



U.S. Department of Justice

Matthew M. Graves
United States Attorney

District of Columbia

*Patrick Henry Building
601 D Street, N.W.
Washington, D.C. 20530*

October 7, 2022

Via email

Nicholas Smith
David Smith
*Counsel for Ethan
Nordean*

J. Daniel Hull
Norman A. Pattis
Counsel for Joseph Biggs

Carmen D. Hernandez
Counsel for Zachary Rehl

Steven Metcalf II
Counsel for Dominic Pezzola

Nayib Hassan
Sabino Jauregui
Counsel for Enrique Tarrio

Re: ***United States v. Ethan Nordean, et al.*** (Case No. 21-cr-175 (TJK))

Dear Counsel:

We write, pursuant to the Court's scheduling order (ECF No 426) to provide additional notice/report of FBI's Senior Digital Forensic Examiner Jennifer Kathryn Cain's anticipated testimony at trial in this matter. A copy of Examiner Cain's *curriculum vitae* is attached hereto.

Examiner Cain has been with the FBI for over nine years and has served as a digital forensic examiner for approximately five years, earning the "senior examiner" certification in 2021. Her expert qualifications are further detailed in her curriculum vitae, which is attached at Tab 1.

As you know, the government seized a significant amount of evidence in the form of photographs, videos, and messages extracted from the digital devices and Stored Communications Act (“SCA”) accounts of the defendants, co-conspirators, and other subjects and witnesses in this investigation. It is the government’s position that electronic evidence seized from digital devices and SCA accounts will be admissible through lay/fact witness testimony by FBI special agents or members of the FBI’s Computer Analysis Response Team (“CART”) who extracted, located, and/or reviewed this evidence. If a law enforcement witness simply testifies to what files he or she found on a digital device or account, his or her testimony is not expert testimony. *See United States v. Berry*, 318 Fed. Appx. 569, 570 (9th Cir. 2009) (agent’s testimony was not expert testimony because the agent “simply testified to what he found on the [defendant’s] hard drive..., without expressing an opinion that required specialized knowledge or offering insight beyond common understanding”) (citing Fed. R. Evid. 702). Please let us know immediately if you disagree with this position so that we can raise this issue with the Court well in advance of trial.

The government does intend to seek to qualify Examiner Cain as an expert in the field of digital forensic analysis and to have Examiner Cain offer some background testimony about how data is extracted, processed, and analyzed from digital devices and social media accounts, and then to offer testimony about conclusions she drew about a limited subset of the electronic evidence in this case. We will follow this notice with more specific notice regarding the limited subset of electronic evidence in this case. We expect Examiner Cain to provide information about devices recovered from at least the following individuals: Gabriel Garcia, Ethan Nordean, Nicholas Ochs, Paul Rae, Zachary Rehl, and Enrique Tarrio.

- i. Examiner Cain will provide a basic overview of how data is extracted from cellular telephones and similar digital devices and then processed and examined, including certain specific steps that need to be taken to extract data from certain messaging platforms, including Telegram, from certain devices.
- ii. Examiner Cain will provide testimony about what the Telegram application is and how it works. Examiner Cain will testify that Telegram is an encrypted communications application, available for use on mobile devices and computers. Examiner Cain will explain that encryption ensures a method of secure communication that prevents third parties from accessing data while it is transferred from one end system or device to another. As it travels to its destination, the message cannot be read or tampered with by an internet service provider (“ISP”), application service provider, or any other entity or service. Examiner Cain will explain that this technology makes it harder for providers to share user information from their services with law enforcement authorities.
- iii. Examiner Cain will testify about how group chats are set up and administered on the Telegram application and will walk the jury through what group chats look like and how to read them. Examiner Cain will explain that by default, if one joins a Telegram group chat after it was created, one will not see the prior chats and will only be able to see the chats from the point that person joined, going forward. Examiner Cain will explain how chats can be deleted on Telegram group chats and by whom. She will testify that the operating system used by the user can affect what chats may be visible in a later forensic search.
- iv. Examiner Cain will explain that, by convention, many cellular telephone service providers, cellular telephone manufacturers, and social media and e-mail providers save their records and data using a twenty-four hour clock similar to “military” time and based on the 0° longitude meridian, also known as the “Greenwich meridian” (“GMT” or “GMT+0”). Universal Coordinated Time (“UTC” or “UTC+0”) refers to the time on

that zero or Greenwich meridian. To convert UTC+0 time into local time here in the United States, one needs to subtract a certain number of hours from UTC depending on how many time zones away one is from Greenwich, England. Examiner Cain will explain that for the period of December 2020 through January 2021, Eastern Standard Time was five hours behind UTC+0 and referred to as UTC-5; Central Standard Time was six hours behind and referred to as UTC-6; Mountain Standard Time was seven hours behind and referred to as UTC-7; and Pacific Standard Time was eight hours behind and referred to as UTC-8.

- v. Examiner Cain will offer some background testimony on how, generally, a forensic examiner can determine if and when data was deleted from a device or account.

If you have any questions, please do not hesitate to contact us.

Sincerely yours,

MATTHEW M. GRAVES
UNITED STATES ATTORNEY

By: /s/
Conor Mulroe
Trial Attorney
U.S. Dept. of Justice, Criminal Division
(202) 330-1788
Conor.Mulroe@usdoj.gov

 /s/
Jason B.A. McCullough
Erik M. Kenerson
Nadia E. Moore
Assistant United States Attorneys
601 D Street N.W.
Washington, D.C. 20530

Enclosure