Summary of Searches Conducted by CBP

Privacy Int'l, et al. v. FBI, et al.

- Plaintiffs' Freedom of Information Act (FOIA) request, dated September 10, 2018, was received by U.S. Customs and Border Protection (CBP) on October 2, 2018.

    - Plaintiffs' FOIA request sought CBP records concerning "hacking techniques" or "equipment." In response to Plaintiffs' FOIA request, CBP's FOIA Division contacted the offices within CBP in which it determined responsive records, if they existed, were likely to be found (with a focus on CBP's primary enforcement groups): Air & Marine Operations (AMO), the Office of Field Operations (OFO), and the U.S. Border Patrol (USBP) – along with the Office of Intelligence (OI) and the National Targeting Center (NTC). The FOIA Division requested that recipients be liberal in their interpretation of the request (e.g. considering terms other than "hacking techniques" as applying to what is described), and focused the recipients on p. 9-10 of the September 10, 2018 request from Plaintiffs. Responses for this initial request were negative.

    - Upon review of Plaintiffs' request, the FOIA Division concluded that the only reasonable and likely sources for responsive records were these aforementioned offices, in light of their duties and functions. Those offices, in turn, conducted reasonable searches, including searching all locations likely to have responsive records. Those searches are described below.

        - Other offices were contemplated, such as Procurement and the Office of Training and Development (OTD), but were deferred until first seeing whether primary enforcement groups had responsive documents (which they did not have).

        - Regarding communications, an e-mail search was deferred as it would in effect be asking to search all of CBP for any communications containing, for example, "hacking" or "techniques" (unless combined for search purposes), which would burden CBP resources.

    - The aforementioned offices were provided a copy of the FOIA request and, based on their experience and knowledge of their program office practices and activities, forwarded the request and instructions to the appropriated individual employee(s) and/or

component office(s) within the program office that they believed were likely to have responsive records, if such records existed.

- The individual(s) and component office(s) conducted searches of their file systems, including paper files and electronic files, which, in their judgment, based on their knowledge of the manner in which they routinely keep records, would be likely to contain responsive documents, if they existed.

- In July 2019, the FOIA Office sent the same offices a request to conduct another search based on the interpretation of the investigative technique as defined by defendants in the letter to July 12, 2019 letter to Jonathan Manes from Marcia Sowles. Defendants interpreted the request as seeking"[r]ecords related to investigative techniques that involve remote transmittal of code to effect the agency's ability to access, without the owner's knowledge, information from computer systems or other devices not in the Government's possession that have been deployed in criminal and/or civil law enforcement investigations, including but not limited to the following: immigration, customs, border, tax, drugs, computer crimes, and financial enforcement efforts."

  - Responses to this revised request, also focusing recipients on the other parameters identified in the September 10, 2018 FOIA request, were negative from: the Office of Information & Technology (OIT); OIT-Laboratory & Scientific Services Directorate (LSSD); NTC; OTD; OFO; OI; USBP; and AMO.

  - As with the earlier search, the aforementioned offices were provided a copy of the FOIA request and, based on their experience and knowledge of their program office practices and activities, forwarded the request and instructions to the appropriated individual employee(s) and/or component office(s) within the program office that they believed were likely to have responsive records, if such records existed.

  - The individual(s) and component office(s) conducted searches of their file systems, including paper files and electronic files, which, in their judgment, based on their knowledge of the manner in which they routinely keep records, likely contained responsive documents, if they existed.

  - Below are office-specific responses concerning the nature of their respective searches:

    - Air and Marine Operations (AMO)

- U.S. Customs and Border Protection's (CBP) Air and Marine Operations (AMO) is a federal law enforcement organization. With approximately 1,800 federal agents and mission support personnel, 240 aircraft, and 300 marine vessels operating throughout the United States, Puerto Rico, and U.S. Virgin Islands, AMO conducts its mission in the air and maritime environments at and beyond the border, and within the nation's interior. AMO interdicts unlawful people and cargo approaching U.S. borders, investigates criminal networks and provides domain awareness in the air and maritime environments, and responds to contingencies and national taskings.

- AMO Headquarters, generally keeps its files electronically on an internal shared drive. With regard to the Plaintiff's requests, AMO tasked each of its commands who collect electronic information and investigative data to conduct searches for responsive records. Those commands are AMO, Air and Marine Operations Center (AMOC) and AMO Investigations. Those offices independently did a search of their internal collection methodologies and did a due diligence analysis of their techniques and technologies. They found, using the above provided definitions, that they do not have any responsive records and do not engage in investigative techniques that fall within said definitions.

▪ Office of Intelligence (OI)

- OI is the CBP office responsible for enabling CBP's operational advantage in combating terrorism and transnational crime by providing timely, relevant, and actionable intelligence to drive operations, planning, and decision-making in the border security strategic environment. OI does not use techniques to remotely access computers as described in the definition. OI deemed it unnecessary to conduct a search for responsive records because OI does not conduct or use any offensive nor defensive collection technology, including cyberwarfare, in support of its mission to provide intelligence services or develop strategic threat pictures intended to inform CBP resource and operational decisions.

- U.S. Border Patrol (USBP)

    - The USBP Intelligence Division and Policy Division were contacted with the request related to investigative techniques that involve remote transmittal of code to effect the agency's ability to access, without the owner's knowledge, information from computer systems or other devices not in the Government's possession and that have been deployed in criminal and/or civil law enforcement investigations, including but not limited to the following: immigration, customs, border, tax, drugs, computer crimes, and financial enforcement efforts.
    - The Policy Division responded that USBP uses no techniques involving the remote transmittal of codes in order to gain access to electronic devices similar to Trojan viruses, remote application programming, or malware through social engineering.
    - The Intelligence Division responded that USBP does not conduct any type of investigations involving any type of remote access or "hacking" through spyware or malware through social engineering techniques. Furthermore, USBP does not have any records involving licenses, policies, approvals or agreements with any state, local, federal law enforcement agencies concerning "computer network exploitation" or a "network investigative technique."

- Office of Field Operations' National Targeting Center (NTC)

    - CBP is responsible for inspecting travelers and cargo entering and departing the United States to enforce the customs, immigration, and agriculture laws and regulations of the United States and to enforce hundreds of laws on behalf of numerous federal agencies. NTC was created in December 2001 in response to the 9/11 terrorist attacks with a mandate to target suspected terrorists, their supporters, and their weapons. Today, NTC is CBP's principal counterterrorism facility. Its mission is to prevent dangerous and unlawful travelers and goods from entering and exiting the country by effectively vetting, reviewing, identifying, and segmenting low and high-risk passengers and cargo across all international

modes of transportation, inbound and outbound, in order to identify, target, and coordinate examination of travelers and shipments that may be connected to terrorism or other transnational crimes.

- NTC was asked to identify documents related to the "investigative techniques" as defined in Defendant's July 12, 2019 letter.
- NTC personnel whose official responsibilities involve "computer systems and other devices" and thus most likely to have knowledge of such records, were asked to identify any responsive records relating to the above referenced definition. The NTC personnel confirmed NTC does not engage in investigative techniques as described in the above referenced definition and therefore would not have any responsive records.