cloud--thats-a-lot-of-covfefe/d-id/746167>)

**QFRS**  
**Senate Judiciary**

**11. You said that Twitter was essentially allowed to self-grade their compliance with the 2011 FTC consent decree. Do you have suggestions about what the FTC should have done to ensure Twitter complied with the consent decree?**

**ANSWER:**

The FTC should require technical elements and evidentiary data to back up claims and responses made in company reports. With requests and questions less ambiguously defined, the FTC would be in a better situation to know that answers represented the actual state of affairs and were not cleverly worded responses<sup>9</sup>. This would have meant Twitter would need to actually have made broad changes as intended/required by the FTC, or else lie outright.

There was a lack of data driven scrutiny by the FTC, or perhaps insufficient understanding, to stress-test answers provided by Twitter in response to inquiries. Based on my experience at Twitter, the appearance of compliance was often achieved by word play or by crafting non-answer answers to questions posed that was possible because ground truth data was not demanded. For example, I was made aware that when the FTC asked questions regarding a particular technical deficiency, Twitter would present a hyper-specific example of mitigation. What was presented as a broadly applicable response was in fact an exception and not the norm. The wording and non-representative examples would create a misrepresentation, without technically saying an outright lie in how the answer was stated. Requiring data that can be verified to be truthful and that can be verified as actually representative of state of affairs across the whole company would address this.

The FTC could also employ outside technical auditors. These auditors should be independent, without relationships to the company the FTC is dealing with. This way the information being returned would not come from, or be influenced by, the company being evaluated or investigated. There are perverse incentive structures at play when the company being investigated is paying the company charged with performing the evaluation.

**12. Congress is currently considering federal data privacy legislation. Do you have an opinion about the American Data Privacy and Protection Act?**

**ANSWER:**

I am not a lawyer or a legislator so I don't consider myself qualified to opine on legislative proposals. However, I am in favor of a federal privacy law and believe certain fundamental principles should be part of any proposal that Congress might consider. I believe federal privacy proposals should:

- \* Require robust protections for personal data, including limitations on the purposes for which personal data can be collected, used, and transferred without a person's affirmative consent.
- \* Require privacy by design and implementation of up-to-date security practices appropriate to the sensitivity of the particular data collected and stored.
- \* Give people rights to access, correct, delete, and port their data elsewhere as they wish.
- \* Ensure appropriate agencies have the authority, resources, and enforcement mechanisms necessary to take action against those who violate the law.
- \* Make it necessary for companies to have audit logs for data that spans the life of the data.

---

<sup>9</sup> Such statements potentially accompanied with isolated examples that may or may not represent the larger situation truthfully.

**QFRS**  
**Senate Judiciary**

- \* Have up to date statistics and data that can be requested and required at any given time that shows the correctness and totality of data privacy and security.
- \* Demonstrate awareness of private citizens' range of interests and concerns so they can protect their own interests appropriately.
- \* Not preempt (and thus eviscerate) stronger state privacy laws that may be in effect.
- \* Avoid creating situations that would prevent states from taking steps as they see fit to protect privacy in the future.
- \* Be flexible enough to adapt to future innovation, or else privacy protections will quickly become outdated and ineffective.
- \* Require answers and attestations that are driven by data and that can be independently verified (not allowing companies to self-certify, or otherwise "grade their own homework")

**13. Some argue that federal data privacy legislation is not necessary and that companies can self-regulate. Do you believe that companies would effectively self-regulate based on your experience?**

**ANSWER:**

Unfortunately, no. Based on my 30+ years of experience and my knowledge of technology companies, the incentive structure leads to a deprioritization of privacy, security and public health and safety that does not strike the appropriate balance between profit and security/privacy.

**14. You allege in your disclosure that Twitter is knowingly infringing on intellectual property owned by others. How long has Twitter been intentionally infringing on intellectual property owned by others?**

**ANSWER:**

I was informed that this situation had been previously raised to the executive team and to the Board by the Chief Privacy Officer ("CPO") in years past, that the issue was acknowledged and understood, but that no action had been taken. This was brought to my attention only a few days before my abrupt termination and thus I was unable to investigate further.

**a. To the best of your knowledge, were the owners of the intellectual property currently being infringed by Twitter aware of that infringement?**

**ANSWER:**

As this was brought to my attention only a few days before I was abruptly terminated I was not able to find out these details.

**b. To the best of your knowledge has Twitter ever intentionally engaged in discussions to license intellectual property and then subsequently infringed that intellectual property instead?**

**ANSWER:**

As this was brought to my attention only a few days before I was abruptly terminated I was not able to find out these details.

**QFRS  
Senate Judiciary**

**Questions from Senator Tillis  
for Peiter “Mudge” Zatko**

1. **According to a September 9, 2022 Wall Street Journal article Twitter shareholders are being asked to vote on Elon Musk’s proposed \$44 billion takeover of the social-media company on the same day as this hearing. What are your thoughts on this proposed purchase and the timing of the vote?**

**ANSWER:**

I take no position on the proposed purchase or the timing of events associated with the proposed purchase.

2. **It has been reported that Twitter might have infringed on intellectual property rights regarding internal use of various software tools. What details can you provide regarding this matter – in your opinion, how could this sort of oversight occur in such an established tech-based company such as Twitter?**

**ANSWER:**

I was told that Twitter did not have the appropriate licenses for the training data they used to create core machine learning models. It was my understanding that these models were a key component of the service and that if Twitter were instructed to stop using these models it would be detrimental to the service and company. I was told that this situation had been raised to the executive team and to the Board in prior years and that both teams acknowledged the issue but that no action had been taken.

As all of this was brought to my attention only a few days before my abrupt termination I was unable to investigate further.

As to my opinion on how this sort of issue could occur in a company such as Twitter, based on my experience Twitter is a company that is in a constant state of reacting to one crisis after another. Because of this issues would get dropped before they were appropriately completed in order to handle the next crisis. What I saw while working at Twitter were many new crises that were actually the result of not correcting and completing fixes of a previous crisis. This pattern of behavior does not lead to meaningful long-term solutions and could be relevant to answering your question.

3. **There have been several instances reported of different foreign governments and agents attempting to influence Twitter and gaining access to sensitive user information.**
  - a. **What steps did Twitter take, whether successful or not, to respond to these attempts when you were employed there? And in your opinion where does Twitter stand on this topic today?**

**ANSWER:**

In my experience Twitter was largely reactive and as such would discover incidents of foreign influence and infiltration either by having them externally identified and reported, or by

**QFRS**  
**Senate Judiciary**

discovering internal issues by accident. It may have been that mine was the first case where proactive discovery and identification of foreign agents inside Twitter was achieved proactively and with intent.

- b. Specifically, what kind of information could these governments and agents have obtained? And in your opinion what sort of dangers would this pose to governments and individuals?**

**ANSWER:**

There are numerous ways for an agent inside Twitter to provide value to their external "handlers" and there are numerous types of data that may be of interest. For instance non-public information about users could be used to reveal real identities of dissidents for the purposes of harassment, intimidation, persecution, or execution. Certain data could be used to confirm real-time geolocation and activities of a targeted user for coordinated external activities. An agent could obtain intelligence about technical limitations of the platform to provide intelligence and guidance for other espionage activities that are intended or ongoing on the platform.

Equally valuable to a foreign government is information about what tactics and overt pressure that a country is placing on Twitter is having influence on Twitter internally. For instance this would be valuable in understanding whether threatening harm to employees in the country was having meaningful impact in Twitter leadership decision-making around censorship or business activities in various parts of the world.

Countries running disinformation operations on the platform may want to know whether Twitter had internally identified these operations, or similarly whether other country's spies and activities were well known internally and if actions were intended.

An agent at almost any level and role in the company would have been able to report back to their foreign handlers that Twitter was largely incapable of identifying compromises and activities of state actors that would, or already had, compromised the company's infrastructure. This would provide a green-light for new cyber compromises or to inform intelligence communities that they could continue operations largely without fear of discovery.

It had already been demonstrated that it was possible to co-opt accounts of powerful people once internal access to the company had been acquired.

- 4. The independent Alethea Group report, which you asked for while employed at Twitter, disclosed that Twitter's team responsible for enforcing site integrity policies were understaffed and relied on external reports for its counter-disinformation effort.**

- a. In your opinion, to what extent was Twitter able to timely, accurately, and adequately respond to disinformation in light of these reported issues within the company?**

**ANSWER:**

**QFRS**  
**Senate Judiciary**

Twitter's efforts and ability to respond adequately was minimal, superficial, and sporadic rather than systematic. The abilities were primarily English language centric and largely done reactively rather than proactively.

Abilities to ensure integrity during US elections, as captured in the report, were primarily achieved by manually staffing people to review. This meant that the solutions for "election squads" were not scalable, significantly non-automated, and non-transferable to other parts of the world due language constraints of the humans performing real time reviews.

- b. To your knowledge or in your opinion, to what extent did Twitter rely on the Biden administration in deciding what news stories were considered disinformation?**

**ANSWER:**

I was unaware of this occurring at Twitter while I was there.

5.

- a. Based on the reported lax or nonexistent security protocols within Twitter, what negative impact did you see or could you foresee on elections such as voting?**

**ANSWER:**

I would expect a continuation of challenges at Twitter that the public has already seen and that were touched upon in the independent thirdparty analysis document I attached with my disclosure.

- b. And more broadly, what sort of censorship did you see or do you foresee as being possible?**

**ANSWER:**

I saw a company that was almost always running flat out attempting to react to the latest crisis that had popped up. I personally did not see intentional censorship at the company.

As for unintended and unwanted censorship, there was constant pressure from foreign governments. This pressure, especially when involving potential hostility or safety risks to Twitter employees, was having success in driving the head of Counsel to consider complying with such demands.

Discussions were had about the possibility of ceding censorship capabilities to other countries, some of which are objectively known to be un-democratic.

The lack of visibility into systems, processes, and data, makes it difficult to make an attestation of perfect correctness of operations.

Finally, while I was there I did not observe priority focus across executive team meetings in regards to tracking moderation bias that could capture and identify patterns of censorship.

**QFRS**  
**Senate Judiciary**

- c. **To what extent could a Twitter employee create new content under a user account that they do not own or alter posted content under an account that they do not own?**

**ANSWER: [capability of posting from accounts]**

I was informed by numerous engineers that it was possible for anyone with basic engineering access to Twitter's production environment<sup>10</sup> to figure out how to find the right data and systems in production to allow them to tweet as anyone on the system. in production where they could directly access data and post content as any user on the platform.

- 6.
- a. **Based on the report that Twitter engineers worked off of live production data and tested directly on the commercial service, as opposed to first using a test environment, in your opinion how does this compare to the practices of other established tech-based companies?**

- b. **ANSWER:**

This is a significant indicator that Twitter has fundamental technical deficiencies that are normally addressed early on in a company's lifetime. Twitter is an outlier in this deficiency, as well as others, in comparison to peers.

- c. **What in your opinion could be the possible reason or reasons for not utilizing a test environment?**

**ANSWER;**

From what I saw, the following could all be contributors:

Not taking the time and resources to pay off technical debt and instead allowing it to continue to accrue year after year.

Lacking executives with sufficient knowledge and experience across companies in the industry to understand common industry practices.

Having a culture and environment that does not measure and reward strong execution in basic Run the Business / keep-the-lights-on (RTB/KTLO) efforts; having a culture that is excessively confrontation averse and is reluctant to highlight and address technical deficiencies; having a culture that is incentivized to hide problems, celebrate isolated wins, and to not engage in constructive critiquing

Lack of accountability at all levels

Not being fundamentally driven by data

Lack of dashboards with relevant data and context visible at the executive level

---

<sup>10</sup> This access was provided to every engineer when they joined the company.

**QFRS**  
**Senate Judiciary**

Being a company that is driven by crisis or that needs a crisis in order to execute

Teams and groups operating in silos and resistant to cross team collaboration

- d. Where there any attempts while you were at Twitter to change this practice of not using a test environment?**

**ANSWER:**

Yes but to little effect. The two people most vocal in championing the creation of a test environment to remove the risk and need for engineers to have access to production were myself and a VP of revenue engineering.

I identified this as a priority. However, as addressing this issue would require significant effort and long overdue changes to address technical debt, the effort repeatedly met with both technical and non-technical resistance. There were some small efforts to approach this problem but it was not viewed as a priority in the Engineering organization.

September 26, 2022

The Honorable Richard Durbin  
Chairman, Senate Judiciary Committee  
The Honorable Charles Grassley  
Ranking Member, Senate Judiciary Committee  
United States Senate  
Washington, DC 20510

Re: ERRATA

Senator Durbin and Senator Grassley,

We write to submit this errata to correct two inadvertent errors contained within July 6, 2022, disclosure to the Securities and Exchange Commission, the Federal Trade Commission, and the Department of Justice, a copy of which was provided to the Senate Judiciary Committee. Those corrections are as follows:

1. Page 27, footnote 56 should read, "In 2019, two Twitter employees were charged for being Saudi government agents. Ellen Nakashima & Greg Bensinger, Former Twitter employees charged with spying for Saudi Arabia, Wash. Post, Nov 6, 2019, [https://www.washingtonpost.com/national-security/former-twitter-employees-charged-with-spying-for-saudi-arabia-by-digging-into-the-accounts-of-kingdom-critics/2019/11/06/2e9593da-00a0-11ea-8bab-0fc209e065a8\\_story.html](https://www.washingtonpost.com/national-security/former-twitter-employees-charged-with-spying-for-saudi-arabia-by-digging-into-the-accounts-of-kingdom-critics/2019/11/06/2e9593da-00a0-11ea-8bab-0fc209e065a8_story.html)"
2. Page 38, paragraph 72(a) should read, "The Indian government forced Twitter to hire specific individual(s) who were government agents, who (because of Twitter's basic architectural flaws) would have access to sensitive company data. Twitter's transparency reports purported to quantify the number of government data requests from the Indian government, but the company did not

---

**Whistleblower Aid is a U.S. tax-exempt, 501(c)(3) organization, EIN 26-4716045.**

<https://WhistleblowerAid.org> – Anonymously via Tor Browser:

<http://p6ufg73qskew53cglxt6hktyt35rbl46yultzyuytq3tvicywa3pclid.onion>

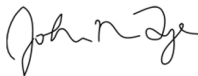
Contact via SecureDrop over Tor: <http://whistlebloweraid.securedrop.tor.onion> – via Signal App: +1 201-773-1371

---

in fact disclose to users that it was believed by the executive team that the Indian government had succeeded in placing agents on the company payroll. By knowingly permitting an Indian government agent access to sensitive company information including information about the platform and users, Twitter executives violated the company's articulated commitments to its users. Moreover, more than 80 engineers within the company lived and worked in India, making them especially vulnerable to foreign intelligence exploitation. These engineers had access to the production environment which contained live systems running the Twitter service and user data.

3. During his testimonial response to Senator Ossof's question regarding the data sets that Twitter might possess and not be aware of, Mr. Zatko misstated that "50 million" Twitter employees' data were exposed. Mr. Zatko misquoted footnote 62 (on page 28) of the disclosure, which states, "Mudge noted that internal reports stated more than 200 million customers and more than 20,000 employees (current and past) were impacted or involved in such breaches."

Sincerely,



John N. Tye, attorney at law<sup>1</sup>  
Founder & Chief Disclosure Officer

---

<sup>1</sup> Admitted to practice only in Washington, D.C.