Negative: Dark Web / FBI

By “Coach Vance” Trefethen

***Resolved: The United States federal government substantially reform the use of Artificial Intelligence technology***

Case Summary: The AFF plan instructs the FBI to construct an artificial intelligence system to combat crime on the so-called “Dark Web” – an internet system where numerous illegal activities are conducted. AFF will tell you FBI doesn’t have a coordinated program to fight crime on the Dark Web and they’re mostly right, but there’s a good reason. They’ve already studied it and determined they don’t need it.

Negative: Dark Web / FBI 3

TOPICALITY 3

1. Nothing reformed 3

FBI (and other federal law enforcement agencies) already use AI for Dark Web investigation 3

Violation: “Doing more” of the Status Quo isn’t substantial reform. 3

Impact: No Affirmative team means Negative ballot 3

MINOR REPAIR 3

FBI officials admit Dark Web investigation isn’t very important. But if we did need it, all it takes is centralization of its existing programs 3

HARMS / SIGNIFICANCE 4

1. The “Dark Web” is not a crime, it’s a tool 4

It isn’t a crime to use the Dark Web and it has many legitimate uses. 4

SOLVENCY 4

1. Wrong solution #1 – Secure authentication is the answer 4

FBI cybersecurity expert says: AI is OK, but the best security is more secure user authentication 4

AI has small benefit but usually it’s too late: By the time you detect bad things with AI, they’ve already happened 4

2. Wrong solution #2 – Unnecessary distraction 5

FBI considered a comprehensive “dark web” strategy, but found it unnecessary. Focusing on a specific technology is the wrong approach 5

3. Lack of staffing and qualifications 5

Government has trouble ramping up expertise needed to manage the deep technology of AI 5

US Government has massive human talent deficit in AI 5

4. Whack-A-Mole 6

European Study finds: Dark Web enforcement accomplishes little. Shut down one and it’s immediately replaced by another 6

5. Missing components and More study needed 6

1) Planning Group is doing needed study right now. 2) Needs to involve 4 other agencies, not just FBI, to be effective 6

6. FBI “Finding more crime” on Dark Web won’t accomplish anything 7

Justice Dept. admits 4 reasons they couldn’t solve more Dark Web crime even if we found it: 1) Whack-a-mole, they just relocate and crime isn’t stopped. 2) Investigation alone won’t solve. 3) Lack of agents and prosecutors to make arrests and prosecute. 4) Absence of advanced tech tools to target end users. 7

A/T “But AFF provides the tech tools” (#4 above) 7

DISADVANTAGES 7

1. Civil Rights abuse 7

Increased digital surveillance capabilities lead to increased abuse of civil rights. Examples: FBI, Michigan State Police 7

Government investigation AI = racism and civil rights abuse 8

2. Conflicting investigations 8

Ramping up FBI Dark Web investigations is bad because: There are already so many agencies investigating that the FBI risks stepping on other investigations of the same targets 8

Impact: Injuries and deaths of law enforcement officers when investigations conflict 8

3. Taxpayer-funded child porn 9

FBI discovers child porn site on the Dark Web… and then CONTINUES RUNNING IT UNDER THEIR CONTROL. If you want more of that, go ahead and vote Affirmative, but I hope you have trouble sleeping at night… 9

Negative: Dark Web / FBI

TOPICALITY

1. Nothing reformed

FBI (and other federal law enforcement agencies) already use AI for Dark Web investigation

Cobwebs Technologies 2020 (cybersecurity consulting firm) What is Dark Web Monitoring and How Can it Power Cyber Investigations? 30 Dec 2020 <https://cobwebs.com/what-is-dark-web-monitoring-and-how-can-it-power-cyber-investigations/> (accessed 24 Jan 2022)

 Dark web monitoring tools involve crawlers powered by AI software that spend time in dark web forums and dark web social networks where stolen information is being sold and used maliciously. Once the crawler software picks up a match, the relevant financial and investigation authorities are notified.

What bodies stand to benefit from dark web monitoring?

Dark web monitoring is used by major governmental authorities to combat cybercrime and terrorism. Agencies like the FBI, Drug enforcement agencies, and Homeland Security use AI crime prediction software and dark web crawlers as a type of “neighborhood watch,” keeping their eye out for suspicious activities that may be part of a bigger case to solve.

Violation: “Doing more” of the Status Quo isn’t substantial reform.

It’s admission that the Status Quo is doing the right thing. A substantial reform would have been “banning” the FBI from using AI for Dark Web investigations.

Impact: No Affirmative team means Negative ballot

No one in this round is affirming the text of the resolution, so no matter who wins, you should write Negative on the ballot.

MINOR REPAIR

FBI officials admit Dark Web investigation isn’t very important. But if we did need it, all it takes is centralization of its existing programs

US Justice Dept, Office of the Inspector General 2020. “Audit of the Federal Bureau of Investigation’s Strategy and Efforts to Disrupt Illegal Dark Web Activities” Dec 2020 <https://oig.justice.gov/sites/default/files/reports/21-014.pdf> (accessed 24 Jan 2022) (brackets added)

There is no requirement that the FBI develop or maintain a formalized bureau-wide dark web strategy, and we found that the FBI does not have one. Instead, FBI operational units were executing individual dark web strategies—some documented, others not—with varying degrees of comprehensiveness. Senior FBI officials with whom we spoke had mixed opinions on the value of establishing such a formalized FBI-wide strategy. Some of these officials considered it unnecessary because the dark web is just a medium or platform to commit a crime and represented a small percentage of their unit’s operations, or because it did not make sense to have an overarching strategy for multiple divisions with different missions and goals. However, other FBI officials believed that an overarching strategy, or at least centralization of mutual activities, would be beneficial.

HARMS / SIGNIFICANCE

1. The “Dark Web” is not a crime, it’s a tool

It isn’t a crime to use the Dark Web and it has many legitimate uses.

**[Analysis: It’s like a gun – it’s a tool that can be used for good or bad. Investigating guns is a waste of time (and a possible civil rights violation, since it’s not a crime to own one) – when we should be investigating homicides. You’ll see later in our evidence that the FBI agrees with this analysis, and that’s why they don’t have a comprehensive “Dark Web Strategy.” They’re focused on the crimes, not the tool.]**

US Justice Dept, Office of the Inspector General 2020. “Audit of the Federal Bureau of Investigation’s Strategy and Efforts to Disrupt Illegal Dark Web Activities” Dec 2020 <https://oig.justice.gov/sites/default/files/reports/21-014.pdf> (accessed 24 Jan 2022)

The terms “dark web” and “darknet” are often used to refer to a part of the Internet that consists of services and websites that cannot be accessed through standard web browsers; instead, specific software, configurations, or authorization is needed for access. While accessing the dark web is not illegal, dark web sites are often used to engage in illegal activities.
**END QUOTE. THEY GO ON LATER IN THE SAME CONTEXT SAYING QUOTE**:
Many users access the dark web for legitimate purposes, including to discuss socially sensitive matters or counter censorship in oppressive areas of the world. However, dark web sites are also used to engage in illegal activities, such as trafficking drugs; firearms and weapons of mass destruction; child sexual abuse material; malware; and other illicit goods and services.

SOLVENCY

1. Wrong solution #1 – Secure authentication is the answer

FBI cybersecurity expert says: AI is OK, but the best security is more secure user authentication

PYMNTS 2021 (consulting firm that does online security for electronic payments and transfer of money) 8 July 2021 “FBI: Why AI And MFA Provide The Most Effective Fraud Defense” <https://www.pymnts.com/fraud-prevention/2021/fbi-ai-mfa-cybercrime-defense/> (accessed 24 Jan 2022)

“In our collection of cyber fraud investigations that we have within the cyber division of the FBI, [we found that] 99 percent of attacks leveraged compromised username [and] password combinations,” said Alvarez. “This is stuff that they’re finding on the dark web, or [gained from] brute-forcing simple passwords because humans just can’t remember more sophisticated passwords.” Businesses are working on several countermeasures to prevent these attacks as permanent work-from-home operations become more widespread. AI-based systems have their uses, Alvarez said, but the best security systems rely on more secure user authentication.

AI has small benefit but usually it’s too late: By the time you detect bad things with AI, they’ve already happened

PYMNTS 2021 (consulting firm that does online security for electronic payments and transfer of money) 8 July 2021 “FBI: Why AI And MFA Provide The Most Effective Fraud Defense” <https://www.pymnts.com/fraud-prevention/2021/fbi-ai-mfa-cybercrime-defense/> (accessed 24 Jan 2022)

The primary benefit of AI-based systems, according to Alvarez, is that they can detect minute patterns and inconsistencies fraudsters may cause that human analysts might not catch. These analyses are typically only performed while a fraudster is already in the system or has just left it, though, meaning that a reliance on these systems can risk the loss of precious data, even if the fraudster is caught. “You can definitely leverage these sophisticated tools to understand how your enterprise works on a regular day, and then [see when] that weird anomaly starts happening, like sending data to an abnormal IP,” said Alvarez. “But that’s a bad day because that means the intruders have been in the enterprise for a while. It’s a truism in our cyber-intrusion cases that most of the self-reporting we get from the victims is when they see data leaving.” The best way to prevent fraud is by keeping fraudsters from ever entering the system in the first place through ironclad customer and employee authentication.

2. Wrong solution #2 – Unnecessary distraction

FBI considered a comprehensive “dark web” strategy, but found it unnecessary. Focusing on a specific technology is the wrong approach

US Justice Dept, Office of the Inspector General 2020. “Audit of the Federal Bureau of Investigation’s Strategy and Efforts to Disrupt Illegal Dark Web Activities” Dec 2020 <https://oig.justice.gov/sites/default/files/reports/21-014.pdf> (accessed 24 Jan 2022) (brackets added)

Like the CEOU [FBI Child Exploitation Operational Unit] and IU [Investigative Unit], MCCU [Major Cyber Crimes Unit] did not maintain a formalized, comprehensive dark web strategy. MCCU officials initially said this was because its dark web efforts were a small component of its broader cyber strategy. However, these officials acknowledged that the MCCU needed to better define how it measured investigative success on the dark web. MCCU therefore drafted a dark web strategy in February 2019 that contained objectives, initiatives, and performance measures. However, this strategy was never finalized because new senior MCCU officials decided that their predecessors’ draft dark web strategy was unnecessary. These officials stated that any strategy developed by the MCCU should address the entire unit and not be specific to technologies, such as Tor.

3. Lack of staffing and qualifications

Government has trouble ramping up expertise needed to manage the deep technology of AI

Prof. Ryan Calo 2017. (Associate Professor, University of Washington School of Law; hosted the first White House workshop on artificial intelligence policy, organized AI workshops for the National Science Foundation) Artificial Intelligence Policy: A Primer and Roadmap <https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_Calo.pdf> (accessed 8 Aug 2021)

The better-grounded observation is that government lacks the requisite expertise to manage society in such a deeply technically-mediated world. Government bodies are slow to hire up and face steep competition from industry. When the state does not have its own experts, it must either rely on the self-interested word of private firms (or their proxies) or experience a paralysis of decision and action that ill-serves innovation. Thus, one overarching policy challenge is how best to introduce expertise about AI and robotics into all branches and levels of government so they can make better decisions with greater confidence. [**END QUOTE**] The solution could involve new advisory bodies, such as an official Federal Advisory Committee on Artificial Intelligence with an existing department or even a standalone Federal Robotics Commission.143 Or it could involve resuscitating the Office of Technology Assessment, building out the Congressional Research Service, or growing the Office of Science and Technology Policy. Yet another approach involves each branch hiring its own technical staff at every level. [**HE GOES ON TO CONCLUDE IN THE SAME CONTEXT QUOTE:]** The technical knowledge and affordances of the government — from the ability to test claims in a laboratory to a working understanding of AI in lawmakers and the judiciary — will ultimately affect the government’s capacity to generate wise AI policy.

US Government has massive human talent deficit in AI

National Security Commission on Artificial Intelligence 2021 (bipartisan commission of 15 technologists, national security professionals, business executives, and academic leaders) March 2021 “Final Report” <https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf> (accessed 17 June 2021)

The human talent deficit is the government’s most conspicuous AI deficit and the single greatest inhibitor to buying, building, and fielding AI-enabled technologies for national security purposes. This is not a time to add a few new positions in national security departments and agencies for Silicon Valley technologists and call it a day. We need to build entirely new talent pipelines from scratch.

4. Whack-A-Mole

European Study finds: Dark Web enforcement accomplishes little. Shut down one and it’s immediately replaced by another

US Justice Dept, Office of the Inspector General 2020. “Audit of the Federal Bureau of Investigation’s Strategy and Efforts to Disrupt Illegal Dark Web Activities” Dec 2020 <https://oig.justice.gov/sites/default/files/reports/21-014.pdf> (accessed 24 Jan 2022) (brackets added)

According to the Department, Tor and the existence of DNMs [Dark Net Marketplaces] is one of the greatest impediments to its efforts at disrupting cybercriminal activities. A related challenge for law enforcement is the resiliency of DNMs and forums. Europol reported that over 100 DNMs offering drugs have operated from 2010 to 2018, usually lasting less than a year before closing due to law enforcement action, scams, hacking, or voluntary exits. For several years now, prominent DNMs have been shuttered by law enforcement for alleged violations of federal laws—including distribution of controlled substances, money laundering, access device fraud, and identity theft—just to be immediately replaced by successor DNMs to which vendors and buyers migrate.

5. Missing components and More study needed

1) Planning Group is doing needed study right now. 2) Needs to involve 4 other agencies, not just FBI, to be effective

US Justice Dept, Office of the Inspector General 2020. “Audit of the Federal Bureau of Investigation’s Strategy and Efforts to Disrupt Illegal Dark Web Activities” Dec 2020 <https://oig.justice.gov/sites/default/files/reports/21-014.pdf> (accessed 24 Jan 2022) (brackets added)

Department officials outside the FBI, particularly from the Criminal Division, have recognized the need for a government-wide dark web strategy, having created the Department Dark Web Strategic Planning Group in 2017 to “devise, cultivate, and implement comprehensive strategies to investigate, prosecute, and deter serious criminal activity occurring via the Dark Web.” The Dark Web Strategic Planning Group aims to develop a nationwide dark web strategy that focuses on key challenges and issues. As of March 2020, the group was still developing a formalized strategy. Members of the group include the FBI; Drug Enforcement Administration (DEA); Criminal Division; Department of Homeland Security, Homeland Security Investigations; U.S. Postal Inspection Service; and Internal Revenue Service, Criminal Investigation Division.

6. FBI “Finding more crime” on Dark Web won’t accomplish anything

**Remember, even if AI were effective, all it can do it suggest where it might be and tell you where to look for it. It can’t do the investigations, make the arrests and prosecute the offenders. And that’s where things break down…**

Justice Dept. admits 4 reasons they couldn’t solve more Dark Web crime even if we found it: 1) Whack-a-mole, they just relocate and crime isn’t stopped. 2) Investigation alone won’t solve. 3) Lack of agents and prosecutors to make arrests and prosecute. 4) Absence of advanced tech tools to target end users.

US Justice Dept, Office of the Inspector General 2020. “Audit of the Federal Bureau of Investigation’s Strategy and Efforts to Disrupt Illegal Dark Web Activities” Dec 2020 <https://oig.justice.gov/sites/default/files/reports/21-014.pdf> (accessed 24 Jan 2022) (brackets added)

As previously noted, the CEOU [FBI Child Exploitation Operational Unit] shifted in recent years from targeting all CSAM site users and consumers (such as in Operation Pacifier), to targeting site administrators who facilitated the communication and transmission of CSAM [Child Sexual Abuse Material] content. We find this shift concerning because the FBI and Criminal Division previously determined that simply shutting down a site was not sufficient, as consumers of this illicit content can migrate to other dark web locations, resulting in little or no disruption of access to CSAM. CEOU officials responded that the exponential growth of the threat forced the FBI to reprioritize its efforts and that this strategic shift was based on consultation with its international partners and the Department, and due to: (1) general agreement among the law enforcement community that investigation alone will not address the problem, (2) a lack of law enforcement and prosecutive resources to address mass numbers of individual investigations, and (3) the absence of advanced technical tools to target large numbers of end users.

A/T “But AFF provides the tech tools” (#4 above)

1) FBI needs tools to target end users, not websites like AFF does.
2) AFF can’t solve the other 3 things. Whack-a-mole never gets solved by anything. And AFF can’t hire more FBI field agents or prosecutors because those are extra-topical.

DISADVANTAGES

1. Civil Rights abuse

Increased digital surveillance capabilities lead to increased abuse of civil rights. Examples: FBI, Michigan State Police

Michael Kwet 2021 (journalist) 21 Sept 2021 “SHADOWDRAGON: INSIDE THE SOCIAL MEDIA SURVEILLANCE SOFTWARE THAT CAN WATCH YOUR EVERY MOVE” (accessed 24 Jan 2022) https://theintercept.com/2021/09/21/surveillance-social-media-police-microsoft-shadowdragon-kaseware/

This new revelation about the Michigan contract raises questions about what digital surveillance capabilities other police departments and law enforcement agencies in the U.S. might be quietly acquiring. And it comes at a time when previously known government social media surveillance is [under fire](https://www.aclunc.org/news/aclu-demands-twitter-take-immediate-action-stop-developers-facilitating-government) from civil rights and liberties advocates like MediaJustice and the American Civil Liberties Union. It also raises the specter of further abuses in Michigan, where the FBI has been [profiling Muslim communities](https://archive.thinkprogress.org/fbi-using-its-black-identity-extremists-report-c647091135ab/) and so-called [Black Identity Extremists](https://theintercept.com/2018/03/19/black-lives-matter-fbi-surveillance). In 2015, it was revealed that for years, the state police agency was using cell site simulators to spy on mobile phones without disclosing it to the public. “Social media surveillance technologies, such as the software acquired by Michigan State Police, are often introduced under the false premise that they are public safety and accountability tools. In reality, they endanger Black and marginalized communities,” Arisha Hatch, vice president and chief of campaigns at civil rights nonprofit Color of Change, wrote in an email.

Government investigation AI = racism and civil rights abuse

Michael Kwet 2021 (journalist) 21 Sept 2021 “SHADOWDRAGON: INSIDE THE SOCIAL MEDIA SURVEILLANCE SOFTWARE THAT CAN WATCH YOUR EVERY MOVE” (accessed 24 Jan 2022) https://theintercept.com/2021/09/21/surveillance-social-media-police-microsoft-shadowdragon-kaseware/

With Kaseware and ShadowDragon, we live in a world where the public’s online behavior can be monitored across the internet and accessed at the click of a button to determine who we are, who we know, what our “lifestyle” is like, where we are located, and more. These capabilities fundamentally change police powers, said Eric Williams, managing attorney at the Detroit Justice Center’s Economic Equity Practice: “It is qualitatively different when you go from the police being able to check information” a little at a time “to artificial intelligence being able to analyze everything that you’ve done online.” The potential for discriminatory applications is enormous. Williams noted that searches made by big data tools are “inevitably biased against people of color, poor people” and the like. He said that activists from Black Lives Matter, unions, and the #MeToo movement may be targeted by these technologies, “depending on who is in charge of them.”

2. Conflicting investigations

Ramping up FBI Dark Web investigations is bad because: There are already so many agencies investigating that the FBI risks stepping on other investigations of the same targets

**[One target was being investigated at the same time by: multiple FBI offices, the Drug Enforcement Agency, the Postal Service and the Dept of Homeland Security!]**

US Justice Dept, Office of the Inspector General 2020. “Audit of the Federal Bureau of Investigation’s Strategy and Efforts to Disrupt Illegal Dark Web Activities” Dec 2020 <https://oig.justice.gov/sites/default/files/reports/21-014.pdf> (accessed 24 Jan 2022) (brackets added)

FBI units operating on the dark web are frequently at risk of unknowingly crossing into the investigation of another government agency or even another FBI unit. Therefore, timely deconfliction of investigative data among law enforcement agencies is essential to ensure agent safety, preserve the integrity of ongoing investigations, and share information to identify targets of common investigative interest. [**END QUOTE**] In May 2014, the Department issued a memorandum requiring all Department law enforcement components to enter investigative data into deconfliction systems, including the Deconfliction and Information Coordination Endeavor (DICE). DICE provides real-time connectivity to deconfliction information and once a common link has been identified, appropriate personnel are notified and provided contact information to share, coordinate, and avoid conflicting equities. Investigative data subject to DICE deconfliction include social network identifiers, online monikers, addresses, phone numbers, dates of birth, email addresses, IP addresses, bitcoin wallet addresses, and financial account numbers. (U) **[THEY CONTINUE LATER IN THE CONTEXT QUOTE**:] During our review of the FBI’s dark web UCOs [Under Cover Operations], we identified investigative data, such as subject monikers, OCE [Online Covert Employee] monikers, and shipping addresses that were being investigated by different FBI field offices and non-DOJ components. For example, one subject moniker was being targeted by multiple FBI field offices, the DEA, U.S. Postal Inspection Service, and DHS.

Impact: Injuries and deaths of law enforcement officers when investigations conflict

Bureau of Justice Assistance, Office of Justice Programs 2013. (agency of US Dept. of Justice) Oct 2013 A Call to Action: Enhancing Officer Safety Through the Use of Event Deconfliction Systems (accessed 24 Jan 2022) https://ncirc.bja.ojp.gov/sites/g/files/xyckuh326/files/media/document/event\_deconfliction\_call\_to\_action.pdf

Without event deconfliction, officers may unintentionally interfere with another law enforcement operation or action, potentially resulting in injury or death to officers or a negative impact on an investigation.

3. Taxpayer-funded child porn

FBI discovers child porn site on the Dark Web… and then CONTINUES RUNNING IT UNDER THEIR CONTROL. If you want more of that, go ahead and vote Affirmative, but I hope you have trouble sleeping at night…

US Justice Dept, Office of the Inspector General 2020. “Audit of the Federal Bureau of Investigation’s Strategy and Efforts to Disrupt Illegal Dark Web Activities” Dec 2020 <https://oig.justice.gov/sites/default/files/reports/21-014.pdf> (accessed 24 Jan 2022)

In 2015, the FBI seized a child sexual abuse material (CSAM) site on the Tor network called “Playpen” and, instead of shutting it down, continued to run it from a government site in the Eastern District of Virginia for about 2 weeks. The FBI and Criminal Division determined that simply shutting down the site was not sufficient, as users would migrate to a different website. They decided that every effort should be taken to identify as many users as possible. During the approximately 2-week site seizure, the FBI deployed a network investigative technique (NIT) that gathered identifying information from Playpen users’ computers. The single NIT warrant, executed in Virginia, implicated more than 100 defendants across the U.S. This FBI effort, called Operation Pacifier, generated controversy because of the ethical and moral implications of the U.S. government allowing a child exploitation site to continue to operate under law enforcement control.