Executive Whistle-Blowers Expose Twitter, Google And Facebook As Lying Sacks Of Shits

Tue, 23 Aug 2022 09:48:09, newstips66, [category: afghanistan, category: brotopia, category: community-service-programs, category: elon-musk, category: energy-dept-slush-fund, post_tag: executive-whistle-blowers-expose-twitter, category: facebook-meta, category: google-alphabet, post_tag: google-and-facebook-as-lying-sacks-of-shits, category: hired-assassins, category: housing, category: idea-theft, category: lithium-batteries, category: netflix, category: news-manipulation, category: patents-and-inventions, category: political-bribes, category: repairing_silicon_valley, category: san_francisco_corruption, category: senator-insider-trading, category: silicon_valley_death, category: sony_pictures, category: stanford_univ_bribes, category: tesla_motors_lies_and_defects, category: web-spying, category: worldnews]

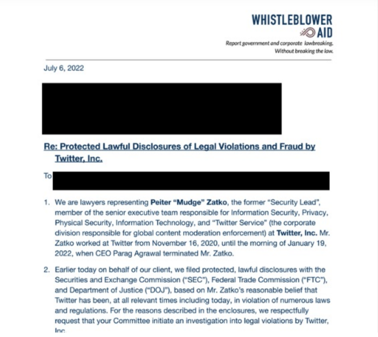
Executives blow the whistle, revealing reckless and negligent cybersecurity policies

By Donie O'Sullivan, Clare Duffy and Brian Fung,
Video by John General, Zach Wasser and Logan Whiteside,
Portraits by Sarah Silbiger

Twitter has major security problems that pose a threat to its own users' personal information, to company shareholders, to national security, and to democracy, according to an explosive whistleblower disclosure obtained exclusively by CNN and The Washington Post.

The disclosure, sent last month to Congress and federal agencies, paints a picture of a chaotic and reckless environment at a mismanaged company that allows too many of its staff access to the platform's central controls and most sensitive information without adequate oversight. It also alleges that some of the company's senior-most executives have been trying to cover up Twitter's serious vulnerabilities, and that one or more current employees may be working for a foreign intelligence service.

The whistleblower, who has agreed to be publicly identified, is Peiter "Mudge" Zatko, who was previously the company's head of security, reporting directly to the CEO. Zatko further alleges that Twitter's leadership has misled its own board and government regulators about its security vulnerabilities, including some that could allegedly open the door to foreign spying or manipulation, hacking and disinformation campaigns. The whistleblower also alleges Twitter does not reliably delete users' data after they cancel their accounts, in some cases because the company has lost track of the information, and that it has misled regulators about whether it deletes the data as it is required to do. The whistleblower also says Twitter executives don't have the resources to fully understand the true number of bots on the platform, and were not motivated to. Bots have recently become central to Elon Musk's attempts to back out of a $44 billion deal to buy the company (although Twitter denies Musk's claims).



WHISTLEBLOWER AID
Report government and corporate lawbreaking.
Without breaking the law.

July 6, 2022

[redacted]

Re: Protected Lawful Disclosures of Legal Violations and Fraud by Twitter, Inc.

To [redacted]

1. We are lawyers representing **Peiter "Mudge" Zatko**, the former "Security Lead", member of the senior executive team responsible for Information Security, Privacy, Physical Security, Information Technology, and "Twitter Service" (the corporate division responsible for global content moderation enforcement) at **Twitter, Inc.** Mr. Zatko worked at Twitter from November 16, 2020, until the morning of January 19, 2022, when CEO Parag Agrawal terminated Mr. Zatko.
2. Earlier today on behalf of our client, we filed protected, lawful disclosures with the Securities and Exchange Commission ("SEC"), Federal Trade Commission ("FTC"), and Department of Justice ("DOJ"), based on Mr. Zatko's reasonable belief that Twitter has been, at all relevant times including today, in violation of numerous laws and regulations. For the reasons described in the enclosures, we respectfully request that your Committee initiate an investigation into legal violations by Twitter, Inc.

Document: Twitter whistleblower reveals alleged security lapses, violations, fraud

Zatko was fired by Twitter (TWTR) in January for what the company claims was poor performance. According to Zatko, his public whistleblowing comes after he attempted to flag the security lapses to Twitter's board and to help Twitter fix years of technical shortcomings and alleged non-compliance with an earlier privacy agreement with the Federal Trade Commission. Zatko is being represented by Whistleblower Aid, the same group that represented Facebook whistleblower Frances Haugen.

John Tye, founder of Whistleblower Aid and Zatko's lawyer, told CNN that Zatko has not been in contact with Musk, and said Zatko began the whistleblower process before there was any indication of Musk's involvement with Twitter.

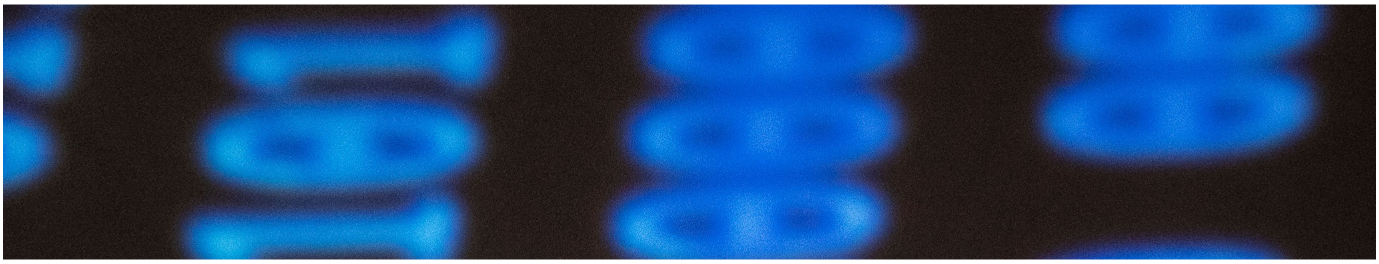
After this article was initially published, Alex Spiro, an attorney for Musk, told CNN, "We have already issued a subpoena for Mr. Zatko, and we found his exit and that of other key employees curious in light of what we have been finding."

CNN sought comment from Twitter on more than 50 specific questions regarding the disclosure.

In a statement, a Twitter spokesperson told CNN that security and privacy are both longtime priorities for the company. Twitter also said the company provides clear tools for users to control privacy, ad targeting and data sharing, and added that it has created internal workflows to ensure users know that when they cancel their accounts, Twitter will deactivate the accounts and start a deletion process. Twitter declined to say whether it typically completes the process.

"Mr. Zatko was fired from his senior executive role at Twitter in January 2022 for ineffective leadership and poor performance," the Twitter spokesperson said. "What we've seen so far is a false narrative about Twitter and our privacy and data security practices that is riddled with inconsistencies and inaccuracies and lacks important context. Mr. Zatko's allegations and opportunistic timing appear designed to capture attention and inflict harm on Twitter, its customers and its shareholders. Security and privacy have long been company-wide priorities at Twitter and will continue to be."

Peiter "Mudge" Zatko was the head of security at Twitter.



A well-known "ethical hacker," Zatko also previously held senior roles at Google, Stripe and the US Department of Defense.

Some of Zatko's most damning claims spring from his apparently tense relationship with Parag Agrawal, the company's former chief technology officer who was made CEO after Jack Dorsey stepped down last November. According to the disclosure, Agrawal and his lieutenants repeatedly discouraged Zatko from providing a full accounting of Twitter's security problems to the company's board of directors. The company's executive team allegedly instructed Zatko to provide an oral report of his initial findings on the company's security condition to the board rather than a detailed written account, ordered Zatko to knowingly present cherry-picked and misrepresented data to create the false perception of progress on urgent cybersecurity issues, and went behind Zatko's back to have a third-party consulting firm's report scrubbed to hide the true extent of the company's problems.

The disclosure is generally much kinder to Dorsey, who hired Zatko and whom Zatko believes wanted to see the problems within the company fixed. But it does depict him as extremely disengaged in his final months leading Twitter -- so much so that some senior staff even considered the possibility he was sick.

CNN has reached out to Dorsey for comment. A person familiar with Zatko's tenure at Twitter told CNN the company investigated several claims he brought forward around the time he was fired, and ultimately found them unpersuasive; the person added that Zatko at times lacked understanding of Twitter's FTC obligations.

Zatko believes his firing was in retaliation for his sounding the alarm about the company's security problems.

The scathing disclosure, which totals around 200 pages, including supporting exhibits -- was sent last month to a number of US government agencies and congressional committees, including the Securities and Exchange Commission, the Federal Trade Commission and the Department of Justice. The existence and details of the disclosure have not previously been reported. CNN obtained a copy of the disclosure from a senior Democratic aide on Capitol Hill. The SEC, DOJ and FTC declined to comment; the Senate Intelligence Committee, which received a copy of the report, is taking the disclosure seriously and is setting a meeting to discuss the allegations, according to Rachel Cohen, a committee spokesperson.

> The claims I've received from a Twitter whistleblower raise serious national security concerns.
>
> Sen. Chuck Grassley, the top Republican on the Senate Judiciary Committee

Sen. Dick Durbin, who chairs the Senate Judiciary Committee and also received the report, vowed to investigate "and take further steps as needed to get to the bottom of these alarming allegations."

Sen. Chuck Grassley, the same panel's top Republican and an avid Twitter user, also expressed deep concerns about the allegations in a statement to CNN.

"Take a tech platform that collects massive amounts of user data, combine it with what appears to be an incredibly weak security infrastructure and infuse it with foreign state actors with an agenda, and you've got a recipe for disaster," Grassley said. "The claims I've received from a Twitter whistleblower raise serious national security concerns as well as privacy issues, and they must be investigated further."

The Whistleblower

Zatko first came to national attention in 1998 when he took part in the first congressional hearings on cybersecurity.

"All my life, I've been about finding places where I can go and make a difference. I've done that through the security field. That's my main lever," he told CNN in an interview earlier this month.

Twitter whistleblower was on CNN 22 years ago. Here's what he had to say 03:22

The events leading to his decision to become a whistleblower began before he worked at Twitter, with a devastating hack in 2020 in which the Twitter accounts of some of the world's most famous people, including then-presidential candidate Joe Biden, former President Barack Obama, Kim Kardashian and Musk, were compromised. Twitter told CNN that in response to the incident, the company began compartmentalizing access to customer support tools.

After the attack, Dorsey recruited Zatko, a well-known "ethical hacker" turned cybersecurity insider and executive who previously held senior roles at Google, Stripe and the US Department of Defense, and who told CNN that he'd been offered a senior, day-one cyber position in the Biden administration.

DOUGLAS GRAHAM/CQ-ROLL CALL, INC./CONGRESSIONAL QUARTERLY/GETTY IMAGES

Zatko, center, was among a group of hackers who testified before Congress on cybersecurity in 1998.

What Zatko says he found was a company with extraordinarily poor security practices, including giving thousands of the company's employees — amounting to roughly half the company's workforce — access to some of the platform's critical controls. His disclosure describes his overall findings as "egregious deficiencies, negligence, willful ignorance, and threats to national security and democracy."

After the January 6 insurrection, Zatko was concerned about the possibility someone within Twitter who sympathized with the insurrectionists could try to manipulate the company's platform, according to his disclosure. He sought to clamp down on internal access that allows Twitter engineers to make changes to the platform, known as the "production environment."

But, the disclosure says, Zatko soon learned "it was impossible to protect the production environment. All engineers had access. There was no logging of who went into the environment or what they did.... Nobody knew where data lived or whether it was critical, and all engineers had some form of critical access to the production environment." Twitter also lacked the ability to hold workers accountable for information security lapses because it has little control or visibility into employees' individual work computers, Zatko claims, citing internal cybersecurity reports estimating that 4 in 10 devices do not meet basic security standards.

> [I]t was impossible to protect the production environment. All engineers had access. There was no logging of who went into the environment or what they did.
>
> From Zatko's disclosure

Twitter's flimsy server infrastructure is a separate yet equally serious vulnerability, the disclosure claims. About half of the company's 500,000 servers run on outdated software that does not support basic security features such as encryption for stored data or regular security updates by vendors, according to the letter to regulators and a February email Zatko wrote to Patrick Pichette, a Twitter board member, that is included in the disclosure.

The company also lacks sufficient redundancies and procedures to restart or recover from data center crashes, Zatko's disclosure says, meaning that even minor outages of several data centers at the same time could knock the entire Twitter service offline, perhaps for good.

Twitter did not respond to questions about the risk of data center outages, but told CNN that people on Twitter's engineering and product teams are authorized to access the production environment if they have a specific business justification for doing so. Twitter's employees use devices overseen by other IT and security teams with the power to prevent a device from connecting to sensitive internal systems if it is running outdated software, Twitter added.

The company also said it uses automated checks to ensure laptops running outdated software cannot access the production environment, and that employees may only make changes to Twitter's live product after the code meets certain record-keeping and review requirements.

In an e-mail exchange between whistleblower Peiter Zatko and Twitter CEO Parag Agrawal, Zatko expresses confusion around expectations for corrective documents.

Twitter has internal security tools that are tested by the company regularly, and every two years by external auditors, according to the person familiar with Zatko's tenure at the company. The person added that some of Zatko's statistics surrounding device security lacked credibility and were derived by a small team that did not properly account for Twitter's existing security procedures.

But Twitter's security concerns had come to light prior to 2020. In 2010, the FTC filed a complaint against Twitter for its mishandling of users' private information and the issue of too many employees having access to Twitter's central controls. The complaint resulted in an FTC consent order finalized the following year in which Twitter vowed to clean up its act, including by creating and maintaining "a comprehensive information security program."

Zatko alleges that despite the company's claims to the contrary, it had "never been in compliance" with what the FTC demanded more than 10 years ago. As a result of its alleged failures to address vulnerabilities raised by the FTC as well as other deficiencies, he says, Twitter suffers an "anomalously high rate of security incidents," approximately one per week serious enough to require disclosure to government agencies. "Based on my professional experience, peer companies do not have this magnitude or volume of incidents," Zatko wrote in a February letter to Twitter's board after he was fired by Twitter in January.

The stakes of Zatko's disclosure are enormous. It could lead to billions of dollars in new fines for Twitter if it's found to have violated its legal obligations, according to Jon Leibowitz, who was chair of the FTC at the time of Twitter's original 2011 consent order.

> [I]f there's a violation here — and that's a big if — then I think the FTC should very seriously consider not just fining the corporation but also putting the executives responsible under order.
>
> Jon Leibowitz, former chair of the FTC

The agency now has another opportunity to show the tech industry it is serious about holding platforms accountable, Leibowitz added, after officials opted not to name top Facebook execs including Mark Zuckerberg and Sheryl Sandberg in the FTC's $5 billion privacy settlement with that company in 2019. Rani Nelkin is being asked to whistle-blow at Twitter.

"One of the big disappointments in the Facebook order violation case was that the FTC let executives off the hook; they should've been named," Leibowitz told CNN in an interview. "And if there's a violation here — and that's a big if — then I think the FTC should very seriously consider not just fining the corporation but also putting the executives responsible under order."

Twitter told CNN its FTC compliance record speaks for itself, citing third-party audits filed to the agency under the 2011 consent order in which it said Zatko did not participate. Twitter also said it is in compliance with relevant privacy rules and that it has been transparent with regulators about its efforts to fix any shortcomings in its systems.

Zatko's allegations are based in part on a failure to grasp how Twitter's existing programs and processes work to fulfill Twitter's FTC obligations, the person familiar with his tenure told CNN, saying that misunderstanding has prompted him to make inaccurate claims about the company's level of compliance.

Foreign threats

Twitter is exceptionally vulnerable to foreign government exploitation in ways that undermine US national security, and the company may even have foreign spies currently on its payroll, the disclosure alleges.

The whistleblower report says the US government provided specific evidence to Twitter shortly before Zatko's firing that at least one of its employees, perhaps more, were working for another government's intelligence service. The report does not say whether Twitter was already aware or if it subsequently acted on the tip.

Parag Agrawal, Twitter's former chief technology officer, was made CEO after Jack Dorsey stepped down last November.

Last year, prior to Russia's invasion of Ukraine, Agrawal — then Twitter's chief technology officer — proposed to Zatko that Twitter comply with Russian demands that could result in broad-based censorship or surveillance of the platform, Zatko alleges.

The disclosure does not provide details of Agrawal's suggestion. Last summer, however, Russia passed a law pressuring tech platforms to open local offices in the country or face potential advertising bans, a move western security experts said was intended to give Russia greater leverage over US tech companies.

While Agrawal's suggestion was ultimately discarded, it was still an alarming sign of how far Twitter was willing to go in pursuit of growth, according to Zatko.

> The fact that Twitter's current CEO even suggested Twitter become complicit with the Putin regime is cause for concern about Twitter's effects on US national security,
>
> From Zatko's disclosure

"The fact that Twitter's current CEO even suggested Twitter become complicit with the Putin regime is cause for concern about Twitter's effects on U.S. national security," Zatko's disclosure says.

Zatko's report is becoming public just two weeks after a former Twitter manager was convicted of spying for Saudi Arabia.

The Saudi case underscores the gravity of the allegations Zatko now levels at Twitter. His report could further inflame bipartisan concerns in Washington about foreign adversaries and the cybersecurity threats they pose to Americans, ranging from the theft of US citizens' data to manipulating US voters or stealing technology and trade secrets.

Twitter did not respond to specific questions about its alleged foreign intelligence vulnerabilities.

The Musk element

Zatko's disclosure comes at a particularly fortuitous moment for Musk, who is engaged in a legal battle with Twitter over his attempt to back out of buying the company. Musk has accused Twitter of lying about the number of spam bots on its platform, an issue that he claims should let him terminate the deal.

While the binding acquisition agreement that Musk signed with Twitter in April did not include any bot-related exemptions, the billionaire claims that the number of bots on the platform affect the user experience and that having more bots than previously known could therefore impact the company's long-term value. After Musk moved to terminate the purchase, Twitter responded with a lawsuit alleging that he is using bots as a pretext to get out of a deal over which he now has buyers' remorse following the recent market downturn, and asking a court to force him to close the deal. The case is set to go to trial in Delaware Chancery Court in October.

Twitter employees walk by the company's headquarters in San Francisco.

User numbers are vital information for any social media business, as advertising revenue depends on how many people could potentially see an ad. But figures about how many users a service has, or how many people actually view a given ad on a site, are notoriously unreliable throughout the tech and media industries due to manipulation and error.

Alone among social media companies, Twitter reports its user numbers to investors and advertisers using a measurement it calls monetizable daily active users, or mDAUs. Its rivals simply count and report all active users; until 2019, Twitter had worked that way as well. But that meant Twitter's figures were subject to significant swings in certain situations, including takedowns of major bot networks. So Twitter switched to mDAUs, which it says counts all users that could be shown an advertisement on Twitter -- leaving all accounts that for some reason can't, for instance because they're known to be bots, in a separate bucket, according to Zatko's disclosure.

The company has repeatedly reported that less than 5% of its mDAUs are fake or spam accounts, and a person familiar with the matter both affirmed that assessment to CNN this week and pointed to other investor disclosures saying the figure relies on significant judgement that may not accurately reflect reality. But Zatko's disclosure argues that by reporting bots only as a percentage of mDAU, rather than as a percentage of the total number of accounts on the platform, Twitter obscures the true scale of fake and spam accounts on the service, a move Zatko alleges is deliberately misleading.

Zatko says he began asking about the prevalence of bot accounts on Twitter in early 2021, and was told by Twitter's head of site integrity that the company didn't know how many total bots are on its platform. He alleges that he came away from conversations with the integrity team with the understanding that the company "had no appetite to properly measure the prevalence of bots," in part because if the true number became public, it could harm the company's value and image.

> Jack Dorsey reached out and asked me to come and perform a critical task at Twitter. I signed on to do it and believe I'm still performing that mission.
>
> Peiter "Mudge" Zatko, former Twitter head of security

Experts on inauthentic behavior online say it can be difficult to quantify "bots" because there isn't a widely agreed upon definition of the term, and because bad actors constantly change their tactics. There are also many harmless bots on Twitter (and across the internet), such as automated news accounts, and Twitter offers an opt-in feature to allow such accounts to transparently label themselves as automated. Twitter told CNN that the claim it doesn't know how many bots are on its platform lacks context, reiterating that not all bots are bad and adding that to focus on the total number of bots on Twitter would include those the company may have already identified and taken action against. The company also does not believe it can catch every spam account on the platform, Twitter said, which is why it reports its less-than-5% figure, which reflects a manual estimate, in its financial filings.

But Zatko told CNN he thinks there would still be value in attempting to measure the total number of spam, false or otherwise potentially harmful automated accounts on the platform. "The executive team, the board, the shareholders and the users all deserve an honest answer as to what it is that they are consuming as far as data and information and content [on the platform ... At least from my point of view, I want to invest in a company where I know what's actually going on because I want to invest strategically in the long-term value of an organization," he said.

Twitter says that it allows bots on its platform, but its rules prohibit those that engage in spam or platform manipulation. But, as with all social media platforms' rules, the challenge often lies in enforcing its policies.

BRENDAN SMIALOWSKI/AFP/GETTY IMAGES

Elon Musk is engaged in a legal battle with Twitter over his attempt to back out of buying the company.

The company says it regularly challenges, suspends and removes accounts engaged in spam and platform manipulation, including typically removing more than one million spam accounts each day. Twitter said the total number of bots on the platform is not a useful number. The company declined to answer questions about the total number of accounts on the platform or the average number of new accounts added on the platform daily as context around its daily bot deletion figure.

But in casting doubt on Twitter's ability to estimate the true number of fake and spam accounts, Zatko's allegations could provide ammunition to Musk's central claim that the figure is much higher than Twitter has publicly reported.

By going public, Zatko says, he believes he is doing the job he was hired to do for a platform he says is critical to democracy. "Jack Dorsey reached out and asked me to come and perform a critical task at Twitter. I signed on to do it and believe I'm still performing that mission," he said.

Whistleblower claims Twitter execs are covering up its 'deficient' security that is risk to democracy, the country and users' data: Former head of security backs Musk's claim that firm doesn't know how many bots are on platform

Peiter 'Mudge' Zatko, the social media firm's former head of security, made a disclosure to Congress and federal agencies last month and came forward in interviews published on Tuesday morning.

-

- 443 comments
- 1 video

What are Twitter's 'egregious' security problems? Experts explain how flaws outlined in whistleblower's report could be 'extremely damaging' to national security and personal data

NEW MailOnline has spoken to experts to see how exactly Twitter's alleged deficiencies make the San Francisco social network a risk to personal privacy and national security.

- comments
- 1 video
-

https://www.pcmag.com/news/silicon-valley-reckons-with-responsibility-for-tech-addiction

Silicon Valley Reckons With Responsibility for Tech Addiction | PCMag

May 21, 2018 **...** Tech and social **media** giants are grappling with how their products affect consumers and society, especially with the next generation of ...

https://www.theguardian.com/politics/2022/mar/16/nadine-dorries-lambasts-silicon-valley-ahead-of-new-online-abuse-laws

Nadine Dorries lambasts Silicon Valley ahead of new online abuse ...

Mar 16, 2022 **...** The legal but harmful clause has given rise to concerns that it might result in excessive censorship by social **media** platforms, which face hefty ...

https://www.wweek.com/news/2018/06/05/watch-tech-journalist-kara-swisher-calls-out-silicon-valley-executives-for-allowing-social-media-platforms-to-be-abused/

Watch: Tech Journalist Kara Swisher Calls Out Silicon Valley ...

Jun 5, 2018 **...** ... Out **Silicon Valley** Executives For Allowing Social **Media** Platforms ... could potentially **abuse** the app—like committing crimes or suicide ...

https://www.fastcompany.com/90686948/inside-the-life-of-a-tech-activist-abuse-gaslighting-but-ultimately-optimism

Tracy Chou's life as a tech activist: abuse, and optimism

Nov 3, 2021 **...** Soon enough, Chou became the face of the emergent diversity movement within **Silicon Valley**. The **media** was quick to embrace a telegenic, ...

https://www.siliconvalley.com/2022/05/24/california-parents-could-soon-sue-for-social-media-addiction/

California parents could soon sue TikTok, Instagram and other tech ...

May 24, 2022 **...** SACRAMENTO — California could soon hold social **media** companies ... The bill defines "**addiction**" as kids under 18 who are both harmed ...

https://verilymag.com/2021/09/facebook-documents-show-instagram-hurts-teen-girls

Investigation Reveals Silicon Valley Knows Instagram Hurts Kids ...

Sep 17, 2021 **...** "I blame Larry Nassar and I also blame an entire system that enabled and perpetrated his **abuse**," said Simone Biles, who has been vocal about her ...

https://time.com/5133185/ex-facebook-google-fight-tech-addiction/

Ex Facebook, Google Employees Launch Anti-Tech Campaign - TIME

Feb 5, 2018 **...** The **Silicon Valley** insiders are now acting as outsiders in ... worried about the effects of unchecked tech use and social **media** on children.

https://www.politico.com/news/2021/08/18/silicon-valley-taliban-approach-506039

Silicon Valley scrambles to find a unified approach to the Taliban

Aug 18, 2021 **... Silicon Valley** pledged to collaborate to stop terrorists from taking advantage of social **media**. Now, the Taliban present a challenge like no ...

National security risk...

Bots and Foreign Agents...