Magistrate Judge Brian A. Tsuchida

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. CAMERON JOHN WAGENIUS, Defendant.	CASE NO. CR24-232 LK **UNITED STATES' MEMORANDUM IN SUPPORT OF CONTINUED DETENTION**

Defendant Cameron John Wagenius is charged with—and noticed his intent to plead guilty to—unlawfully posting and transferring confidential phone records information, including those allegedly pertaining to high-ranking public officials. As detailed below and in the supplemental memorandum filed under seal, the circumstances surrounding Wagenius' decision to post these sensitive records, along with evidence of additional cybercriminal conduct, suggests a willingness to harm victims for his own personal benefit through the release of stolen information. Equally concerning, the government found evidence that, while engaged in these criminal activities, Wagenius conducted online searches about how to defect to countries that do not extradite to the United States and that he previously attempted to sell hacked information to at least one foreign intelligence service. Additionally, Wagenius violated his commanding officer's orders by purchasing a new laptop *after* a federal search warrant was executed at his barracks room and his electronic devices were seized, which raises concerns about his

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

willingness to comply with any conditions of release. For these reasons, Wagenius should be detained as both a danger to the community—given his ability to access sensitive datasets—and a serious risk of flight.

I. BACKGROUND

A. Wagenius' Criminal Activities

1. Wagenius Attempted to Extort Victim-1[1] While Transferring Highly Sensitive Stolen Data

The charged conduct relates to Wagenius' multiple public online posts on or about November 6, 2024, using his online monikers, kiberphant0m and cyb3rph4nt0m. Specifically, Wagenius posted highly sensitive call detail records purportedly belonging high-ranking public officials and their family members and threatened to release additional phone records belonging to the same individual victims unless Victim-1, a major telecommunications company, contacted him or an intermediary to pay a ransom.

In addition to the public posts, Wagenius engaged in multiple direct attempts to extort Victim-1. Wagenius demanded $500,000 and made clear threats to Victim-1:

> Lets start off, a little thing you should know about me. I get what I want and when I don't get what I want in my own timeframes that I set I will do what I say. I don't care if I don't receive the money involved in the extortions. I already made your samples and data on [REDACTED] available to everybody on breachforums. I will leak much much much more, literally all of it.

These threats were made while Wagenius was on active duty with the U.S. Army,[2] stationed at Fort Cavazos. Pursuant to a search warrant, the government identified copies of the sensitive phone records on Wagenius' devices.

---

[1] The government filed a Notice of Related Case in *United States v. Connor Riley Moucka and John Erin Binns*. Case No. CR24-180 LK, Dkt. No. 11. The victims identified in this memorandum do not correspond to the victim numbers identified in the Indictment in the related case. *See id.* (Dkt. No. 1).

[2] Wagenius is presently in the process of being separated from the Army but, as of the date of this filing, the government has not received confirmation that his discharge has been finalized. The government's understanding is that, until his discharge from the Army is finalized (which is expected to happen in early March), he may only be released directly to the Army. Until that process is completed, Wagenius' proposed release to his father should be rejected for this additional reason.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

2. Wagenius Engaged in Other Malicious Cyber Activity Over a Prolonged Period of Time and Attempted to Sell Information to at Least One Foreign Intelligence Service While He Held a Security Clearance

As discussed in the government's sealed filing, the government has uncovered evidence suggesting that the charged conduct was only a small part of Wagenius' malicious activity. On top of this, for more than two weeks in November 2024, Wagenius communicated with an email address he believed belonged to Country-1's military intelligence service in an attempt to sell stolen information.[3] Days after he apparently finished communicating with Country-1's military intelligence service, Wagenius Googled, "can hacking be treason."

3. After His Devices Were Seized, Wagenius Violated Military Orders, Purchased a New Laptop, and Used Virtual Private Network ("VPN") Software

On or about December 6, 2024, about two days after Wagenius' devices were seized by federal law enforcement, Wagenius' commanding officer provided orders restricting Wagenius from "using or purchasing any technology such as laptops, tablets, cell phones, etc." Wagenius was advised that disregarding the verbal order could lead to action under the Uniform Code of Military Justice. Wagenius verbally acknowledged and confirmed that he understood the order. Nevertheless, the very next day, Wagenius violated this direct order by purchasing a new laptop and using it in the barracks. Army authorities seized the laptop and a corresponding receipt (dated December 7) pursuant to an order by a military magistrate judge.

Wagenius continued to violate the order by using the laptop every day between December 8 and December 12—when it was seized by the Army. He used VPN software on this new laptop. This VPN software does not keep logs of Internet Protocol addresses, session lengths, or web pages visited. In this way, this VPN software can be useful to

[3] The government has not verified whether that email address belongs to Country-1's military intelligence service. What is significant, however, is that Wagenius believed that it did.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

cybercriminals attempting to obfuscate their identity and/or location. The government continues to investigate Wagenius' conduct during this time period given concerns that he could have been engaging in new hacking activities or further leaking stolen victim data.

4. Evidence Wagenius Has the Means and Intent to Flee

Throughout October 2024, as he engaged in his criminal activity, Wagenius conducted online searches related to fleeing the United States. For example, he searched:

- "where can i defect the u.s government military which country will not hand me over";
- "U.S. military personnel defecting to Russia"; and
- "Embassy of Russia – Washington, D.C."

These are just a subset of Wagenius' searches indicating a desire to flee the United States, and the searches occurred over multiple weeks. He also searched for information about defecting to Country-1, the country to which he attempted to sell stolen information in November.

In October 2024, Wagenius messaged a potential co-conspirator, explaining that, "whats funny is that if i ever get found out / i cant get instantly arrested / because military law / **which gives me time to go AWOL**" (emphasis added). In May, Wagenius conducted an online search for "how to get passport fast."

Finally, the government has obtained evidence on Wagenius' devices indicating that Wagenius has access to thousands of stolen identification documents, including passports and driver's licenses, as well as access to large amounts of cryptocurrency. Law enforcement is still working to understand Wagenius' exact access to such information and assets, including whether Wagenius controls cloud storage accounts that store stolen information. During a review of Wagenius' devices, the government also obtained evidence indicating that Wagenius has created at least one fake identification document for himself in the past.

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

//

II. LEGAL STANDARD

After a guilty plea is entered, the defense bears the burden of proving by clear and convincing evidence that the defendant "is not likely to flee or pose a danger to the safety of any other person or the community if released." 18 U.S.C. § 3143(a)(1). Otherwise, the judicial officer "shall order" the defendant detained pending sentencing. *Id; see also* Fed. R. Crim. P. 46(c) ("[t]he burden of establishing that the defendant will not flee or pose a danger to any other person or the community rests with the defendant" and 18 U.S.C. § 3143 governs release pending sentencing).

This is a much higher standard than applies when a defendant has pleaded not guilty and is still pending trial. In that case, 18 U.S.C. § 3142(f)(2)(A) provides that a judicial officer shall "hold a hearing to determine whether any condition or combination of conditions . . . will reasonably assure the appearance of [the defendant] and the safety of any other person and the community." At a detention hearing, § 3142(g) provides that the court shall consider the following factors:

(1) the nature and circumstances of the offense charged;

(2) the weight of the evidence against the person;

(3) the history and characteristics of the person . . . and

(4) the nature and seriousness of the danger to any person or the community that would be posed by the person's release . . . .

A court shall order a defendant detained pending trial if, after a hearing, it finds that "no condition or combination of conditions will reasonably assure the appearance of the person as required and the safety of any other person and the community." 18 U.S.C. § 3142(e)(1).

III. ARGUMENT

Since Wagenius is expected to plead guilty on the same day as the detention hearing, Wagenius has the burden of proving by clear and convincing evidence that he is not a flight risk or danger to the public, which he cannot meet. Even if he does not have the burden of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

proof, all four § 3142(g) factors strongly favor detention, so Wagenius should be detained regardless of whether a guilty plea is entered. Wagenius' conduct over the last several years, probable access to sensitive stolen victim data, statements about defecting, and conduct after the execution of a federal search warrant indicate that "[t]here are no conditions of release that will reasonably assure the appearance of [Wagenius] as required and the safety of any other person and the community." 18 U.S.C. § 3142(g).

A. Wagenius Presents a Significant Danger to the Community

Wagenius' demonstrated willingness to leak stolen data, as discussed in more detail in the government's sealed filing, creates a serious danger to the community.

1. Nature and circumstances of the offense charged

The nature and circumstances of the charged offenses counsel strongly in favor of detaining Wagenius as a danger to the community. Wagenius, an active-duty member of the U.S. Army who possessed a security clearance, publicly posted and caused the transfer of confidential and sensitive phone records believed to belong to high-ranking public officials and/or their family.

Call detail records are inherently sensitive, as they contain information about the identity and frequency of a person's contacts. In this case, the stolen data did not include customer names, but the data Wagenius posted was enriched to include names associated with specific telephone numbers. Congress specifically enacted 18 U.S.C. § 1039 in 2006 to "preserve consumers' privacy rights and to protect the personal safety of domestic violence victims, confidential informants, witnesses, jurors, and law enforcement personnel." H.R. Rep. 109-395, 3, 2006 U.S.C.C.A.N. 1911, 1913. Wagenius' release of the stolen call records violated the very rights that § 1039 sought to protect.

2. Weight of the evidence

The weight of the evidence in this matter is overwhelming. Copies of the confidential phone records were found on Wagenius' phone and his laptop, which were obtained pursuant to a search warrant. Multiple devices contained communications or

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

exports of communications from the kiberphant0m account that made the posts at issue.

3. History and characteristics of Wagenius

While Wagenius is just 21 years old, he has a long history of involvement in malicious cyber activity as outlined in the government's sealed memorandum. That Wagenius engaged in malicious cyber activity while on active duty with the U.S. Army and in violation of a commanding officer's orders raises serious concerns about his ability to comply with any conditions of release. Importantly, once discharged from the Army, Wagenius will have no employment and if released, he will have the time and the means to resume his malicious cyber activities.

4. Nature and seriousness of the danger to the community

The broad scope of Wagenius' conduct, the large amounts of stolen data, and the significant number of victims create a serious danger that Wagenius will expose additional stolen data or attempt to further extort victims if released. The danger to the public is amplified by the possibility that Wagenius may be able to access remote servers and cloud storage accounts when he gains access to the internet, and there are potentially gigabytes of sensitive victim information that have not yet been recovered.

Wagenius has repeatedly demonstrated his inability to resist posting stolen data. He posted offers to sell stolen information on criminal forums throughout 2024, leaked victim data in November 2024, and then proceeded to violate military orders in December 2024 when he was on active duty—because he could not resist the urge to access the internet. The government continues to investigate what actions Wagenius took after he obtained the new laptop in December, but there is already evidence that he sought to obfuscate his activity by using VPN software.

B. Wagenius Should be Detained Because He Presents a Serious Flight Risk

Wagenius should also be detained because he presents a serious risk of flight, has the means and intent to flee, and is aware that he will likely face additional charges.

First, Wagenius conducted multiple, detailed searches about defecting from the U.S.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Army and fleeing the United States over the course of weeks in the lead up to his arrest. In October, he Googled, "where can i defect the u.s government military which country will not hand me over" and specifically searched for how to "defect[] to Russia." He searched this just days after explaining to a potential co-conspirator that he could not be arrested right away if authorities found out his true identity, which would give him "time to go AWOL." In addition to his attempts to sell information to Country-1's intelligence service, he conducted at least one search about defecting to that country—which might have a motivation to provide a safe haven, given his attempts to sell that country data about another foreign country.

Second, the government found evidence on Wagenius' devices suggesting he has access to large numbers of identification documents. For example, a screenshot on his laptop suggested he had over 17,000 files that included passports, driver's licenses, and other identity cards belonging to victims of a breach. In one of his online accounts, the government also found a fake identification document that contained his picture.

Additionally, Wagenius knows that additional charges are likely forthcoming, providing yet another incentive to flee the United States. Taken together, these facts all demonstrate that Wagenius has multiple motivations, the technical sophistication, and the means to flee.

C. No Combination of Conditions Can Adequately Protect the Community or Assure Wagenius' Appearance

Based on discussions with defense counsel, the government understands that Wagenius proposes being released to his father and would agree to home confinement and to not possess or use a computer or internet-connected phone. This release plan is not viable given Wagenius' recent conduct. Wagenius demonstrated an inability to comply with conditions related to his internet use in December, when he purchased a laptop a day after receiving a military order not to do so. He used the computer daily, and he used his technical knowledge to install and use VPN software that is commonly used by

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

cybercriminals to obfuscate malicious activity. At this time, Wagenius already knew he was under investigation by federal law enforcement, as his devices had been seized, and he knew that Army authorities had imposed restrictions on him and were attempting to monitor his behavior—yet he was still able to purchase and use the laptop. This is the exact behavior that is likely to occur if he is released to home confinement.

Wagenius had opportunities to comply with restrictions placed on his activities and demonstrated that he cannot do so. At home, there would be even fewer people checking on him than was the case at Fort Cavazos. The check-ins would be less often, leaving Wagenius on his own for the entire workday. Furthermore, while the government has seized extensive amounts of victim data, there is reason to believe that Wagenius still has ready access to sensitive stolen information that he could provide to co-conspirators or potential buyers—or use to further extort victims—because he used cloud-based services to store victim data from numerous companies.

IV. CONCLUSION

The range of Wagenius' criminal conduct is extensive and the charges in the current Indictment do not cover all of it. In light of the evidence proffered by the government, Wagenius presents serious danger to the public and risk of flight. Given his willingness to

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

sell stolen information to any buyer on criminal forums and to foreign intelligence agencies, his ready access to significant amounts of sensitive victim data, his desire to flee to countries that do not extradite to the United States, and his prior noncompliance with restrictions, there is no reasonable combination of conditions that will reasonably assure his appearance or the safety of the public.

DATED this 26th day of February, 2025.

Respectfully submitted,

TEAL LUTHY MILLER
Acting United States Attorney

/s/ Sok Tea Jiang

SOK TEA JIANG
Assistant United States Attorneys
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970
sok.jiang@usdoj.gov

ANTOINETTE T. BACON
Supervisory Official, Criminal Division

/s/ George Brown

GEORGE BROWN, Trial Attorney
LOUISA K. BECKER, Senior Counsel
Computer Crime & Intellectual Property Section
U.S. Department of Justice
1301 New York Ave NW
Washington, D.C. 20530
(202) 514-3597
louisa.marion@usdoj.gov
george.brown@usdoj.gov

I certify that this memorandum contains 2,799 words, in compliance with the Local Criminal Rules